



ADMINISTRATOR GUIDE

UC Software 7.1.0 | June 2021 | 3725-49793-005A

# Poly CCX Business Media Phones with OpenSIP

## Getting Help

For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)  
345 Encinal Street  
Santa Cruz, California  
95060

© 2021 Plantronics, Inc. All rights reserved. Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.

# Contents

---

<b>Before You Begin.....</b>	<b>11</b>
Audience, Purpose, and Required Skills.....	11
Related Poly and Partner Resources.....	11
Privacy Policy.....	12
Poly CCX Phones Model Numbers.....	12
<b>Getting Started.....</b>	<b>13</b>
Product Overview.....	13
Configuration Options.....	13
UC Software Provisioning Methods.....	13
Default Configuration File.....	14
Configure a Phone Using Simple Setup.....	14
Configure a Phone Through the System Web Interface.....	15
Configure a Phone with a USB Flash Drive.....	15
<b>Setting Up the Phone.....</b>	<b>17</b>
Power CCX Phones.....	17
Complete the Setup Wizard.....	17
Managing Peripheral Devices.....	18
Disable Headset Use.....	18
Connect a Computer to a Network Through the Phone.....	18
Disable USB Audio Mode.....	19
<b>Networking.....</b>	<b>20</b>
System Names Transmitted with Network Protocols.....	21
Configuring Internet Protocol Settings.....	21
Configure a Static IPv4 Address.....	21
Enable IPv4 ICMP Redirects.....	22
DHCP IP Address.....	22
Wi-Fi Network Connectivity.....	24
Configure Wi-Fi Using a Configuration File.....	24
Configure Wi-Fi Using the Local Interface.....	25
Remove Wi-Fi from the Basic Settings Menu.....	26
Bluetooth Settings.....	26
Enable Bluetooth.....	27
Update the Bluetooth Device Name.....	27
Configure Bluetooth Features.....	27

Setting the Time and Date.....	28
Configure Time and Daylight Saving Time.....	28
Set the Time Zone Location.....	29
Configure Olson Time Zone.....	33
IP Multimedia Subsystem Features.....	37
Enable 3GPP IP Multimedia.....	37
Create a Custom TCP Keep-Alive Message.....	38
Create a Custom UDP Keep-Alive Message.....	38
Enable the P-Early-Media Header.....	38
Remove the Outbound Proxy Address from the Route Header.....	39
Add Path Extension Header to Request Message.....	39
Subscribe to Registered Line State Change Notifications.....	39
Reject Calls with Network Determined User Busy Events.....	40
Enable Server-Specific Features.....	40
Include Service Route Information in VQMon Messages.....	40
Enable Support for the 199 Response Code.....	41
Enable Advice of Charge.....	41
Enable and Configure TWAMP.....	41
Technical Report-069.....	42
Configure TR-069 in the System Web Interface.....	42
Enable and Configure TR-069 Using a Configuration File.....	43
TR-106 Parameters Mapped to Poly Parameters.....	43
TR-104 Parameters Mapped to Poly Parameters.....	44
Supported TR-069 Remote Procedure Call (RPC) Methods.....	46
Configure Network Signaling Validation.....	47
Jitter Buffer and Packet Error Concealment.....	48
Configure Jitter Buffer for Wired Network Voice Traffic.....	49
Configure Jitter Buffer for IP Multicast Voice Traffic.....	49
Set 802.1p/Q Priority.....	50
Provisional Polling of Phones.....	50
Configure Polling for Provisioning Updates.....	51
Configure Provisional Polling for Multiple Phones at Random Times.....	52
Configure SIP Subscription Timers.....	52
Configure the SIP Instance Identification Settings.....	53
Configure SIP Header Warnings.....	54
<b>IP Type-of-Service.....</b>	<b>54</b>
Enable IP Type-of Service.....	54
Configure IP Type-of-Service for Video.....	55
SIP Server Registration.....	56
Configure VoIP Server DHCP Settings.....	56
SIP Signaling Failure for Outgoing Calls.....	57
Static DNS Cache.....	58

Configure the SIP Server.....	58
Configure the Static DNS Cache with A Record IP Addresses.....	59
Configure the Static DNS Cache with NAPTR and SRV Records.....	60
DNS SIP Server Name Resolution.....	61
For Outgoing Calls (INVITE Fallback).....	61
Customer Phone Configuration.....	62
Server Redundancy.....	62
Configuring Server Redundancy for a Registered Line.....	63
Configure Server Redundancy for VoIP.....	64
Configure NAT.....	65
Real-Time Transport Protocol.....	66
Configure SIP RTP for FECC.....	67
Configure RTP Media Ports.....	67
Configure RTP Video Ports.....	68
Configure STUN Settings.....	68
Enable GZIP Encoding.....	69
<b>Securing the Phones.....</b>	<b>70</b>
Phone Passwords .....	70
Configure Password Settings.....	70
Set the Administrator Password on the Local Interface.....	71
Set the User Password on the Local Interface.....	71
California SB-327 Password Requirement Compliance.....	72
System Web Interface Security Settings.....	72
Configure a Security Banner for the System Web Interface.....	72
Locking the System Web Interface After Failed Login Attempts.....	72
Configure Session Management Rules.....	73
Locking the Phone.....	74
Lock the Basic Settings Menu.....	74
Enable Phone Lock.....	74
Set an Automatic Phone Lock.....	75
Define Authorized Contacts to Call from a Locked Phone.....	75
Enable Do Not Disturb When the Phone Locks.....	75
Remotely Unlock a Phone.....	75
Advanced User Access to Administration Settings.....	76
Enable Advanced User Access.....	76
Disable Advanced User Access to Network Settings.....	76
Disable Advanced User Access to TLS Security.....	77
Hide the MAC Address.....	77
Hide the Address of Record.....	77
Certificates.....	77

Using the Factory-Installed Certificate.....	77
Creating CSRs.....	78
Custom URL Locations for LDAP Server CAs.....	79
Enable OCSP.....	80
Enable and Configure SCEP.....	81
Custom Wi-Fi Certificates.....	82
Encryption.....	83
Encrypt Files for Upload.....	83
Change the Encryption Key from the Local Interface.....	84
Web Proxy.....	85
Supported HTTP/HTTPS Web Proxy Services.....	85
Manually Configure Web Proxy Access.....	85
Disable Unused External Ports.....	86
Enable Voice over Secure IP.....	87
Enable and Configure 802.1X Security.....	87
Enable FIPS 140-2 Encryption.....	88
<b>Configuring Audio Settings.....</b>	<b>89</b>
Automatic Gain Control.....	89
Enable AEC for Headsets.....	89
Noise Suppression.....	90
Poly NoiseBlock.....	90
Acoustic Fence.....	90
Configure VAD.....	92
Comfort Noise.....	93
Configure Comfort Noise for Speakerphone Calls.....	93
Configure Comfort Noise for Handset Calls.....	94
Audio Codecs.....	94
Supported Audio Codec Specifications.....	94
Set Audio Codec Priority.....	96
Configure the SILK Audio Codec.....	98
Configure the Opus Audio Codec.....	98
<b>Configuring Video Settings.....</b>	<b>100</b>
Camera Options.....	100
Disable Far End Camera Control.....	100
Enable the Camera Button in the Main Menu.....	101
Remove Camera Settings from the Basic Menu.....	101
Configure a Camera Home Preset.....	101
Configuring the Call Mode for Outgoing Calls.....	102
Set the Default Call Mode to Audio-Only.....	102

Mute Video at the Start of Video Calls.....	102
Enable the Audio Call Button.....	103
Enable Call Mode Persistence.....	103
I-Frames.....	103
<b>Configuring Call Controls.....</b>	<b>105</b>
Do Not Disturb.....	106
Enable Call Server-Based Do Not Disturb on a Registered Line.....	107
Call Hold.....	107
Configure Call Hold Reminders.....	107
Configure Hold Music.....	108
Change the Reinvite Method.....	108
Configure Default Call Transfer Type.....	108
Call Forwarding.....	109
Forward Calls While Busy.....	109
Forward Calls While DND Is Active.....	109
Forward Unanswered Calls.....	110
Disable Call Forwarding.....	110
Convert the Call Timer to Display in Seconds.....	110
Call Waiting Alerts.....	111
Silence the Ringtone for Call Waiting.....	111
Disable Call Waiting Alerts.....	111
Configure Call Waiting for a Specific Line.....	111
Use Network Signaling for Caller ID.....	112
Enable the Remote Party Disconnect Alert.....	112
Configure Directed Call Pickup.....	113
Configure the Call Park and Retrieve Star Code.....	113
Voicemail.....	114
Configure Voicemail Settings.....	114
Disable Voicemail.....	114
Enable Local Call Recording.....	114
Missed Call Notifications.....	115
Configure Last Call Return.....	115
Enable the Conference Meeting Dial-In Options List.....	115
Conference Call Host Management.....	116
Enable Conference Host to Place Participants on Hold.....	116
End a Conference Call When the Host Disconnects.....	116
Disable Conference Management Options.....	117
Configure Hot Dialing.....	117
Multiple Call Appearances.....	117
Configure the Number of Line Keys Per Registration.....	117

Configure the Maximum Number of Concurrent Calls Per Registration.....	118
Flexible Call Appearances.....	118
Busy Lamp Field.....	119
Busy Lamp Field Icons.....	119
Subscribe to a Busy Lamp Field Resource List on a Call Server.....	120
Configure a Busy Lamp Field Resource in the Configuration File.....	120
Configure Key System Emulation.....	121
Enable Instant Messaging.....	123
Shared Lines.....	123
Enable a Shared Line.....	123
Shared Call Appearances.....	124
Enable Private Hold on Shared Lines.....	125
SIP-B Automatic Call Distribution.....	125
Configure Bridged Line Appearance.....	126
PTT and Group Paging.....	127
Configure Phones to Receive Group Pages.....	127
Configuring PTT.....	128
Enable SIB-B Group Call Pickup .....	130
Intercom Calls.....	130
Enable Intercom Calls.....	130
Creating a Custom Intercom Soft Key.....	131
Configure E.911.....	131
<b>Configuring Phone Settings.....</b>	<b>132</b>
Multiple Line Registrations.....	132
Local Digit Map.....	133
Configure a Local Digit Map.....	133
Change the Dialing Timeout.....	133
Change the International Dialing Prefix.....	134
User Profiles.....	134
Enable Multiple User Profiles on the Phone.....	134
User Profile Authentication.....	135
Require a User Login.....	138
Mask the User Password Entry.....	138
Enable User Login Persistence.....	138
Presence Status.....	139
Enable Presence Status to Display on the Phone.....	139
Disable Presence Softkeys.....	139
Power Saving on CCX Phones.....	139
Configure Power Saving.....	140
Disable Power Saving.....	140

Microphone Mute.....	141
Enable Microphone Mute/Unmute Alert.....	141
Configure Mute Reminder Alert Interval.....	141
Disable Microphone Mute Persistence.....	141
Enable Persistent Call Volume.....	142
Disable DTMF Tones.....	142
Audible Notifications and Sounds.....	143
Set the Audible Notification and Sound Output.....	143
Disable the Phone's Welcome Sound.....	143
Disable Audible Notifications and Sounds.....	144
Disable the Voicemail Stutter Dial Tone.....	144
Ringtones and Visual Incoming Call Indicators.....	144
Sound Effects.....	147
<b>Third-Party Servers.....</b>	<b>153</b>
Microsoft Exchange Integration.....	153
Configuring the Microsoft Exchange Server.....	153
Microsoft Exchange Calendar.....	155
Ribbon Communications Server.....	157
Multiple Appearance Directory Number - Single Call Appearance.....	157
Configure the Global Address Book.....	159
Configure the Personal Address Book.....	159
Configuring 911 Location for Ribbon Communications.....	160
Configure Emergency Instant Messages.....	160
BroadSoft BroadWorks Server.....	161
Authentication with BroadWorks XSP Service Interface.....	161
Polycom BroadSoft UC-One Application.....	162
Enable Anonymous Call Rejection.....	164
Enable BroadWorks Call Decline on a Shared Line.....	164
Enable and Configure Hoteling.....	164
Flexible Seating.....	165
Executive-Assistant Lines.....	166
Configure Enhanced Call Park.....	168
Enable BroadSoft Directories.....	168
Centralized Call Recording.....	169
Enable Simultaneous Ring.....	170
Enable Line ID Blocking.....	170
Enable BroadWorks Anywhere.....	171
Enable Remote Office.....	171
BroadSoft Server-Based Call Forwarding.....	171
Enable Visual Security Classification Display.....	172



Enable Feature-Synchronized Automatic Call Distribution.....	172
Enable uaCSTA on a Dedicated Line.....	173
<b>Directories and Contacts.....</b>	<b>175</b>
Local Contact Directory.....	175
Set the Maximum Number of Contacts in the Local Directory.....	175
Creating Directory Files.....	175
Disable the Local Contact Directory.....	179
Create a Speed Dial Entry in the Directory File.....	179
Disable Local Speed Dial Edits.....	180
Corporate Directory.....	180
Connect to a Corporate Directory Using LDAP.....	180
Securely Store LDAP Credentials.....	181
Call Lists.....	181
Disable the Missed Call List.....	181
Disable the Placed Call List.....	182
Disable the Received Call List.....	182
Disable All Call Lists.....	182
Disable Consultation Call Logging.....	182
List Consecutive Calls Individually.....	183
Enable Exchange Call Logs.....	183
<b>Configuring the Local Interface.....</b>	<b>184</b>
Localizing the User Interface.....	184
Edit Phone Languages.....	184
Change the Keyboard Layout.....	185
Enable Pinyin Text on the Phone.....	186
Configure the Phone's Display Name.....	186
Configuring Labels.....	187
Configure Labels in the Local Interface.....	187
Create a Custom Label with a Configuration File.....	187
Configure Unique Line Labels for Registration Lines.....	188
Enable and Configure the Digital Phone Label.....	189
Time and Date Display.....	189
Disable the Time and Date on the Idle Display.....	189
Configure Time and Date Display Settings.....	189
Change the Date Format.....	190
Set a Preferred Home Screen.....	191
Change Colors for Display Elements.....	191
Set Up a Custom Background.....	192
Configure a Line Registration Key Icon.....	193

Digital Picture Frame.....	194
Map Digital Picture Frame Location.....	194
Adjust the Digital Picture Frame Refresh Duration.....	194
Disable the Digital Picture Frame.....	194
LED Indicators.....	195
LED Indicator Pattern Types.....	195
Set an LED Pattern for Active Calls.....	196
Set an LED Pattern on BLF for Held Calls.....	196
Set an LED Pattern for Incoming Calls.....	197
Set an LED Pattern for Self-Parked Calls.....	197
Set an LED Pattern for Remote-Parked Calls.....	197
Configure LED Behavior for Held Calls on Shared Lines.....	197
Disable the Headset Key LED in Headset Memory Mode.....	198
Disable Message Waiting Indicator in Power Saving Mode.....	198
<b>Phone Maintenance.....</b>	<b>199</b>
Analytics Support for Poly Cloud Services.....	199
Busy Lamp Field Analytics.....	199
Shared Call Appearance Analytics.....	200
User Interface Analytics.....	200
UPtime Analytics.....	200
Hardware Analytics.....	201
Device Details Sent to the Cloud.....	202
VQMon Reports.....	205
Configure VQMon Alerts.....	205
Monitoring the Phone's Memory Usage.....	206
Phone Memory Resources.....	207
Check Memory Usage from the Local Interface.....	208
Configure a Phone Memory Alert.....	208
Memory Usage Errors in the Application Log.....	208
Capturing the Phone's Screen.....	208
Enable Screen Capture.....	208
Capture the Phone's Screen.....	209
Rebooting the Phone.....	209
Reboot the Phone.....	209
Reboot the Phone at a Scheduled Time.....	210
Disable the Phone Boot Status Message.....	210
Upgrading the Software.....	210
Upgrading the Software on a Single Phone.....	211
Configure User-Controlled Software Updates and Polling.....	211
Upgrade UC Software Using a USB Flash Drive.....	211

Resetting a Phone to Factory Defaults.....	212
Reset the Phone and Configuration.....	212
Factory Reset the Phone at Power-Up.....	213
Enable Users to Reset the Phone to Factory.....	213
<b>Troubleshooting.....</b>	<b>215</b>
Record Your Phone's Version Information.....	215
System Logs.....	216
Configuring Log Files.....	216
Logging Levels.....	216
Upload Logs to a USB Flash Drive.....	217
Retrieve Logs Using the System Web Interface.....	217
Retrieve Logs from the Support Information Package.....	218
View the Phone's Status.....	218
Upload a Phone's Configuration Files.....	219
Test Phone Hardware.....	220
Perform Network Diagnostics.....	220
Configure Remote Packet Capture.....	220
Updater Error Messages and Possible Solutions.....	221
Polycom UC Software Error Messages.....	222
Network Authentication Failure Error Codes.....	223
Power and Start-up Issues.....	225
Screen and System Access Issues.....	225
Calling Issues.....	226
Display Issues.....	227
Audio Issues.....	228
Software Upgrade Issues.....	228
Provisioning Issues.....	229

# Before You Begin

---

## Topics:

- [Audience, Purpose, and Required Skills](#)
- [Related Poly and Partner Resources](#)
- [Privacy Policy](#)
- [Poly CCX Phones Model Numbers](#)

This *Poly CCX Business Media Phones with OpenSIP Administrator Guide* contains overview information for navigating and performing tasks on Poly CCX phones.

The information in this guide applies to the following Poly devices except where noted:

- Poly CCX 400 business media phone
- Poly CCX 500 business media phone
- Poly CCX 600 business media phone
- Poly CCX 700 business media phone
- Polycom EagleEye Mini USB camera

## Audience, Purpose, and Required Skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment
- OpenSIP networks and VoIP endpoint environments

## Related Poly and Partner Resources

See the following sites for information related to this product.

- The [Poly Online Support Center](#) is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The [Poly Document Library](#) provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The [Poly Community](#) provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The [Poly Partner Network](#) is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs,

making it easy for you to communicate face-to-face using the applications and devices you use every day.

- The [Poly Services](#) help your business succeed and get the most out of your investment through the benefits of collaboration.

## Privacy Policy

Poly products and services process customer data in a manner consistent with the [Poly Privacy Policy](#). Please direct comments or questions to [privacy@poly.com](mailto:privacy@poly.com)

## Poly CCX Phones Model Numbers

The following table lists the product names, model numbers for Poly CCX business media phones.

Product Name	Model Number
Poly CCX 400 business media phone	3111-49700-001
Poly CCX 500 business media phone	3111-49710-001
Poly CCX 600 business media phone	3111-49770-001
Poly CCX 700 business media phone	3111-49740-001

# Getting Started

---

## Topics:

- [Product Overview](#)
- [Configuration Options](#)

Although you can deploy UC Software by configuring individual phones, Poly recommends setting up a provisioning server on your LAN or the internet for large-scale deployments.

## Product Overview

UC software manages the protocol stack, the digital signal processor (DSP), the local interface, and the network interaction on Poly phones.

UC software implements the following functions and features on the phones:

- VoIP signaling for a wide range of voice and video telephony functions using SIP signaling for call setup and control.
- Industry-standard security techniques for ensuring that the systems robustly authenticate and encrypt all provisioning, signaling, and media transactions.
- Advanced audio signal processing for speakerphone communications using a wide range of audio codecs.
- Flexible provisioning methods to support single-phone, small business, and large multisite enterprise deployments.

## Configuration Options

Poly offers several methods to configure or provision your phone.

Poly phones come installed with updater software that resides in the flash memory of the phone. When you boot up or reboot the phone, the updater automatically updates, downloads, and installs new software versions or configuration files as needed, based on the server or phone settings.

You can configure the phone's settings using simple setup, the system web interface, or a USB flash drive. You can also use configuration files through the system web interface to copy phone settings from one phone to another.

If you need to set up more than 20 phones, Poly recommends using a centralized provisioning server instead of manual configuration.

## UC Software Provisioning Methods

Poly provides several methods to provision phones and configure phone features. The method you use depends on the number of phones in your deployment, the phone model(s), and how you want to apply features and settings.

You can use multiple methods simultaneously to provision and configure features. There is a priority among the methods that impacts your phone deployment when you use multiple methods simultaneously.

If there is a discrepancy among multiple provisioning methods or configuration settings, the Poly phone uses the setting set with the higher-priority method based on the following hierarchy:

1. Quick setup
2. Local interface (the phone menu)
3. System web interface (Web Configuration Utility)
4. USB
5. Polycom RealPresence Resource Manager
6. Centralized provisioning
7. Default phone values

For example, when you provision the phones using a provisioning server and subsequently apply settings using the system web interface, the system web interface setting overrides any duplicate settings you set from the provisioning server. Likewise, any settings set from the local interface override any duplicate settings you set using the system web interface.

For more information on provisioning phones, see the Poly CCX Business Media Phones Provisioning Guide

## Default Configuration File

The default configuration file provides flexibility in large deployments to customize features and settings for your phones.

Use this file to configure features and apply settings for all the phones in your deployment, including groups of phones, specific phone models, or a single phone. The default configuration file applies settings from the component configuration files listed in the CONFIG\_FILES XML attribute in the following ways:

- Phones read the files you enter from left to right.
- Duplicate settings are applied from the configuration file in the order you list them.

The default name for the configuration file is `000000000000.cfg`. You can use the default name or rename the default configuration file. The file name must contain at least five characters and end with `.cfg`.

You can also specify the location of the default configuration file you want the phones to use, for example, `http://usr:pwd@server/dir/example1.cfg`.

## Configure a Phone Using Simple Setup

Use the **Simple Setup** option in the system web interface to configure the minimum settings you need for your phone to work.

### Procedure

1. Enter your phone's IP address into a web browser.  
To find your phone's IP address, go to **Settings > Status > System Information**.
2. Select **Admin** as the login type and enter the administrator password.
3. Select **Simple Setup**.
4. Configure the following settings:

Settings	Description
Phone Language	Phone display language
SNTP Server	Server that the phone uses to calculate the time that shows on the display
Time Zone	Time zone where the phone is located
SIP Server	Server address and port that the phone uses for line registrations
SIP Outbound Proxy	Server address and port that the phone uses to send all SIP requests
SIP Line Identification	Information your phone needs to make calls

5. Select **Save**.

## Configure a Phone Through the System Web Interface

Export and then reimport a configuration file through the system web interface to configure a single phone.

### Procedure

1. Enter your phone's IP address into a web browser.  
To find your phone's IP address, go to **Settings > Status > System Information**.
2. Select **Admin** as the login type and enter the administrator password.
3. Go to **Utilities > Import & Export Configuration**.
4. Choose the file to export from the **Export Configuration (except Device Settings)** drop-down menu.
5. Select **Export**.
6. Open the configuration file in an XML editor.
7. Enter or update the parameters in the **Configuration** list and save the configuration file to your system.
8. In the system web interface, go to **Utilities > Import & Export Configuration**.
9. Select **Import**.
10. Select your configuration file.
11. Select **OK**.

## Configure a Phone with a USB Flash Drive

You can manually configure one phone at a time with a USB flash drive.

---

**Note:** Format your USB flash drive as FAT 32. Poly recommends that you use a USB 2.0 flash drive. If you've used the drive before, delete any previous files before you format it.

---

### Procedure

1. Download the UC Software from the [Poly Online Support Center](#).



2. Copy your phone's the configuration files to use to the root of the USB flash drive. The minimum required configuration files are as follows:
  - Primary configuration file: 00000000000000.cfg.
  - The \*.sip.ld file for your phone.
3. Insert the USB flash drive into a USB port on the phone, enter the administrator password, and power cycle the phone.

Wait several minutes for your device to reboot.

# Setting Up the Phone

---

## Topics:

- [Power CCX Phones](#)
- [Complete the Setup Wizard](#)
- [Managing Peripheral Devices](#)

See the setup sheets applicable to your phone and its peripheral devices at the [Poly Online Support Center](#).

## Power CCX Phones

Poly recommends powering your phones with PoE when available. If your Ethernet port doesn't support PoE, use an optional power supply.

---

**Important:** If you're using a power supply, ensure you use the correct power supply for your phone.

---

### Poly CCX Power over Ethernet Classes

Phone Model	PoE Class	PoE Class Maximum	Normal Call	Maximum with All USB Loading
CCX 400	3	12.95 W	5 W	12 W
CCX 500	0	12.95 W	7 W	12 W
CCX 600	4	25.5 W	11 W	18 W
CCX 700	4	25.5 W	13 W	20 W

### Procedure

- » Do one of the following:
  - Plug a cable from a PoE-enabled Ethernet wall port to the Ethernet port on the phone.
  - Plug a supported AC power adapter from a power outlet to the power jack on the phone.

## Complete the Setup Wizard

The phone walks you through a setup wizard when you first power it on.

### Procedure

1. Power on the phone.
2. Enter and confirm a new administrator password.

---

**Note:** You can't set the administrator password as the default password, which is 456.

---

3. The system displays the Polycom End User License Agreement (EULA). Review and accept the EULA by selecting **Accept**.

You can also review the EULA in the **Documentation** tab for your phone's support page at the [Poly Online Support Center](#).

4. Select a system language.
5. Set your time zone ID.
6. Choose the system's base profile from the displayed list. Select **Next** and confirm your selection.

The phone starts in your selected base profile.

## Managing Peripheral Devices

Configure the phone to work with other hardware in the workspace.

### Disable Headset Use

Prevent the phone from using headsets plugged into it.

#### Procedure

- » Disable headset use.

```
up.headsetModeEnabled="0"
```

### Connect a Computer to a Network Through the Phone

Poly phones allow you to connect your computer to your network through the phone.

The phone includes an Ethernet and LAN port (both RJ-45 connectors) with an internal Ethernet switch. This switch allows you to use your phone as an Ethernet hub.

---

**Note:** If you're using a VLAN, set the 802.1p priorities for both default and RTP packet types to 2 or greater. Setting this priority ensures that audio packets from the phone have priority over packets from the PC port.

---

#### Procedure

1. Connect one side of a network cable to an available port in your network. The phone side should be an RJ-45 connector.
2. Connect the other side of the network cable to the Ethernet RJ-45 port on the back of the phone.
3. Using a second Ethernet networking cable, plug an RJ-45 connector into the LAN RJ-45 port.
4. Connect the other side of the cable connected to the phone's LAN port to the network port on the PC.

## Disable USB Audio Mode

USB audio mode enables users to connect their Poly CCX Business media phones to a computer to use as an external USB audio device.

This mode is enabled by default. Once you disable USB audio mode, users can't set the phone as a USB audio device.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Disable USB audio mode on the phone.

```
feature.usb.device.audio="0"
```

# Networking

---

## Topics:

- [System Names Transmitted with Network Protocols](#)
- [Configuring Internet Protocol Settings](#)
- [Wi-Fi Network Connectivity](#)
- [Bluetooth Settings](#)
- [Setting the Time and Date](#)
- [IP Multimedia Subsystem Features](#)
- [Enable Advice of Charge](#)
- [Enable and Configure TWAMP](#)
- [Technical Report-069](#)
- [Configure Network Signaling Validation](#)
- [Jitter Buffer and Packet Error Concealment](#)
- [Set 802.1p/Q Priority](#)
- [Provisional Polling of Phones](#)
- [Configure SIP Subscription Timers](#)
- [Configure the SIP Instance Identification Settings](#)
- [Configure SIP Header Warnings](#)
- [IP Type-of-Service](#)
- [SIP Server Registration](#)
- [Static DNS Cache](#)
- [DNS SIP Server Name Resolution](#)
- [Server Redundancy](#)
- [Real-Time Transport Protocol](#)
- [Configure STUN Settings](#)
- [Enable GZIP Encoding](#)

Poly phones support several wireless modes, security options, radio controls, and Quality of Service monitoring.

All phones connect through Ethernet, although some can connect via Wi-Fi as well.

## System Names Transmitted with Network Protocols

The phone transmits its system name with network protocols. To customize your network for specific phone models, parse the network packets for these strings.

The phone's system name is the model name with no spaces, followed by an underscore and the last 4 digits of the phone's MAC address.

For example: CCX700\_D1EB

### System and Model Names

Model	System Name
CCX 400	CCX400_<MAC>
CCX 500	CCX500_<MAC>
CCX 600	CCX600_<MAC>
CCX 700	CCX700_<MAC>

## Configuring Internet Protocol Settings

The phone depends on a reliable network connection to perform all of its core functions.

Poly phones place and receive audio/video calls using a network connection. Other features rely on a network connection as well, such as the phone's ability to sync with a user's calendar to join meetings.

### Configure a Static IPv4 Address

Configure IPv4 mode in the phone's local interface.

Connect your phone to an Ethernet network connection.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Ethernet Menu**.
2. Select **IP Mode > IPv4**.
3. Select **IPv4 Configuration**.
4. Clear the **DHCP** check box.
5. Configure the following settings:
  - **IP Address**

- **Subnet Mask**
  - **IPv4 Gateway**
6. Back out of the menus. When prompted, select **Save Config**.  
The phone reboots.

## Enable IPv4 ICMP Redirects

To ensure your phones communicate using the optimal network route, configure IPv4 to allow Internet Control Message Protocol (ICMP) redirects.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Configure the phone to allow you to enable the ICMP redirect parameter.

```
device.icmp.ipv4IcmpIgnoreRedirect.set="1"
```

2. Enable ICMP redirects.

```
device.icmp.ipv4IcmpIgnoreRedirect="0"
```

## DHCP IP Address

The phone enables DHCP by default.

If the phone can't communicate with the DHCP server on startup, the phone's status bar reports **Network Down**. The phone communicates with the DHCP server every 5 minutes to acquire an IP address or for lease renewal.

## Set the DHCP Boot Server Option in IPv4 Mode

Configure the phone based on the DHCP boot server option in IPv4 mode.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Set the phone to get the boot server details from the custom options number provided through DHCP.

The following values apply:

- 0 (Default) - The phone gets the boot server address from option 66.
- 1 - The phone gets the boot server details from the custom option number provided through DHCP.
- 2 - The phone uses the boot server configured through the **Server** menu.

- 3 - The phone uses the custom option first or uses option 66 if the custom option isn't present.

```
device.dhcp.bootSrvUseOpt="<value>"
```

## Enable DHCP IP Address Cache

Enable DHCP IP address cache to retain IP addresses on the phones when the DHCP server becomes unavailable.

When you enable the IP address cache feature, there isn't a service interruption even if the IP address lease time expires and the DHCP server doesn't respond. The phone periodically attempts to resume DHCP service with a new DHCP Discover message for the entire time the cached IP address is in use.

DHCP IP address cache stores the following lease parameters:

- Interface
- IP address
- Subnet mask
- Gateway
- DNS server
- Domain name

DHCP IP address cache has the following limitations:

---

**Important:** If a DHCP server restarts and loses lease details, enabling DHCP IP address cache can lead to IP address conflicts on the phones. This results in cascading service outages.

---

- The phones don't cache DHCP option 99 values for Enhanced 911 location services. A WAN outage may affect IP address cache and emergency calling services.
- If a DHCP server restarts and loses lease details, enabling DHCP IP address cache can lead to IP address conflicts on the phones. This results in cascading service outages.
- DHCP IP address cache supports only IPv4 addresses. DHCP IP address cache doesn't currently support IPv6 addresses.
- DHCP IP address cache doesn't support DHCP VLAN Discovery (DVD).
- If you move a phone from one VLAN to another VLAN where DHCP doesn't respond, the phone continues to use the cached IP address.
- The phones can't update the software using DHCP IP address cache. When the phones attempt to update Poly UC software without DHCP server availability, the phones experience a reboot loop. This continuous reboot loop occurs only when:
  - A cached IP address is in use.
  - The DHCP server is unavailable.
  - A software provisioning server is available.
  - New software is available on the provisioning server.
- You can use DHCP IP address cache only for the UC Software application; you can't use it for the Updater.



## Procedure

1. Enable the phone to use a cached IP address if the phone doesn't receive a new IP address from the DHCP user.

```
device.net.cachedIPAddress="1"
```

2. If the phone uses a cached IP address, configure how long the phone waits, in seconds, to attempt to get a new IP address from the DHCP server. This parameter is only available when you enable `device.net.cachedIPAddress`.

The default is 3600. The value range is 300 to 7200.

```
device.net.cachedIPAddressRetryTime="<value>"
```

## Wi-Fi Network Connectivity

Enabling Wi-Fi automatically disables the Ethernet port. You can't use Wi-Fi and Ethernet simultaneously to connect phones to your network.

---

**Note:** CCX 400 and CCX 500 business media phones don't support Wi-Fi.

---

Note the following when using Wi-Fi:

- The phone still requires power using a power adapter for power when using Wi-Fi.
- When you connect the system to your network over Wi-Fi, you can only place audio-only calls.
- The phone doesn't support Wi-Fi captive portals or Wireless Display (WiDi).

Your phone supports the following wireless modes:

- 2.4 GHz / 5 GHz operation
- IEEE 802.11a radio transmission standard
- IEEE 802.11b radio transmission standard
- IEEE 802.11g radio transmission standard
- IEEE 802.11n radio transmission standard

---

**Note:** When you provision via a Wi-Fi connection to the network, the phone looks for files on the provisioning server using the LAN MAC address and not the Wi-Fi MAC address.

---

## Configure Wi-Fi Using a Configuration File

Configure your phone's Wi-Fi settings using a provisioning file.

Connect the phone to your Ethernet network to receive the provisioning file.

Set `device.set="1"`.

---

**Note:** CCX 400 and CCX 500 business media phones don't support Wi-Fi.

---

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable Wi-Fi.

```
device.wifi.enabled="1"
```

2. Optional: Set a country of operation.

---

**Note:** Poly recommends this step to ensure the best performance on a Wi-Fi network. If you don't set the country of origin, the phone operates in a world safe mode, which restricts Wi-Fi channels and power.

---

```
device.wifi.country="<two-letter country code>"
```

3. Enable DHCP for Wi-Fi.

```
device.wifi.dhcpEnabled="1"
```

4. Enter the SSID for your Wi-Fi network. The SSID is the network's name as it appears in a network search.

```
device.wifi.ssid="<SSID>"
```

5. Optional: Specify your Wi-Fi network security mode.

```
device.wifi.securityMode="<wireless security mode type>"
```

- If your network uses WEP, configure the WEP key.

```
device.wifi.wep.key="<WEP key>"
```

- If your network uses WPA PSK, WPA2 PSK, or WPA2 PSK Enterprise, configure the security credentials.

```
device.wifi.wpa2Ent.method="<EAP setting>"
device.wifi.wpa2Ent.user="<WPA2 username>"
device.wifi.wpa2Ent.password="<WPA2 password>"
```

## Configure Wi-Fi Using the Local Interface

Using the menus available on the phone's local interface, connect the phone to a Wi-Fi network. This is useful if you don't have an Ethernet connection available so the phone can send a provisioning file to the server.

---

**Note:** CCX 400 and CCX 500 business media phones don't support Wi-Fi.

---

### Procedure

1. Go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu**

2. Optional: Set a country of operation.

---

**Note:** Poly recommends this step to ensure the best performance on a Wi-Fi network. If you don't set the country of origin, the phone operates in a world safe mode, which restricts Wi-Fi channels and power.

---

1. Select **Country of operation**.
2. Choose your country from the list.
3. Select the back arrow.
3. Select **Wi-Fi**.
4. Toggle Wi-Fi on and select the back arrow.  
The phone reboots.
5. Go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu > Wi-Fi**.
6. Select an available Wi-Fi network.
7. Optional: If required, enter the Wi-Fi network's security password.
8. Select **Connect**.  
The phone connects to the network.

## Remove Wi-Fi from the Basic Settings Menu

The default configuration includes a **Wi-Fi** menu item in the **Basic** settings menu.

For increased network security, you can remove the wireless network option from the **Basic** menu. You can restrict phone users from updating wireless network settings from the phone's local interface.

### Procedure

- » Remove the wireless menu option from the **Basic** menu.

```
homeScreen.wifi.enable="0"
```

## Bluetooth Settings

The base configuration disables Bluetooth by default. You can disable Bluetooth entirely, disable certain features, and configure Bluetooth settings.

Limitations with Bluetooth technology may cause voice quality issues when using a Bluetooth headset. You may not experience the highest voice quality using a Bluetooth headset with the 2.4 GHz band enabled. Other Bluetooth devices in the area may also cause interference and quality loss.

## Enable Bluetooth

By default, the phone disables Bluetooth and Bluetooth discovery. Enable Bluetooth on the phone and display it on the local interface.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable Bluetooth.

```
feature.bluetooth.enabled="true"
```

2. Enable Bluetooth radio.

```
bluetooth.radioOn="1"
```

3. For security, you can completely disable Bluetooth or turn it off by default. To disable Bluetooth discovery, set:

```
bluetooth.device.discoverable="0"
```

## Update the Bluetooth Device Name

By default, the system uses the model number as the Bluetooth device name. Update the device name to something that better identifies the device.

### Procedure

- » Update the Bluetooth device name. The maximum length is 20 characters.

```
bluetooth.device.name="<Device name>"
```

## Configure Bluetooth Features

Adjust the default Bluetooth values based on your deployment requirements.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Set the max time that the phone attempts to connect with other devices.

The default value 0 disables the discoverable timeout. The value ranges from 0 to 3600 seconds.

```
bluetooth.discoverableTimeout="x"
```

2. Set the maximum number of devices stored in the phone's memory.

By default, 10 devices remain in the phone's memory. The value ranges from 0 to 3600 seconds.

```
bluetooth.pairedDeviceMemorySize="x"
```

3. Set the maximum number of devices the phone can pair with. If you don't want the phone to store devices in memory, set this value to 0.

By default, 10 devices remain in the phone's memory.

```
bluetooth.device.maxPaired="x"
```

4. Set the amount of time, in minutes, that the phone remains paired with a device when you set `bluetooth.device.maxPaired` to 0.

By default, the phone remains paired for 30 minutes.

```
bluetooth.device.pairedTimeout="x"
```

## Setting the Time and Date

Synchronizing the phone to the SNTP server gives you the most accurate time and date. The phone continuously flashes the time and date until it receives a successful SNTP response.

### Related Links

[Time and Date Display](#) on page 189

## Configure Time and Daylight Saving Time

Configure time, time zone, and daylight saving time on the phone.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Configure the SNTP server to automatically configure the time.

```
tcpIpApp.snmp.address="<valid SNTP hostname or IP address>"
tcpIpApp.snmp.resyncPeriod="<# of seconds>"
```

2. Optional: For time zones offset from GMT by fractions of a whole hour, specify the offset (in seconds) up to one hour (+/- 3600 seconds). A value 0 (default) represents GMT.

```
tcpIpApp.snmp.gmtOffset="<positive or negative integer>"
```

3. Optional: Configure Daylight Saving Time.

```
tcpIpApp.snmp.daylightSavings.fixedDayEnable="1"
tcpIpApp.snmp.daylightSavings.start.month="<set month to start DST>"
tcpIpApp.snmp.daylightSavings.start.date="<date of set month to start DST>"
```

```
DST>"
tcpIpApp.snmp.daylightSavings.start.time="<hour of set date to start
DST>"
tcpIpApp.snmp.daylightSavings.stop.month="<set month to stop DST>"
tcpIpApp.snmp.daylightSavings.stop.date="<date of set stop to start
DST>"
tcpIpApp.snmp.daylightSavings.stop.month="<set month to stop DST>"
```

## Set the Time Zone Location

If you configure your time zone with `device.snmp.gmtOffset` or `tcpIpApp.snmp.gmtOffset`, you must set the correct time zone location to display on the phone and in the system web interface.

Your configuration file must include `device.set="1"`.

### Procedure

- » Set the correct time zone location to display on the local interface and the system web interface.

```
device.snmp.gmtOffsetcityID="<time zone location parameter value>"
```

Use the following parameters to configure the time zone location.

#### Time Zone Location Parameter Values

Permitted Value	Time Zone Description
0	(GMT -12:00) Eniwetok, Kwajalein
1	(GMT -11:00) Midway Island
2	(GMT -10:00) Hawaii
3	(GMT -9:00) Alaska
4	(GMT -8:00) Pacific Time (US & Canada)
5	(GMT -8:00) Baja California
6	(GMT -7:00) Mountain Time (US & Canada)
7	(GMT -7:00) Chihuahua, La Paz
8	(GMT -7:00) Mazatlan
9	(GMT -7:00) Arizona
10	(GMT -6:00) Central Time (US & Canada)

Permitted Value	Time Zone Description
11	(GMT -6:00) Mexico City
12	(GMT -6:00) Saskatchewan
13	(GMT -6:00) Guadalajara
14	(GMT -6:00) Monterrey
15	(GMT -6:00) Central America
16	(GMT -5:00) Eastern Time (US & Canada)
17	(GMT -5:00) Indiana (East)
18	(GMT -5:00) Bogota, Lima
19	(GMT -5:00) Quito
20	(GMT -4:30) Caracas
21	(GMT -4:00) Atlantic Time (Canada)
22	(GMT -4:00) San Juan
23	(GMT -4:00) Manaus, La Paz
24	(GMT -4:00) Asuncion, Cuiaba
25	(GMT -4:00) Georgetown
26	(GMT -3:30) Newfoundland
27	(GMT -3:00) Brasilia
28	(GMT -3:00) Buenos Aires
29	(GMT -3:00) Greenland
30	(GMT -3:00) Cayenne, Fortaleza
31	(GMT -3:00) Montevideo
32	(GMT -3:00) Salvador
33	(GMT -3:00) Santiago
34	(GMT -2:00) Mid-Atlantic
35	(GMT -1:00) Azores
36	(GMT -1:00) Cape Verde Islands
37	(GMT 0:00) Western Europe Time
38	(GMT 0:00) London, Lisbon
39	(GMT 0:00) Casablanca
40	(GMT 0:00) Dublin

Permitted Value	Time Zone Description
41	(GMT 0:00) Edinburgh
42	(GMT 0:00) Monrovia
43	(GMT 0:00) Reykjavik
44	(GMT +1:00) Belgrade
45	(GMT +1:00) Bratislava
46	(GMT +1:00) Budapest
47	(GMT +1:00) Ljubljana
48	(GMT +1:00) Prague
49	(GMT +1:00) Sarajevo, Skopje
50	(GMT +1:00) Warsaw, Zagreb
51	GMT +1:00) Brussels
52	(GMT +1:00) Copenhagen
53	(GMT +1:00) Madrid, Paris
54	(GMT +1:00) Amsterdam, Berlin
55	(GMT +1:00) Bern, Rome
56	(GMT +1:00) Stockholm, Vienna
57	(GMT +1:00) West Central Africa
58	(GMT +1:00) Windhoek
59	(GMT +2:00) Bucharest, Cairo
60	(GMT +2:00) Amman, Beirut
61	(GMT +2:00) Helsinki, Kyiv
62	(GMT +2:00) Riga, Sofia
63	(GMT +2:00) Tallinn, Vilnius
64	(GMT +2:00) Athens, Istanbul
65	(GMT +2:00) Damascus
66	(GMT +2:00) E.Europe
67	(GMT +2:00) Harare, Pretoria
68	(GMT +2:00) Jerusalem
69	(GMT +2:00) Kaliningrad (RTZ 1)
70	(GMT +2:00) Tripoli



Permitted Value	Time Zone Description
71	(GMT +3:00) Moscow
72	(GMT +3:00) St.Petersburg
73	(GMT +3:00) Volgograd (RTZ 2)
74	(GMT +3:00) Kuwait, Riyadh
75	(GMT +3:00) Nairobi
78	(GMT +3:00) Baghdad
76	(GMT +3:00) Minsk
77	(GMT +3:30) Tehran
79	(GMT +4:00) Abu Dhabi, Muscat
80	(GMT +4:00) Baku, Tbilisi
81	(GMT +4:00) Izhevsk, Samara (RTZ 3)
82	(GMT +4:00) Port Louis
83	(GMT +4:00) Yerevan
84	(GMT +4:30) Kabul
85	(GMT +5:00) Yekaterinburg (RTZ 4)
86	(GMT +5:00) Islamabad
87	(GMT +5:00) Karachi
88	(GMT +5:00) Tashkent
89	(GMT +5:30) Mumbai, Chennai
90	(GMT +5:30) Kolkata, New Delhi
91	(GMT +5:30) Sri Jayawardenepura
92	(GMT +5:45) Kathmandu
93	(GMT +6:00) Astana, Dhaka
94	(GMT +6:00) Almaty
95	(GMT +6:00) Novosibirsk (RTZ 5)
96	(GMT +6:30) Yangon (Rangoon)
97	(GMT +7:00) Bangkok, Hanoi
98	(GMT +7:00) Jakarta
99	(GMT +7:00) Krasnoyarsk (RTZ 6)
100	(GMT +8:00) Beijing, Chongqing

Permitted Value	Time Zone Description
101	(GMT +8:00) Hong Kong, Urumqi
102	(GMT +8:00) Kuala Lumpur
103	(GMT +8:00) Singapore
104	(GMT +8:00) Taipei, Perth
105	(GMT +8:00) Irkutsk (RTZ 7)
106	(GMT +8:00) Ulaanbaatar
107	(GMT +9:00) Tokyo, Seoul, Osaka
108	(GMT +9:00) Sapporo, Yakutsk (RTZ 8)
109	(GMT +9:30) Adelaide, Darwin
110	(GMT +10:00) Canberra
111	(GMT +10:00) Magadan (RTZ 9)
112	(GMT +10:00) Melbourne
113	(GMT +10:00) Sydney, Brisbane
114	(GMT +10:00) Hobart
115	(GMT +10:00) Vladivostok
116	(GMT +10:00) Guam, Port Moresby
117	(GMT +11:00) Solomon Islands
118	(GMT +11:00) New Caledonia
119	(GMT +11:00) Chokurdakh (RTZ 10)
120	(GMT +12:00) Fiji Islands
121	(GMT +12:00) Auckland, Anadyr
122	(GMT +12:00) Petropavlovsk-Kamchatsky (RTZ 11)
123	(GMT +12:00) Wellington
124	(GMT +12:00) Marshall Islands
125	(GMT +13:00) Nuku'alofa
126	(GMT +13:00) Samoa

## Configure Olson Time Zone

Configure an Olson time zone on your phone to ensure a more accurate time and date display.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

Use the values in this table to configure the Olson time zone.

**Olson Time Zone IDs**

<b>Olson Time Zone ID</b>	<b>Poly Time Zone ID</b>
Pacific/Midway	(GMT -11:00) Midway Island
Pacific/Honolulu	(GMT -10:00) Hawaii
America/Anchorage	(GMT -9:00) Alaska
Mexico/BajaNorte	(GMT -8:00) Baja California
America/Phoenix	(GMT -7:00) Arizona
America/Chihuahua	(GMT -7:00) Chihuahua,La Paz
America/Denver	(GMT -7:00) Mountain Time (US & Canada)
America/Costa_Rica	(GMT -6:00) Central America
America/Chicago	(GMT -6:00) Central Time (US & Canada)
America/Mexico_City	(GMT -6:00) Mexico City
America/Regina	(GMT -6:00) Saskatchewan
America/Bogota	(GMT -5:00) Bogota,Lima
America/New_York	(GMT -5:00) Eastern Time (US & Canada)
America/Caracas	(GMT -4:30) Caracas
America/Barbados	Atlantic Time (Barbados)
America/Halifax	(GMT -4:00) Atlantic Time (Canada)
America/Manaus	(GMT -4:00) Manaus,La Paz
America/Santiago	(GMT -3:00) Santiago
America/St_Johns	(GMT -3:30) Newfoundland
America/Sao_Paulo	(GMT -3:00) Brasilia
America/Argentina/Buenos_Aires	(GMT -3:00) Buenos Aires
America/Godthab	(GMT -3:00) Greenland
America/Montevideo	(GMT -3:00) Montevideo
Atlantic/South_Georgia	(GMT -2:00) Mid-Atlantic
Atlantic/Azores	(GMT -1:00) Azores
Atlantic/Cape_Verde	(GMT -1:00) Cape Verde Islands
Africa/Casablanca	(GMT 0:00) Casablanca

Olson Time Zone ID	Poly Time Zone ID
Europe/London	(GMT 0:00) London,Lisbon
Europe/Amsterdam	(GMT +1:00) Amsterdam,Berlin
Europe/Belgrade	(GMT +1:00) Bratislava
Europe/Brussels	(GMT +1:00) Brussels
Europe/Sarajevo	(GMT +1:00) Sarajevo,Skopje
Africa/Brazzaville	(GMT +1:00) West Central Africa
Africa/Windhoek	(GMT +1:00) Windhoek
Asia/Amman	Amman
Europe/Athens	(GMT +2:00) Athens
Asia/Beirut	Beirut
Africa/Cairo	(GMT +2:00) Bucharest,Cairo
Europe/Helsinki	(GMT +2:00) Helsinki,Kyiv
Asia/Jerusalem	(GMT +2:00) Jerusalem
Africa/Harare	(GMT +2:00) Harare,Pretoria
Europe/Minsk	(GMT +3:00) Minsk
Asia/Istanbul	(GMT +3:00) Istanbul
Europe/Moscow	(GMT +3:00) Moscow
Asia/Kuwait	(GMT +3:00) Kuwait,Riyadh
Africa/Nairobi	(GMT +3:00) Nairobi
Asia/Tehran	(GMT +3:30) Tehran
Asia/Baku	(GMT +4:00) Baku,Tbilisi
Asia/Yerevan	(GMT +4:00) Yerevan
Asia/Dubai	Dubai
Asia/Kabul	(GMT +4:30) Kabul
Asia/Karachi	(GMT +5:00) Karachi
Asia/Tashkent	(GMT +5:00) Tashkent
Asia/Yekaterinburg	(GMT +5:00) Yekaterinburg (RTZ 4)
Asia/Calcutta	(GMT +5:30) Kolkata,New Delhi

Olson Time Zone ID	Poly Time Zone ID
Asia/Colombo	(GMT +5:30) Sri Jayawardenepura
Asia/Katmandu	(GMT +5:45) Kathmandu
Asia/Dhaka	(GMT +6:00) Astana,Dhaka
Asia/Rangoon	(GMT +6:30) Yangon (Rangoon)
Asia/Krasnoyarsk	(GMT +7:00) Krasnoyarsk (RTZ 6)
Asia/Bangkok	(GMT +7:00) Bangkok,Hanoi
Asia/Jakarta	(GMT +7:00) Jakarta
Asia/Shanghai	(GMT +8:00) Beijing,Chongqing
Asia/Hong_Kong	(GMT +8:00) Hong Kong,Urumqi
Asia/Irkutsk	(GMT +8:00) Irkutsk (RTZ 7)
Asia/Kuala_Lumpur	(GMT +8:00) Kuala Lumpur
Asia/Taipei	(GMT +8:00) Taipei,Perth
Asia/Tokyo	(GMT +9:00) Tokyo,Seoul,Osaka
Asia/Yakutsk	(GMT +9:00) Sapporo,Yakutsk (RTZ 8)
Australia/Adelaide	Adelaide
Australia/Darwin	Darwin
Australia/Brisbane	Brisbane
Australia/Hobart	(GMT +10:00) Hobart
Australia/Sydney	Sydney,Canberra
Asia/Vladivostok	(GMT +10:00) Vladivostok
Pacific/Guam	(GMT +10:00) Guam,Port Moresby
Asia/Magadan	(GMT +10:00) Magadan (RTZ 9)
Pacific/Auckland	(GMT +12:00) Auckland,Anadyr
Pacific/Fiji	(GMT +12:00) Fiji Islands
Pacific/Majuro	(GMT +12:00) Marshall Islands
Pacific/Tongatapu	(GMT +13:00) Nuku'alofa

### Procedure

- » Enter an Olson time zone ID. If you set it to an invalid or unrecognized value, the time zone resets to GMT with daylight saving time disabled.

```
tcpIpApp.snmp.olsonTimezoneID="<Olson time zone ID>"
```

## IP Multimedia Subsystem Features

Poly CCX business media phones support several IP multimedia subsystem features.

- The call waiting ring-back tone plays to inform users that a call is waiting at the far end.
- The phone supports SIP response code 199 (defined in RFC 6228).
- The **Path** extension header field in the SIP Register request message enables accumulating and transmitting the list of proxies between a user agent and registrar server.
- The caller phone can support the p-early-media SIP header that determines whether the caller phone plays a network-provided media or its own media as a ringback tone.
- The VQMon messages generated by the phone can contain service route information in SIP route headers.
- In a NAT network, a phone may need to send keep-alive messages to maintain the IP addresses mapping in the NAT table.

### Enable 3GPP IP Multimedia

Enable the phone to support any IP multimedia (IPM) features.

For an IP multimedia subsystem (IMS) environment, Poly supports a subset of the following 3rd Generation Partnership Project technical specifications (3GPP TS): [24.229](#), [24.615](#), and [24.629](#).

In addition, Poly phones provide partial or complete support for the following RFCs:

- RFC 3327
- RFC 3608
- RFC 3680
- RFC 6665
- RFC 6228
- RFC 3261
- RFC 5009
- RFC 7462
- RFC 7329
- RFC 6026
- RFC 3581
- RFC 6947

**Procedure**

- » Enable support for 3GPP IPM features. This parameter applies to all registered and unregistered SIP lines on the phone.

```
voIpProt.SIP.IMS.enable="1"
```

**Create a Custom TCP Keep-Alive Message**

Configure a string as the payload for TCP keep-alive messages.

**Procedure**

- » Create a custom string to use as the payload of a TCP keep-alive message. You can't leave the string value blank.

The default string is CRLF CRLF CRLF CRLF CRLF CRLF CRLF.

```
nat.keepalive.tcp.payload="<string>"
```

**Create a Custom UDP Keep-Alive Message**

Create a string as the payload of a UDP keep-alive message.

**Procedure**

- » Create a custom string to use as the payload of a UDP keep-alive message. You can leave the string value blank to configure an empty payload.

The default string is CRLF CRLF.

```
parameter nat.keepalive.udp.payload="<string>"
```

**Enable the P-Early-Media Header**

Enable support for the p-early-media header for all lines or for specific registered lines.

Enabling this parameter enables the phone to play network-provided media or its own media as a ringback tone.

**Procedure**

- » Do one of the following:
  - Enable the phone to support p-early-media on all outgoing calls.

```
voIpProt.SIP.header.pEarlyMedia.support="1"
```

- Enable the p-early-media header on a registered line. Replace *x* with the registered line number.

```
reg.x.header.pearlymedia.support="1"
```

## Remove the Outbound Proxy Address from the Route Header

Prevent the phone from including the outbound proxy address as the topmost route header on a registered line.

### Procedure

- » Remove the outbound proxy address in the route header. Replace x with the registered line number.

```
reg.x.insertOBPAddressInRoute="0"
```

## Add Path Extension Header to Request Message

Provide the path extension header field in the Register request message for a specific line registration.

### Procedure

- » Support and include the path extension header field in the Register request message for a registered line. Replace x with the registered line number.

```
reg.x.path="1"
```

## Subscribe to Registered Line State Change Notifications

Enable the phone to accept state change notifications for all lines or for specific registered lines.

### Procedure

- » Do one of the following:
  - Subscribe the phone to state change notifications for all lines.

---

**Note:** The `reg.x.regevent` parameter overrides this setting for the registered line it's configured for.

---

```
voIpProt.SIP.regevent="1"
```

- Subscribe the phone to state change notifications for a registered line. Replace x with the registered line number.

---

**Note:** Setting this parameter overrides the setting in the `voIpProt.SIP.regevent` global parameter for the registered line.

---

```
reg.x.regevent="1"
```



## Reject Calls with Network Determined User Busy Events

The phone can reject incoming calls if it detects a Network Determined User Busy (NDUB) event on all lines or on specific registered lines.

If an NDUB event occurs on any registered lines, the phone rejects the call with a 603 *Decline* response code.

### Procedure

» Do one of the following:

- Reject calls when the phone detects an NDUB event on all lines.

```
voIpProt.SIP.rejectNDUBInvite="1"
```

- Reject calls when the phone detects an NDUB event on a registered line. Replace x with the registered line number.

```
reg.x.rejectNDUBInvite="1"
```

## Enable Server-Specific Features

Configure the phone to work with server-specific features on registered lines.

The phone supports the following features:

- Standard (default)
- GENBAND
- ALU-CTS
- ocs2007r2
- lcs2005

### Procedure

» Enable server-specific features on registered on a registered line. Replace x with the desired line key value. Replace y with the desired server key value.

```
reg.x.server.y.specialInterop="<feature>"
```

## Include Service Route Information in VQMon Messages

Include service route information in the voice quality monitoring (VQMon) messages it creates.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

» Enable the phone to include service route information in VQMon messages.

```
voice.qualityMonitoring.processServiceRoute.enable="1"
```

## Enable Support for the 199 Response Code

Enable the phone to support the 199 response code. For information on the 199 response code, see [RFC 6228](#).

### Procedure

- » Enable support for the 199 response code.

```
voIpProt.SIP.supportFor199="1"
```

## Enable Advice of Charge

In an IP multimedia subsystem (IMS) environment, Poly phones support the Advice of Charge (AoC) feature as defined in Technical Specification (TS) [24.647 version 9.1.0 Release 9](#).

```
Set:voIpProt.SIP.IMS.enable="1".
```

Enable Poly phones to display call charges information, which include the following:

- Call setup charge and call tariff information - Displayed at the beginning of a call.
- Cumulative call cost - Displayed on an ongoing call.
- Complete call cost - Displayed after a call ends.

### Procedure

1. Display call charge information on the phone.

```
voIpProt.SIP.aoc.enable="1"
```

2. Optional: Enable the phone to sound a beep when call charges update on the display.

```
feature.adviceOfCharge.allowAudioNotification="1"
```

## Enable and Configure TWAMP

UC Software supports Two-Way Active Measurement Protocol (TWAMP), based on [RFC 5357](#). Enable and configure TWAMP to review packet loss and latency between endpoints.

TWAMP defines a control protocol that uses TCP and a test protocol that uses UDP. TWAMP includes the following limitations:

- TWAMP control and test protocols only support unauthenticated mode.
- A maximum of 10 clients can establish a connection with the server.
- The server handles a maximum of 10 sessions per client.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Enable TWAMP.

```
feature.twamp.enabled="1"
```

2. Set the TWAMP max port range end. The default is 60000. The value range is 1024 to 65486.

```
twamp.port.udp.PortRangeEnd="<Max port range end>"
```

3. Set the TWAMP port range start. The default is 4000. The value range is 1024 to 65485.

```
twamp.port.udp.PortRangeStart="<Port range start>"
```

4. Set the maximum TWAMP sessions that can run simultaneously. The default is 1. The value range is 1 to 10.

```
twamp.udp.maxSession="<Max number of simultaneous sessions>"
```

## Technical Report-069

Technical Report-069 (TR-069) enables you to remotely manage end-user devices.

As a bidirectional SOAP/HTTP-based protocol, TR-069 enables secure communication between auto configuration servers (ACS) and Poly phones. Using TR-069, you can remotely configure and manage Poly phones by provisioning systems that comply with TR-069 technical specification. Configure the TR-069 feature through the system web interface or using configuration parameters on a central provisioning server.

You can configure Poly phones with an ACS server, including username and password, using DHCP option 43 for IPv4. Poly CCX business media phones don't support IPv6.

### Configure TR-069 in the System Web Interface

Configure TR-069 from the system web interface.

**Procedure**

1. In the system web interface, go to **Settings > Provisioning Server > TR-069 Menu**.
2. Select **Enable**.
3. Enter the values as needed in the provided fields.
  - ACS URL
  - ACS Username
  - ACS Password
  - CPE Username
  - CPE Password
  - Periodic Inform
  - Inform Interval
  - Managed Upgrades
4. Select **Save**.

## Enable and Configure TR-069 Using a Configuration File

Configure TR-069 using configuration parameters.

Poly provides parameters for the TR-104 and TR-106 data models that support provisioning of TR-069-enabled devices by an auto configuration server (ACS). TR-104 is a parameter data model for VoIP-only devices, and TR-106 is a parameter data model for all TR-069-enabled devices.

### Procedure

1. Enable TR-069.

```
device.feature.tr069.enabled="1"
```

2. Enable `device.set` for the TR-069 feature.

```
device.feature.tr069.enabled.set="1"
```

3. Enter the TR-069 ACS server URL.

```
device.tr069.acs.url="<valid URL>"
```

4. Enter the TR-069 username and password to authenticate the phone.

```
device.tr069.acs.username="<username>"
device.tr069.acs.password="<password>"
```

5. Enter the username and password to authenticate a connection request from the ACS server.

```
device.tr069.cpe.username="<username>"
device.tr069.cpe.password="<password>"
```

## TR-106 Parameters Mapped to Poly Parameters

The data model TR-106 defines the TR-069 ACS parameter details.

The following tables list the TR-106 parameters and their corresponding Poly parameters.

**Note:** The parameters listed as "Internal Value" don't map directly to a configuration parameter on the phone and the phone generates these values dynamically to provide to the ACS server.

### Device and Device.DeviceInfo

TR-106 ACS parameter names	Poly Parameter	Writable
Manufacturer	Internal Value	No
ManufacturerOUI	Internal Value	No
ModelName	Internal Value	No
ProductClass	Internal Value	No
SerialNumber	Internal Value	No
HardwareVersion	Internal Value	No

TR-106 ACS parameter names	Poly Parameter	Writable
SoftwareVersion	Internal Value	No
UpTime	Internal Value	No

**Device.ManagementServer**

TR-106 ACS parameter names	Poly Parameter	Writable
URL	device.tr069.acs.url	Yes
Username	device.tr069.acs.username	Yes
Password	device.tr069.acs.password	Yes
PeriodicInformEnable	device.tr069.periodicInform.enabled	Yes
PeriodicInformInterval	device.tr069.periodicInform.interval	Yes
ConnectionRequestURL	Internal Value	No
ConnectionRequestUsername	device.tr069.cpe.username	Yes
ConnectionRequestPassword	device.tr069.cpe.password	Yes
UpgradesManaged	device.tr069.upgradesManaged.enabled	Yes
STUNServerAddress	tcpIpApp.ice.stun.server	Yes
STUNServerPort	tcpIpApp.ice.stun.udpPort	Yes
STUNUsername	tcpIpApp.ice.username	Yes
STUNPassword	tcpIpApp.ice.password	Yes

**Device.LAN**

TR-106 ACS parameter names	Poly Parameter	Writable
IPAddress	Internal Value	No
SubnetMask	Internal Value	No
DNSServers	Internal Value	No
MACAddress	Internal Value	No
MACAddressOverride	Internal Value	No

**TR-104 Parameters Mapped to Poly Parameters**

The data model TR-104 defines the TR-069 ACS parameter details.

The following tables list the TR-104 parameters and their corresponding Poly parameters.

**Note:** The parameters listed as "Internal Value" don't map directly to a configuration parameter on the phone and the phone generates these values dynamically to provide to the ACS server.

#### VoiceService.{i}.VoiceProfile.{i}

TR-104 ACS parameter names	Poly Parameters	Writable
DigitMap	dialplan.digitmap	Yes

#### VoiceService.{i}.VoiceProfile.{i}.SIP

TR-104 ACS parameter names	Poly Parameters	Writable
RegistrarServer	voIpProt.server.X.address	Yes
RegistrarServerPort	voIpProt.server.X.port	Yes
OutboundProxy	voIpProt.SIP.outboundProxy.address	Yes
OutboundProxyPort	voIpProt.SIP.outboundProxy.port	Yes
RegisterExpires	voIpProt.server.X.expires	Yes
RegistersMinExpires	voIpProt.server.X.expires.overlap	Yes
RegisterRetryInterval	voIpProt.server.X.retryTimeOut	Yes

#### VoiceService.{i}.VoiceProfile.{i}.SIP.EventSubscribe.{i}

TR-104 ACS parameter names	Poly Parameters	Writable
ExpireTime	voIpProt.server.X.subscribe.expires	Yes

#### VoiceService.{i}.VoiceProfile.{i}.RTP

TR-104 ACS parameter names	Poly Parameters	Writable
LocalPortMin	tcpIpApp.port.rtp.mediaPortRangeStart	Yes
LocalPortMax	tcpIpApp.port.rtp.mediaPortRangeEnd	Yes

#### VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP

TR-104 ACS parameter names	Poly Parameters	Writable
Enable	sec.srtp.enable	Yes

**VoiceService.{i}.VoiceProfile.{i}.ButtonMap.Button.{i}**

TR-104 ACS parameter names	Poly Parameters	Writable
ButtonName	softkey.X.label	Yes
FacilityAction	softkey.X.action	Yes
UserAccess	softkey.X.enable	Yes

**VoiceService.{i}.VoiceProfile.{i}.Line.{i}**

TR-104 ACS parameter names	Poly Parameters	Writable
DirectoryNumber	reg.X.address	Yes

**VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP**

TR-104 ACS parameter names	Poly Parameters	Writable
AuthUserName	reg.X.auth.userId	Yes
AuthPassword	reg.X.auth.password	Yes

**VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures**

TR-104 ACS parameter names	Poly Parameters	Writable
CallForwardUnconditionalEnable	reg.X.fwdStatus	Yes
CallForwardUnconditionalNumber	reg.X.fwdContact	Yes
CallForwardOnBusyEnable	reg.X.fwd.busy.status	Yes
CallForwardOnBusyNumber	reg.X.fwd.busy.contact	Yes
CallForwardOnNoAnswerEnable	reg.X.fwd.noanswer.status	Yes
CallForwardOnNoAnswerNumber	reg.X.fwd.noanswer.contact	Yes
CallForwardOnNoAnswerRingCount	reg.X.fwd.noanswer.ringCount	Yes
DoNotDisturbEnable	divert.dnd.X.enabled	Yes

## Supported TR-069 Remote Procedure Call (RPC) Methods

The following table lists the supported RPC methods.

**RPC Methods**

RPC Method	Description
GetRPCMethods	Discovers the set of methods supported by the phone.

RPC Method	Description
SetParameterValues	Modifies the value of one or more phone parameters.
GetParameterValues	Obtains the value of one or more phone parameters.
GetParameterNames	Discovers the parameters accessible on a particular phone.
GetParameterAttributes	Reads the attributes associated with one or more phone parameters.
SetParameterAttributes	Modifies attributes associated with one or more phone parameters.
Reboot	Reboots the phone.
Download	Causes the phone to download a specified file from the designated location. Supported file types for download: <ul style="list-style-type: none"> <li>▪ Firmware Image</li> <li>▪ Configuration File</li> </ul>
FactoryReset	Resets the phone to its factory default state.
TransferComplete	Informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	Adds a new instance of an object defined on the phone.
DeleteObject	Removes a particular instance of an object.

## Configure Network Signaling Validation

Specify the validation type, method, and the events for validating incoming network signaling

You can choose from the following for validating incoming signaling:

- Source IP address validation - Only accept SIP traffic from trusted IP addresses.
- Digest authentication - Verifies that both parties on a connection (host and endpoint client) know a shared secret (a password). The phone can use this verification method without sending the password in the clear.
- Both source IP address validation and digest authentication

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Set a signaling validation method.
  - Null (default): No validation is made.



- Source: Ensure request is received from an IP address of a server belonging to the set of target registration servers.
- digest - Challenge requests with digest authentication using the local credentials for the associated registration (line).
- both or all: Apply both of the above methods.

```
voIpProt.SIP.requestValidation.x.method="<value>"
```

**2. Set the SIP requests in which validation will be applied.**

- Null (default).
- INVITE
- ACK
- BYE
- REGISTER
- CANCEL
- OPTIONS
- INFO
- MESSAGE
- SUBSCRIBE
- NOTIFY
- REFER
- PRACK
- UPDATE

```
voIpProt.SIP.requestValidation.x.request="<value>"
```

**3. Set which events specified with the Event header should be validated**

- Null (default): all events will be validated.
- A valid string - specified event will be validated

```
voIpProt.SIP.requestValidation.x.request.y.event="<value>"
```

This is applicable only when `voIpProt.SIP.requestValidation.x.request` is SUBSCRIBE or NOTIFY

## Jitter Buffer and Packet Error Concealment

Jitter buffer mitigates packet interarrival jitter and out-of-order, lost, or delayed (by the network) packets. You can configure jitter buffer for wired network voice traffic and IP multicast voice traffic.

You can adapt and configure jitter buffer for different network environments. When the audio stream loses packets, a concealment algorithm minimizes negative audio consequences. This feature is enabled by default.

For a list of configurable parameters, see "Voice Jitter Buffer Parameters" in the *Poly CCX Parameter Reference Guide*.

## Configure Jitter Buffer for Wired Network Voice Traffic

Configure jitter buffer for wired network voice traffic.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

Jitter above the average but below the maximum may result in delayed audio while the jitter buffer adapts. The audio stream doesn't lose packets. Actual jitter above the maximum value always results in packet loss. If you specify legacy `voice.audioProfile.x.jitterBuffer.*` parameters, they configure the jitter buffer and the phone ignores the `voice.rxQoS.*` parameters.

### Procedure

1. Enter an average jitter setting in milliseconds. The default setting is 20. The range of values is 0 to 80.

The average jitter in milliseconds for wired network interface voice traffic.

```
voice.rxQoS.avgJitter=<value>
```

2. Configure the maximum jitter in milliseconds. The default setting is 240. The range of values is 0 to 320.

The wired interface minimum depth adaptively handles this level of continuous jitter without packet loss.

```
voice.rxQoS.maxJitter=<value>
```

## Configure Jitter Buffer for IP Multicast Voice Traffic

Configure jitter buffer for push-to-talk interface voice traffic.

The PTT/paging interface jitter buffer maximum depth is automatically configured to handle this level of intermittent jitter without packet loss.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets are lost. Actual jitter above the maximum value always results in packet loss.

If legacy `voice.audioProfile.x.jitterBuffer.*` parameters are explicitly specified, they will be used to configure the jitter buffer and these `voice.rxQoS.*` parameters are ignored.

### Procedure

1. Enter an average jitter setting in milliseconds. The default setting is 240.

```
voice.rxQoS.ptt.avgJitter=<0 to 320>
```

2. Enter maximum jitter setting in milliseconds. The default setting is 480.

```
voice.rxQoS.ptt.maxJitter="<2 to 500>"
```

## Set 802.1p/Q Priority

The phone uses IEEE 802.1P and 802.1Q frame tagging protocol for call network traffic. Configure user priority for RTP and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

The phone tags all Ethernet packets it transmits with an 802.1Q VLAN header when the following occurs:

- The phone's network configuration specifies a valid VLAN ID.
- The phone configuration instructs the phone tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- DHCP or LLDP obtains a VLAN ID.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Set the user priority for packets without a per-protocol setting. The default is 2. The value range is 0 to 7.

```
qos.ethernet.other.user_priority="<Generic packet priority>"
```

2. Set the user priority for video RTP packets. The default is 5. The value range is 0 to 7.

```
qos.ethernet.rtp.video.user_priority="<Video RTP packet priority>"
```

3. Set the user priority for voice RTP packets. The default is 5. The value range is 0 to 7.

```
qos.ethernet.rtp.user_priority="<Voice RTP packet priority>"
```

4. Set the user priority for call control packets. The default is 5. The value range is 0 to 7.

```
qos.ethernet.callControl.user_priority="<Call control packet priority>"
```

## Provisional Polling of Phones

You can configure phones to poll the server for provisioning updates automatically, and you can set the phone's automatic provisioning behavior to one of the following:

**Absolute:** The phone polls at the same time every day.

**Relative:** The phone polls every x seconds, where x is a number greater than 3600.

**Random:** The phone polls randomly based on a set time interval.

If the time period is less than or equal to one day, the first poll is at a random time between when the phone starts up and the polling period. Afterward, the phone polls every x seconds.

If you set the polling period greater than one day, and rounded up to the nearest day, the phone polls on a random day based on the phone's MAC address. The phone polls within a random time set by the start and end polling time.

## Configure Polling for Provisioning Updates

Configure your phones to poll the provisioning server for configuration updates.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable automatic polling for updates.

```
prov.polling.enabled="1"
```

2. Set the start time for polling the provisioning server.

The default is 03:00.

```
prov.polling.time="<hh:mm>"
```

3. Set the stop time for polling the provisioning server.

The default is Null.

```
prov.polling.timeRandomEnd="<hh:mm>"
```

4. Set the provisioning polling period, in seconds.

The default is 86400. The integer value must be greater than 3600 seconds.

---

**Note:** The server calculates the polling period in seconds and rounds it up to the nearest number of days in absolute and random mode. If you set this value to a time greater than 86400 (one day), polling occurs on a random day based on the phone's MAC address.

---

```
prov.polling.period="<polling period>"
```

5. Set the provisioning polling mode.

- **abs** (default): Absolute; the phone polls every day at the time specified by `prov.polling.time`.
- **rel**: Relative; the phone polls after the number of seconds specified by `prov.polling.period`.
- **random**: Random; the phone polls at random between a starting time set in `prov.polling.time` and an end time set in `prov.polling.timeRandomEnd`.

---

**Note:** If you set the polling period in `prov.polling.period` to a time greater than 86400 seconds (one day), polling occurs on a random day within that polling period and only between the start and end times. The server calculates the day within the period based upon the phone's MAC address and doesn't change with a reboot. However, the server calculates the time within the start and end times again with every reboot.

---

```
prov.polling.mode="<polling mode>"
```

## Configure Provisional Polling for Multiple Phones at Random Times

If you have multiple phones, you can configure polling to happen at different times for each phone.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Configure one or more phones to randomly poll the provisioning server. The phone polls the server between 1:00 AM and 5:00 AM every day. When you configure multiple phones, the phones randomly poll the server based on their IP Address.

### Procedure

1. Set polling to random.

```
prov.polling.mode="random"
```

2. Set the polling period to 604800 seconds (7 days).

```
prov.polling.period="7200"
```

3. Set the random polling start time to 01:00..

```
prov.polling.time="01:00"
```

4. Set the polling period end time to 05:00.

```
prov.polling.timeRandomEnd="05:00"
```

## Configure SIP Subscription Timers

To improve the interoperability and performance of devices in the network environment, configure SIP subscription timers. You can configure a subscription expiry independently of the registration expiry.

---

**Note:** Per-registration configuration parameters override global parameters. If you don't configure values for any user features, the phone uses the default values.

---

You can also configure the following:

- A subscription expiry independently of the registration expiry
- An overlap period for a subscription independently of the overlap period for the registration

- A subscription expiry and subscription overlap for global SIP servers and per-registration SIP servers

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

## Procedure

1. Set the amount of time, in seconds, after which the phone attempts to resubscribe at the beginning of an overlap period. Replace x with the desired server key value. The default value is 60 seconds (1 minute). The value range is from 5 to 65535.

```
voIpProt.server.x.expires.overlap="<value>"
```

2. Set the number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. Replace x with the desired server key value. The default value is 3600 seconds (1 hour). The value range is 10 to 2147483647.

```
voIpProt.server.x.subscribe.expires="<value>"
```

3. The phone's requested subscription period, in seconds, after which the phone attempts to resubscribe at the beginning of the overlap period. Replace x with the registered line number. Replace y with the desired server key value. The default value is 3600 seconds (1 hour). The value range is 10 to 2147483647.

```
reg.x.server.y.subscribe.expires="<value>"
```

4. Set the amount of time, in seconds, after which the phone attempts to resubscribe at the beginning of an overlap period. Replace x with the registered line number. Replace y with the desired server key value. The default value is 60 (1 minute). The value range is 5 to 65535.

```
reg.x.server.y.subscribe.expires.overlap="<value>"
```

## Configure the SIP Instance Identification Settings

Configure the SIP instance to identify individual phones instead of using IP addresses.

If you register multiple phones using the same address of record (AOR), the server identifies the phones using their IP address. However, firewalls set up in these environments can regularly change the IP addresses of phones for security purposes. Enabling `reg.x.gruu` for a line provides a contact address to a specific user agent (UA) instance, which helps to route the request to the UA instance and is required in cases in which the REFER request must be routed to the correct UA instance.

This feature complies with [RFC 3840](#).

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable the phone to send *sip.instance* in the REGISTER request for line 1.

```
reg.1.gruu="1"
```

## Configure SIP Header Warnings

Configure the warning field from a SIP header to display a dialog on the phone, for example, when a call transfer fails due to an invalid extension number.

For a list of supported SIP header warnings, see the [Supported SIP Request Headers](#) article in the Poly Online Support Center Knowledge Base.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Replace x in the parameter with the line you are configuring

**Procedure**

1. Enable the phone to display a dialog with any received SIP warnings in the header.

```
voIpProt.SIP.header.warning.enable="1"
```

2. Specify a list of accepted SIP warning codes to display. Leave Null to enable the phone to accept all warning codes. Note that only codes between 300 and 399 are supported.

Separate multiple codes with a comma.

```
voIpProt.SIP.header.warning.codes.accept="<Code1,Code2,Code3>"
```

## 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.

Type of Service (ToS) and the Differentiated Services Code Point (DSCP) allows specification of a datagram's desired priority and routing through low-delay, high-throughput, or highly-reliable networks.

You can configure the type of service specifically for RTP packets and call control packets, such as SIP signaling packets.

### Enable IP Type-of Service

Type of Service (ToS) and the Differentiated Services Code Point (DSCP) enables specification of a datagram's desired priority and routing through low-delay, high-throughput, or highly-reliable networks.

The IP ToS header consists of four ToS bits and a 3-bit precedence field. DSCP replaces the older ToS specification and uses a 6-bit DSCP in the 8-bit differentiated services field (DS field) in the IP header.

Configure the type of service field RTP and call control packets for Quality of Service (QoS).

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable ToS.

```
qos.ethernet.tcpQosEnabled="1"
```

## Configure IP Type-of-Service for Video

Configure the video-specific IP Type-of-Service parameters.

Ensure that `qos.ip.rtp.video.dscp` is set to NULL. Setting a value in `qos.ip.rtp.video.dscp` overrides other `qos.ip.rtip.video.*` parameters.

When you configure the video ToS parameters, the phone uses the `qos.ip.rtp.*` parameters for audio only.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the reliability bits in the IP ToS field of the IP header used for RTP video.

```
qos.ip.rtp.video.max_reliability="1"
```

2. Enable the throughput bits in the IP ToS field of the IP header used for RTP video.

```
qos.ip.rtp.video.max_throughput="1"
```

3. Enable the min cost bits in the IP ToS field of the IP header used for RTP video.

```
qos.ip.rtp.video.min_cost="1"
```

4. Enable the min delay bits in the IP ToS field of the IP header used for RTP video.

```
qos.ip.rtp.video.min_delay="1"
```

5. Enable the precedence bits in the IP ToS field of the IP header used for RTP video.

```
qos.ip.rtp.video.precedence="1"
```



## SIP Server Registration

After the phone boots up, it registers to all configured servers.

---

**Note:** If you disable `reg.x.server.y.register` for a given server `y`, the phone doesn't register to that server. However, the INVITE fails over to that server if all higher priority servers are down.

---

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, presence, and BLF are established only with Server 1.

When the registration timer of each server registration expires, the phone attempts to reregister. If this is unsuccessful, normal SIP reregistration behavior (typically at intervals of 30 to 60 seconds) proceeds and continues until the registration is successful (for example, when the internet link is again operational).

While the primary server registration is unavailable, the next highest priority server in the list serves as the working server. As soon as the primary server registration succeeds, it returns to being the working server.

## Configure VoIP Server DHCP Settings

Configure how the phone reacts to DHCP changes.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the phone to check the DHCP server for an IP address.

```
voIpProt.server.dhcp.available="1"
```

2. Set the DHCP option.

The default is 128. The value ranges are 128 to 254.

---

**Note:** If `reg.x.server.y.address` contains a value, it takes precedence even if a DHCP server is available.

---

```
voIpProt.server.dhcp.option="<value>"
```

3. If you want the phone to request a string, set the type to 1. Otherwise, the phone requests an IP address.
  - 0 (default) - Request IP address
  - 1 - Request string

```
voIpProt.server.dhcp.type="1"
```

4. If you want the outbound proxy address to be a string, set the type to 1. Otherwise, the outbound proxy requests an IP address.
  - 0 (default) - IP address
  - 1 - String

```
voIpProt.OBP.dhcpv4.type="1"
```

5. Set the outbound proxy option for DHCPv4.  
The default is 120. The value range is 120 to 254.

```
voIpProt.OBP.dhcpv4.option="<value>"
```

6. Define the outbound proxy option for DHCPv6.  
The default is 21. The value range is 0 to 254.

```
voIpProt.OBP.dhcpv6.option="<value>"
```

## SIP Signaling Failure for Outgoing Calls

At the start of a call, SIP signaling failure determines server availability.

---

**Caution:** If the phone uses DNS to resolve the address for servers, the phone attempts to contact the DNS server to resolve the address of all servers in its list before initiating a call. This may happen due to the DNS server being unavailable or because the TTL for the DNS records has expired. These attempts time out, but the timeout mechanism can cause long delays (for example, 2 minutes) before the phone call proceeds using the working server. To prevent this issue, use long TTLs. Poly recommends deploying an on-site DNS server as part of the redundancy solution.

---

SIP signaling failure depends on the SIP protocol you use.

- If the phone uses TCP, then the signaling fails if the connection fails or the Send fails.
- If the phone uses UDP, then the signaling fails if it detects ICMP or if the signal times out.

If the phone attempts signaling 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 isn't the last server in the list, the phone uses the maximum number of retries using the configurable retry timeout.

- When the user initiates a call, the phone completes the following steps to connect the call:
  1. The phone tries to call the working server.
  2. If the working server doesn't respond correctly to the INVITE, the phone tries the next server in the list. The phone tries even if there's no current registration with these servers. This can happen if the internet connection goes down but the registration to the working server isn't yet expired.
  3. If the second server is also unavailable, the phone tries 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 fails.

## Static DNS Cache

Configure a set of static DNS NAPTR SRV or A records in the phone. You can enter a maximum of 12 record entries for DNS-A, DNS-NAPTR, and DNS-SRV records.

Note the following when configuring the static DNS cache:

- The phone makes an initial attempt to resolve a host name that is within the static DNS cache. For example, the phone makes a query to the DNS if the phone registers to its SIP registrar.
- If the initial DNS query returns no results for the host name or if the phone can't contact it, then the phone uses the values in the static cache for the configured time interval.
- After the configured time interval elapses, a resolution attempt of the host name again results in a query to the DNS.
- If a DNS query for a host name that is in the static cache returns a result, the phone uses the values from the DNS and ignores the statically cached values.

You can't always configure the DNS cache to take advantage of failover redundancy. Use failover redundancy only when the configured IP server host name resolves (through an SRV or A record) to multiple IP addresses. Support for negative DNS caching enables faster failover when prior DNS queries return no results from the DNS server. For more information, see [RFC 2308](#).

## Configure the SIP Server

Configure the SIP server settings to use for the static DNS cache.

Note the following when you configure the static DNS cache:

- The phone makes an initial attempt to resolve a host name that is within the static DNS cache. For example, the phone makes a query to the DNS if the phone registers to its SIP registrar.
- If the initial DNS query returns no results for the host name or if the phone can't contact it, then the phone uses the values in the static cache for the configured time interval.
- After the configured time interval elapses, a resolution attempt of the host name again results in a query to the DNS.
- If a DNS query for a host name that is in the static cache returns a result, the phone uses the values from the DNS and ignores the statically cached values.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Specify the call server used for this registration. Replace x with the desired line key value. Replace y with the desired server key value. The default is Null. The maximum string length is 255 characters.

```
reg.x.server.y="<string>"
```

2. Specify the user or the user and host part of the registration SIP URI or the H.323 ID/extension. Replace x with the desired line key value.

The default is Null.

```
reg.x.address="<string>"
```

3. Specify the SIP server that accepts registrations. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

The default is Null.

---

**Note:** If you set this parameter, it takes precedence even if the DHCP server is available. All the parameters you configure in this list override the parameters specified in `voIpProt.server.*`.

---

```
reg.x.server.y.address="<string>"
```

4. Set the SIP server port that doesn't specify registrations.

The default is Null. The value range is 0 to 65535.

---

**Note:** If you set this parameter to 0, the port used depends on the value you set in `reg.x.server.y.transport`.

---

```
reg.x.server.y.port="<value>"
```

5. Set the transport method the phone uses to communicate with the SIP server.
  - **DNSnaptr (Default)** - If `reg.x.server.y.address` is a hostname and `reg.x.server.y.port` is 0 or Null, the phone does NAPTR then SRV lookups to try to discover the transport, ports and servers (as per RFC 3263).  
If `reg.x.server.y.address` is an IP address or if you provide a port for `reg.x.server.y.port`, then the phone uses UDP.
  - **TCPpreferred** - The phone prefers TCP as the transport but uses UDP if TCP fails.
  - **UDPOnly** - The phone uses only UDP.
  - **TLS** - If TLS fails, transport fails. Leave the port field empty (defaults to 5061) or set to 5061.
  - **TCPOnly** - The phone uses only TCP.

```
reg.x.server.y.transport="<value>"
```

## Configure the Static DNS Cache with A Record IP Addresses

Configure the static DNS cache with A record IP addresses in the SIP server address fields.

Configure the SIP server information.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Configure the DNS cache IPv4 address. Replace *y* with the desired server key value.

The default is Null.

```
dns.cache.A.y.address="<string>"
```

2. Configure the DNS cache hostname. Replace y with the desired server key value.

The default is Null.

```
dns.cache.A.y.name="<string>"
```

3. Set the time period, in seconds, the phone uses the static cache record. Replace y with the desired server key value.

The default is 300. The value range is 300 to 536870912.

If a dynamic network request receives no response, this timer begins on first access of the static record. Once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry, and it resets TTL timer again.

```
dns.cache.A.y.ttl="<value>"
```

## Configure the Static DNS Cache with NAPTR and SRV Records

Configure static DNS cache where your DNS provides NAPTR and SRV records.

Configure the SIP server information.

The following configuration causes the phone to build an SRV request based on the address you provide, including all subdomains:

- `voIpProt.SIP.outboundProxy.address="<string>"`
- `voIpProt.SIP.outboundProxy.port="0"`

This SRV request produces a list of servers ordered by weight and priority, enabling you to specify subdomains for separate servers, or you can create partitions of the same system. Note that while making SRV queries and transport is configured as TCP, the phone adds the prefix `<service.proto.>` to the configured address/FQDN but doesn't remove the subdomain prefix. The phone can resolve a single SRV query to many different servers, session border controllers (SBCs), or partitions ordered by weight and priority.

Alternatively, use DNS NAPTR to discover that services that are available at the root domain.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Configure the DNS cache NAPTR parameters. Replace y with the desired server key value.

```
dns.cache.NAPTR.y.name="<string>"
dns.cache.NAPTR.y.ttl="<value>"
dns.cache.NAPTR.y.order="<value>"
dns.cache.NAPTR.y.preference="<value>"
dns.cache.NAPTR.y.flag="<value>"
dns.cache.NAPTR.y.service="<value>"
```

```
dns.cache.NAPTR.y.regexp="<value>"
dns.cache.NAPTR.y.replacement="<string>"
```

2. Configure the DNS cache parameters. Replace y with the desired server key value.

```
dns.cache.SRV.y.name="<string>"
dns.cache.SRV.y.ttl="<value>"
dns.cache.SRV.y.priority="<value>"
dns.cache.SRV.y.weight="<value>"
dns.cache.SRV.y.port="<value>"
dns.cache.SRV.y.target="<string>"
```

## DNS SIP Server Name Resolution

If a DNS name is given for a proxy/registrar address, the IP addresses associated with that name is discovered as specified in [RFC 3263](#).

If a port is given, the only lookup is an A record. If no port is given, NAPTR and SRV records are 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, port 5060 is used. If the registration type is TLS, port 5061 is used.

---

**Caution:** Failure to resolve a DNS name is treated as signaling failure that causes a failover.

---

The following configuration causes the phone to build an SRV request based on the address you provide, including all subdomains.

Use the format:

- `voIpProt.SIP.outboundProxy.address="sip.example.com"`
- `voIpProt.SIP.outboundProxy.port="0"`

This SRV request produces a list of servers ordered by weight and priority, enabling you to specify subdomains for separate servers, or you can create partitions of the same system. Please note that while making SRV queries and transport is configured as TCP, the phone adds the prefix `< service.proto.>` to the configured address/FQDN but doesn't remove the sub-domain prefix, for example `sip.example.com` becomes `_sip._tcp.sip.example.com`. A single SRV query can be resolved into many different servers, session border controllers (SBCs), or partitions ordered by weight and priority, for example, `voice.sip.example.com` and `video.sip.example.com`. Alternatively, use DNS NAPTR to discover what services are available at the root domain.

## For Outgoing Calls (INVITE Fallback)

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.

---

**Caution:** 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 phone attempts to contact the DNS server to resolve the address of all servers in its list before initiating a call. These attempts timeout, but the timeout mechanism can cause long delays (for example, two minutes) before the phone call proceeds using the working server. To prevent this issue, long TTLs should be used. Poly recommends deploying an on-site DNS server as part of the redundancy solution.

---

When the user initiates a call, the phone completes the following steps to connect the call:

1. The phone tries to call the working server.
2. If the working server does not respond correctly to the INVITE, the phone tries and makes 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 phone tries 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 fails.

## Customer Phone Configuration

The phones at the customer site are configured as follows:

- Server 1 (the primary server) is configured with the address of the service provider call server. The IP address of the server(s) is provided by the DNS server, for example: `reg.1.server.1.address=voipserver.serviceprovider.com`.
- Server 2 (the fallback server) is 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`.

---

**Caution:** Be careful when using multiple servers per registration. It is possible to configure the phone for more than two servers per registration but ensure that the phone and network load generated by registration refresh of multiple registrations does not become excessive. This is of particular concern when a phone has multiple registrations with multiple servers per registration and some of these servers are unavailable.

---

## Server Redundancy

VoIP deployments often require server redundancy. Server redundancy ensures phone high availability in the event that the phone loses connection to the server.

Poly phones support failover and fallback server redundancy. In some cases, you can deploy a combination of the two server redundancy types. Consult your SIP server provider for recommended methods of configuring phones and servers for failover configuration.

---

**Note:** The default value of the parameters

`reg.x.server.y.failOver.concurrentRegistration` and `voIpProt.server.y.failOver.concurrentRegistration` is 0 for Poly devices. Use the `y` variable for redundant failover servers. If you want to register the server concurrently with other servers, set `reg.x.server.y.failOver.concurrentRegistration="1"` or `voIpProt.server.y.failOver.concurrentRegistration="1"`.

---

**Note:** The concurrent failover/fallback feature isn't compatible with Microsoft environments.

---

For more information, see *Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Phones* and *Technical Bulletin 66546: Configuring Optional Re-Registration on Failover Behavior*.

## Configuring Server Redundancy for a Registered Line

Configure a fallback server for a registered line on your phones.

### Procedure

1. Set the phone to send a SIP request to the server that sent proxy authentication request in the event of a failover. Replace `x` with the desired line key value.

```
reg.x.auth.optimizedInFailover="1"
```

2. Configure the mode for failover fallback. Replace `x` with the desired line key value.
- 

**Note:** This setting overrides the configuration for `reg.x.server.y.failOver.failBack.mode`.

---

Set one of the following values:

- `duration` (default) - The phone tries the primary server again after the time specified by `reg.x.outboundProxy.failOver.failBack.timeout` expires.
- `newRequests` - All new requests are forwarded first to the primary server regardless of the last used server.
- `DNSTTL` - The phone tries the primary server again after a timeout equal to the DNS TTL you configured for the server the phone is registered to.

```
reg.x.outboundProxy.failOver.failBack.mode="<value>"
```

3. Configure the time to wait, in seconds before fallback occurs. Replace `x` with the desired line key value.
- 

**Note:** This setting overrides the configuration for `reg.x.server.y.failOver.failBack.timeout`.

---

The default is 3600. The value range is 0 (no timeout), and 60 to 65535.

```
reg.x.outboundProxy.failOver.failBack.timeout="<value>"
```



4. Enable the global and per-line `reRegisterOn` parameter. The existing registrations remain active. Replace `x` with the desired line key value.

```
reg.x.outboundProxy.failOver.failRegistrationOn="0"
```

5. Enable the global and per-line `reRegisterOn` and `failRegistrationOn` parameters. Signaling is accepted from and sent to a server that has failed. Replace `x` with the desired line key value.

```
reg.x.outboundProxy.failOver.onlySignalWithRegistered="0"
```

6. Configure the phone to attempt to register with (or via, for the outbound proxy scenario), the secondary server. Replace `x` with the desired line key value.

---

**Note:** This parameter overrides `reg.x.server.y.failOver.reRegisterOn`.

---

```
reg.x.outboundProxy.failOver.reRegisterOn="1"
```

7. Configure the SIP server port to which the phone sends all requests. Replace `x` with the desired line key value.

The default is 0. The value range is 65535

```
reg.x.outboundProxy.port="<value>"
```

8. Configure the transport method the phone uses to communicate with the SIP server. Replace `x` with the desired line key value.

- DNSNaptr (default)
- TCPpreferred
- UDPOnly
- TLS
- TCPOnly

```
reg.x.outboundProxy.transport="<value>"
```

## Configure Server Redundancy for VoIP

Configure a failback server for a VoIP registered line on your phones.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

In the following parameters, `x` refers to the line you're configuring.

### Procedure

1. Set the server to register concurrently with other servers.

```
voIpProt.server.y.failOver.concurrentRegistration="1"
```

2. Set the failback mode to set a timeout

```
voIpProt.server.x.failOver.failBack.mode="duration"
```

3. Enter a time, in seconds, for the server to attempt to connect to the primary servers after a failback.

The default is 3600. The value range is 0, 60 to 35535.

```
voIpProt.server.x.failOver.failBack.timeout="<60 to 65535>"
```

4. Set how the server fails over.

- 1 (default) - When set to 1, and the global or per-line `reRegisterOn` parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over.
- 0 - When set to 0, and the global or per-line `reRegisterOn` parameter is enabled, existing registrations remain active. This means that the phone attempts failback without first attempting to register with the primary server to determine if it has recovered.

```
voIpProt.server.x.failOver.failRegistrationOn="value"
```

5. Set how the server signals a fail over.

- 1 (default) - When set to 1, and the global or per-line `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 phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server.
- 0 - When set to 0, and the global or per-line `reRegisterOn` and `failRegistrationOn` parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).

```
voIpProt.server.x.failOver.onlySignalWithRegistered="value"
```

6. Set which server the fail over signal is registered on.

- 0 (default) - When set to 0, the phone won't attempt to register with the second.
- 1 - When set to 1, the phone attempts to register with (or by, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server.

```
voIpProt.server.x.failOver.reRegisterOn="value"
```

## Configure NAT

Configure the NAT settings for your phone.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

## Procedure

1. Specify the IP address to advertise within SIP signaling. The IP address must match the external IP address used by the NAT device.

```
nat.ip="<IP-Address>"
```

2. Specify the keep-alive interval, in seconds.  
The default is 0. The value range is 0 to 3600.

```
nat.keepalive.interval="<value>"
```

3. Set the initially allocated RTP port.  
The default is 0. The value range is 0 to 65440.

---

**Note:** This parameter overrides the `tcpIpApp.port.rtp.mediaPortRangeStart` parameter.

---

```
nat.mediaPortStart="<value>"
```

4. Set the port used for SIP signaling.  
The default is 0. The value range is 0 to 65535.

---

**Note:** This parameter overrides the `voIpProt.local.port` parameter.

---

```
nat.signalPort="<value>"
```

## Real-Time Transport Protocol

Configure Real-Time Transport Protocol (RTP) for VoIP media on your device.

You can configure RTP ports for your environment in the following ways:

- Filter incoming packets by IP address or port.
- Reject packets arriving from a non-negotiated IP address, an unauthorized source, or non-negotiated port for greater security.
- Enforce symmetric port operation for RTP packets. When you don't set the source port to the negotiated remote sink port, the phone rejects arriving packets.
- Fix the phone's destination transport port to a specified value, regardless of the negotiated port.

This is useful for communicating through firewalls. When you use a fixed transport port, all RTP traffic sends to and arrives on that specified port. Incoming packets are sorted by the source IP address and port, which enables the phone to multiplex multiple RTP streams.

- Specify the phone's RTP port range. The phone supports conferencing and multiple RTP streams, and it can use several ports concurrently.

As specified in [RFC 1889](#), [RFC 3550](#), and [RFC 3551](#), the next-highest odd-numbered port sends and receives RTP.

## Configure SIP RTP for FECC

Configure the SIP RTP settings for far end camera control (FECC).

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable the FECC port range configuration for OpenSIP registrations.

```
tcpIpApp.port.rtp.feccPortRange.enable="1"
```

2. Specify the FECC port range start port for OpenSIP registrations.

The default is 2372. The value range is 1024 to 65486.

```
tcpIpApp.por.rtp.feccPortRangeStart="<value>"
```

3. Specify the FECC port range end port for OpenSIP registrations.

The default is 2419. The value range is 1024 to 65486.

```
tcpIpApp.port.rtp.feccPortRangeEnd="<value>"
```

## Configure RTP Media Ports

Configure the RTP media ports.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Set the maximum supported end range for the audio ports.

The default is 2269. The value range is 1024 to 65535.

**Important:** Each call increments the port number +2 to a maximum of 24 calls after the value resets to the starting point. Because port 5060 is used for SIP signaling, ensure that port 5060 is not within this range when you set this parameter. A call that attempts to use port 5060 has no audio.

```
tcpIpApp.port.rtp.mediaPortRangeEnd="<value>"
```

2. Set the starting port for RTP port range packets.

The default is 2222. The value range is 1024 to 65436.

```
tcpIpApp.port.rtp.mediaPortRangeStart1="<value>"
```

## Configure RTP Video Ports

Select a specific port range for RTP video ports.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable RTP video ports.

```
tcpIpApp.port.rtp.videoPortRange.enable="1"
```

2. Set the starting range for RTP video ports.

The default is 2272. The value range is 1024 to 65486.

```
tcpIpApp.port.rtp.videoPortRangeStart="<value>"
```

3. Set the maximum supported end range for RTP video ports.

The default is 2319. The value range is 1024 to 65535.

```
tcpIpApp.port.rtp.videoPortRangeEnd="<value>"
```

## Configure STUN Settings

Configure the phone to act as a STUN client. The phone sends a request to a STUN server to discover the public IP and port(s). You can also configure the phone to send keep-alive messages to refresh NAT bindings.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable STUN.

When you enable `voIpProt.SIP.rport`, the phone adds the received IP address and port in the VIA header while generating response.

```
feature .nat.stun.enabled="1"
```

2. Enter the STUN server IP address.

```
nat.stun.server="<STUN server IP address>"
```

3. Optional: Enter a port number.

```
nat.stun.port="<STUN server port>"
```

4. Optional: Enable NAT traversal mode with STUN signaling for a particular line.

In the parameter, replace x with the line number.

```
reg.x.nat.traversal.mode="Auto"
```

## Enable GZIP Encoding

To reduce bandwidth consumption, configure the phone to send notifications to the server in GZIP format.

### Procedure

- » Enable GZIP encoding.

```
voIpProt.SIP.gzipEncoding.enable="1"
```

# Securing the Phones

---

## Topics:

- [Phone Passwords](#)
- [System Web Interface Security Settings](#)
- [Locking the Phone](#)
- [Advanced User Access to Administration Settings](#)
- [Hide the MAC Address](#)
- [Hide the Address of Record](#)
- [Certificates](#)
- [Encryption](#)
- [Web Proxy](#)
- [Disable Unused External Ports](#)
- [Enable Voice over Secure IP](#)
- [Enable and Configure 802.1X Security](#)
- [Enable FIPS 140-2 Encryption](#)

Configure your phones to meet your organization's security requirements.

## Phone Passwords

The default configuration includes administrative- and user-level access through the phone's local interface or the system web interface.

The administrator password grants full access to all configuration settings. The user password grants limited access to basic settings and preferences. The default passwords are:

- Administrator password: 456
- User password: 123

If your phone has UC Software version 6.2.21 and later, it requires you to change the default administrator password to access the phone.

## Configure Password Settings

Configure administrative and user password rules for your phone using a configuration file.

---

**Important:** These settings override any locally set passwords.

---

**Procedure**

1. Set the minimum allowed password character counts for administrative and user passwords.

```
sec.pwd.length.admin="<min password length>"
sec.pwd.length.user="<min password length>"
```

2. Set the administrator and user passwords.

---

**Note:** You can't set the administrator password as the default password: 456.

---

```
device.auth.localAdminPassword.set="1"
device.auth.localAdminPassword="<administrator password string>"
device.auth.localUserPassword.set="1"
device.auth.localUserPassword="<user password string>"
```

**Set the Administrator Password on the Local Interface**

If the phone uses the default administrator password, you can't use the local interface or the system web interface until you change it.

**Procedure**

1. Select **Settings > Advanced**.
2. Enter the default password and select **Enter**.
3. Select **Change Admin Password**.
4. Enter the current password, enter a new password, and confirm the new password.

Passwords can contain uppercase and lowercase letters, numerals, and special characters (!, #, %, \$, etc.).

Passwords cannot contain non-ASCII characters (Ã, ç, ë, etc.) or chevrons (<, >).

**Set the User Password on the Local Interface**

Set the user password at any time from the **Advanced** settings menu.

**Procedure**

1. Select **Settings > Advanced**.
2. Enter the user password and select **Enter**.
3. Select **Change User Password**.
4. On the **Change User Password** screen, enter your old and new user password and select **Enter**.

Passwords can contain uppercase and lowercase letters, numerals, and special characters (!, #, %, \$, etc.).

Passwords cannot contain non-ASCII characters (Ã, ç, ë, etc.) or chevrons (<, >).



## California SB-327 Password Requirement Compliance

Your phone meets the California SB-327 password mandate that requires administrators to generate a new password before granting access to the system and the system web interface.

When you first power on a phone or following a factory reset, the phone requires you to change the default administrator password. You must change the default administrator password to a unique password to access the local interface and system web interface.

---

**Note:** You can't use the default password as the newly generated password.

---

## System Web Interface Security Settings

Configure security settings for the system web interface.

Configure the following options:

- Provide security banners on the login page
- Lock the system web interface after failed login attempts
- Session management rules

### Configure a Security Banner for the System Web Interface

Create a security banner to display on the phone's system web interface before administrators or users log in.

#### Procedure

1. Enable the security banner feature.

```
feature.webSecurityBanner.enabled="1"
```

2. Configure the message to display on the security banner. Enter up to 2000 characters.

```
feature.webSecurityBanner.msg="<security banner message>"
```

### Locking the System Web Interface After Failed Login Attempts

For additional security, the system web interface locks after a certain number of failed attempts within a set period of time.

By default, the system web interface locks the user out after five failed user login attempts within a 60 second period. The system web interface unlocks 60 seconds after the phone locks, and the user can attempt to log in again.

## Configure the System Web Interface Lockout

Configure the system web interface's failed attempt limit, how long users have to enter the correct login information, and how long the system web interface stays locked.

### Procedure

1. Configure the number of allowed failed attempts. You can configure between 3 and 20 attempts.

```
httpd.cfg.lockWebUI.noOfInvalidAttempts="<number of allowed attempts>"
```

2. Configure the period of time, in seconds, that the user can attempt to log in again after the first failed login attempt. If the user fails to log in after the number attempts configured in `httpd.cfg.lockWebUI.noOfInvalidAttempts` during this period, the system web interface locks. Configure between 60 and 300 seconds.

```
httpd.cfg.lockWebUI.noOfInvalidAttemptsDuration="<duration in seconds>"
```

3. Configure how long the system web interface stays locked in seconds. Configure between 60 and 300 seconds.

```
httpd.cfg.lockWebUI.lockOutDuration="<duration in seconds>"
```

## Disable the System Web Interface Lockout

Allow users an unlimited number of failed attempts to log in to the phone's system web interface.

### Procedure

- » Disable the system web interface lockout.

```
httpd.cfg.lockWebUI.enable="0"
```

## Configure Session Management Rules

The phone has preset session management rules, but you can customize the rules as needed.

Use session management on the system web interface to enhance phone security by setting the maximum number of sessions and determining session validity.

By default, the phone allows 10 concurrent sessions on the system web interface. The phone allows a single session to remain idle for 900 seconds (15 minutes) before it automatically ends it.

If you change the password, all the existing sessions expire and you must log in with the new password. If a session reaches the maximum limit, all existing sessions expire and the new session continues on the system web interface. If you can't log in to the system web interface, clear your web browser cookies and try again.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Set the duration of a single session in the idle state, in seconds. Configure from 60 to 86,400 seconds. The default is 900 seconds.

```
httpd.cfg.session.maxSessionAge="<session duration>"
```

2. Set the maximum number of concurrent sessions the phone allows. Configure from 1 to 20 concurrent sessions. The phone allows 10 concurrent sessions by default.

```
httpd.cfg.session.maxSessions="<concurrent session max>"
```

## Locking the Phone

Enable users to lock their phones to prevent unauthorized access to phone features such as placing calls, accessing menus, or viewing directories.

If configured, users can call emergency or authorized numbers from a locked phone. You can configure the list of authorized numbers.

---

**Note:** If a locked phone has a registered shared line, calls to the shared line display on the locked phone, and the phone's user can answer the call.

---

### Lock the Basic Settings Menu

Lock the **Basic** settings so that the phone requires either the user or administrator password to update phone preferences.

Normally, any phone user can access the **Basic** settings menu without limitations. The **Basic** settings menu contains phone preference settings such as language, display, and ringer settings.

**Procedure**

- » Enable the password requirement on the **Basic** settings menu.

```
up.basicSettingsPasswordEnabled="1"
```

### Enable Phone Lock

Display the **Lock Phone** menu option in the **Basic** menu.

---

**Important:** Configure this parameter before setting up any other phone lock features.

---

**Procedure**

- » Enable the phone lock feature.

```
phoneLock.enabled="1"
```

## Set an Automatic Phone Lock

Configure the phone to lock itself after a set period of inactivity.

### Procedure

- » Set the amount of idle time before the phone locks automatically.

```
phoneLock.idleTimeout="<number of seconds>"
```

The value ranges from 0 to 65535 seconds. If you set the value to 0, automatic locking is disabled.

## Define Authorized Contacts to Call from a Locked Phone

Define up to five authorized contacts that a user can call from a locked phone. Each contact must have a description to display on the screen and a phone number or address value for the phone to dial.

### Procedure

- » Configure up to five authorized contacts that users can call with a locked phone.

```
phoneLock.authorized.x.description="<Contact Name>"  
phoneLock.authorized.x.value="<Contact's number or address>"
```

Use the same parameters to enable each authorized contact. For the variable *x*, set a number from 1 to 5.

## Enable Do Not Disturb When the Phone Locks

Configure the phone to enter Do Not Disturb (DND) at the same time it locks.

Normally the phone can receive incoming calls even if a user locks it. You can configure the phone to automatically activate DND when the phone locks. This prevents phones from ringing if no one is around to answer them.

### Procedure

- » Configure the phone to activate DND at the same time it locks.

```
phoneLock.dndWhenLocked="1"
```

### Related Links

[Do Not Disturb](#) on page 106

## Remotely Unlock a Phone

Using a configuration file, you can remotely unlock a phone if you can't use either the user or administrative passwords to unlock the phone.

### Procedure

- » Disable the phone lock parameter.

```
phoneLock.enabled="0"
```

## Advanced User Access to Administration Settings

Grant user access to the **Advanced** menu containing a subset of administrator settings.

By default, the **Advanced** menu requires the administrator password to access. When you enable this feature, users can access most of the phone's administrator options using a separate advanced user password.

Users can access all administrator features except the following:

- Line configuration
- Call server configuration
- Test automation

You can also disable access to the network and security settings.

### Enable Advanced User Access

Enable users to access the **Advanced** menu option for the phone.

Set `device.set="1"`.

#### Procedure

1. Enable the **Advanced** settings and display the **Admin** menu in the phone's local interface.

```
feature.advancedUser.enabled="1"
```

2. Configure an advanced user password for the phone. This password grants access to the **Advanced** menu, but it doesn't grant access to the **Admin** menu. This parameter setting overrides the locally set advanced user password.

```
sec.pwd.length.advanced="<min password length>"
device.auth.localAdvancedPassword.set="1"
device.auth.localAdvancedPassword="<advanced password string>"
```

3. Optional: Enable the advanced user login for the system web interface.

```
feature.advancedUser.web.enabled="1"
```

### Disable Advanced User Access to Network Settings

Prevent advanced users from accessing network settings in the phone's system web interface.

---

**Note:** Don't disable this parameter if you want to only disable advanced user access to TLS security options.

---

#### Procedure

- » Remove the **Network** option under **Settings** in the system web interface.

```
ui.menu.advancedUser.networkConfiguration="0"
```

## Disable Advanced User Access to TLS Security

Enable advanced users to access networking options in the system web interface while preventing access to TLS security options.

### Procedure

- » Remove the **TLS** option under **Settings > Network** in the system web interface.

```
ui.menu.advancedUser.networkConfiguration.tls="0"
```

## Hide the MAC Address

Configure the phone to hide MAC address on the phone's display. When you enable this feature, users can't view or retrieve the MAC address from the phone. Only administrators can view or retrieve the MAC address.

Set `device.set="1"`.

### Procedure

- » Hide the MAC address from users.

```
device.mac.hide.set="1"
device.mac.hide="1"
```

## Hide the Address of Record

Configure your phone to hide the address of record (SIP address) for lines on the phone. The `reg.x.address` defines the AOR for the lines registered on the phone. By default, it displays beneath the registered line label in multiple locations on the phone.

### Procedure

- » Hide the address of record for registered lines on the phone's screen.

```
up.secondaryLineLabel="Disabled"
```

## Certificates

Certificates ensure privacy and security while using your phone on your network.

### Using the Factory-Installed Certificate

Poly installs a device certificate unique to the device based on the phone's MAC address during manufacture. Because the certificate is factory installed, it's the easiest option for out-of-box activities, especially phone provisioning.

The certificate, signed by the Poly Certificate Authority (CA), is suitable for all security requirements.

View the Certificate Revocation List (CRL)—a list of all expired certificates signed by the Polycom Root CA—at <http://crl.polycom.com/crl>.

---

**Important:** The certificate expires on March 9, 2044.

---

If you enable mutual TLS, you must have a root CA installed (the Polycom Root CA or your organization's CA) on the HTTPS server. See <http://pki.polycom.com/pki> to download the Polycom Root CA. For more information on using mutual TLS with Microsoft Internet Information Services (IIS) 6.0, see *Mutual Transport Layer Security Provisioning Using Microsoft Internet Information Services 6.0: Technical Bulletin 52609* at [Poly Engineering Advisories and Technical Notifications](#).

## Creating CSRs

When you create a certificate signing request (CSR), the phone requests a 2048-bit certificate with `sha256WithRSAEncryption` as the signature algorithm by default. You can use OpenSSL or another CSR if you require a stronger certificate.

### Create a CSR on the Local Interface

Generate a CSR for a phone directly from the local interface.

Connect the phone to a provisioning server with full write access.

---

**Note:** Poly phones support Subject Alternative Names (SAN) with TLS security certificates, but they don't support asterisks (\*) or wildcard characters in the **Common Name** field of a Certificate Authority (CA) public certificate. If you want to enter multiple host names or IP addresses on the same certificate, use the **SAN** field.

---

### Procedure

1. Go to **Settings > Advanced > Admin Settings > Generate CSR**.
2. Enter the following information:
  - **Common Name**
  - **Organization** (optional)
  - **Email Address** (optional)
  - **Country** (optional)
  - **State** (optional)
3. Select **Generate**.

A CSR generation completed message displays.

If `sec.uploadDevice.privateKey="1"`, `MAC.csr` (certificate request) and `MAC-private.pem` (private key) files upload to the phone's provisioning server.

4. Forward the CSR to a CA to create a certificate.

If your organization doesn't have its own CA, you must forward the CSR to the third-party security company that hosts your CA.

## Download and Install Certificates

Download and install up to nine CA and eight device certificates onto your phone.

After installing the certificates, you can refresh the certificates when they expire or become revoked. You can delete any CA or device certificate that you install.

---

**Note:** Point the certificate URL to a PKCS #7 file in .pem format with the certificate and key concatenated together.

---

### Procedure

1. Go to **Settings > Advanced > Administrative Settings > TLS Security**.
2. Do one of the following:
  - To install a CA, select **Custom CA Certificates**.
  - [Download and Install Certificates](#) on page 79
  - To install a device certificate, select **Custom Device Certificates**.
3. Select **Install**.
4. Enter the URL where the certificate is stored. Note that the phone can't accept chevrons (<, >) in the URL field.  
`http://server.domain.com/ca.crt`  
 The certificate downloads, and the certificate's MD5 fingerprint displays to verify that you're installing the correct certificate.
5. Select **Accept**.  
 The certificate installs successfully.

## Custom URL Locations for LDAP Server CAs

Set a specific URL on the phone to download the custom root CA certificate or a chain of CAs required to authenticate the LDAP server.

By default, all Poly-installed profiles are associated with the default cipher suite and use trusted and widely recognized CAs for authentication. You can download and install up to seven custom CAs onto a phone. The CAs install in descending order starting with the highest Application CA slot (up to 7) and continues to Application CA 1 slot.

---

**Note:** If the custom application CA slots already have CAs installed, downloading LDAP server CAs overwrites any existing certificates on the phone.

---

### Define the Download URL Location for the LDAP Server CA

Define the location from where the phone downloads LDAP server certificates.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---



**Procedure**

1. Enable the corporate directory feature.

```
feature.corporateDirectory.enabled="1"
```

2. Set the corporate directory address to the LDAP server interface.

```
dir.corp.address="<LDAP server interface address>"
```

3. Set the TLS profile to application profile 1.

```
sec.TLS.profileSelection.LDAP="ApplicationProfile1"
```

4. Define the URL location where the phone can download the LDAP server certificates.

```
sec.TLS.LDAP.customCaCertUrl="<LDAP custom root CA location URL>"
```

**Confirm the Installed LDAP Server Certificates**

After you configure the custom URL location for the LDAP server certificates and provision the phone, confirm that the phone downloaded and installed the correct certificates.

**Procedure**

1. Select **Settings > Advanced**.
2. Go to **Administrative Settings > TLS Security > Custom CA Certificates > Application CA placeholders**.
3. Confirm that phone downloaded and installed the correct certificates.

If the certificates didn't download and install, do the following:

- Make sure that the phone provisioned successfully.
- Make sure you defined the correct server location for the LDAP Server CA.
- Make sure that the phone can access the folder on your network.

**Enable OCSP**

Enable the phone to use the Online Certificate Status Protocol (OCSP) to authenticate X.509 digital certificates.

Set `device.set="1"`.

When a user sends a request to a server, the phone checks whether the certificate is valid or revoked via OCSP. It's an alternative to the phone referencing a certificate revocation list (CRL).

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable the phone to use OCSP.

```
device.sec.TLS.OCSP.enabled.set="1"
device.sec.TLS.OCSP.enabled="1"
```

**Enable and Configure SCEP**

Configure your phones to use a Simple Certificate Enrollment Protocol (SCEP) server for certificate enrollment.

SCEP enables you to automatically and securely provision multiple phones with a digital device certificate. This feature vastly streamlines the certificate enrollment process for a large number of deployed phones.

**Procedure**

1. Enable the SCEP feature.

```
SCEP.enable="1"
```

2. Specify the URL address of the SCEP server accepting requests to obtain a certificate.

```
SCEP.url="<SCEP server address>"
```

3. Specify the username and password to authenticate with the SCEP server.

```
SCEP.http.username="<SCEP username>"
SCEP.http.password="<SCEP password>"
```

4. Specify the challenge password to send with the CSR when requesting a certificate.

```
SCEP.challengePassword="<challenge password>"
```

5. Specify the following information for the CSR when requesting a certificate.

```
SCEP.csr.commonName="<common name>"
SCEP.csr.country="<country name>"
SCEP.csr.email="<email address>"
SCEP.csr.organization="<organization name>"
SCEP.csr.state="<state name>"
```

6. Configure the CA certificate fingerprint to confirm the authenticity of the CA response during enrollment.

```
SCEP.CAFingerprint="<CA certificate fingerprint>"
```

7. Specify the number of times to poll the SCEP server when the SCEP server returns a Certificate Enrollment Response Message with `pkiStatus` set to pending. Configure the phone to retry between 1 and 24 times. By default, the phone retries 12 times.

```
SCEP.certPoll.retryCount="<retry count>"
```

8. Specify the number of seconds to wait between poll attempts when the SCEP server returns a Certificate Enrollment Response Message with `pkiStatus` set to pending. Configure the phone to wait between 300 and 3600 seconds. By default, it waits for 300 seconds, or five minutes.

```
SCEP.certPoll.retryInterval="<# of seconds>"
```

9. Specify the time interval to retry certificate renewal. Configure between 28,800 seconds (eight hours) and 259,200 (72 hours) seconds. By default, the phone retries certificate removal 86,400 seconds (24 hours).

```
SCEP.certRenewalRetryInterval="<retry count>"
```

10. Specify the percentage of the certificate validity percentage threshold to initiate a renewal. Configure between 50% and 100%. The default is 80%.

```
SCEP.certRenewalThreshold="<% validity>"
```

11. Specify the number of times to retry the enrollment process in case of enrollment failure. Configure the phone to retry between 1 and 24 times. By default, the phone retries 12 times.

```
SCEP.enrollment.retryCount="<retry count>"
```

12. Specify the time interval to retry the enrollment process in case of enrollment failure. Configure the phone to wait between 300 and 3600 seconds. By default, it waits for 300 seconds, or five minutes.

```
SCEP.enrollment.retryInterval="<# of seconds>"
```

## Custom Wi-Fi Certificates

You can install custom wireless network certificates for added security.

For wireless network certificates:

- The phone shared Platform CA and Application CA certificates between Wi-Fi and Ethernet settings.

The phone can't connect to both Ethernet and Wi-Fi at the same time.

- The phone retains installed and saved certificates until you choose to forget the network.
- Poly phones don't support certificates obtained via SCEP.

### Install and Choose a Root CA Wi-Fi Certificate

Install a custom certificate for connecting to your wireless network.

---

**Note:** Client certificates and key must be in PKCS#8 PEM format.

---



---

**Note:** Only CA 1 and 2 and Platform 1 and 2 are valid for Wi-Fi.

---

If you set `device.wifi.wpa2Ent.caCert.name` to `none`, the phone user must choose the certificate when they connect to a wireless network.

**Procedure**

1. Install the certificates.

```
device.sec.TLS.customCaCert1="<value>"
device.sec.TLS.customCaCert2="<value>"
```

2. Choose the certificate to use.

```
device.wifi.wpa2Ent.caCert.name="<Platform 1 or Platform 2>"
```

**Install and Choose a Client Wi-Fi Certificate**

For added wireless network security, install a client certificate.

---

**Note:** Client certificates and key must be in PKCS#8 PEM format.

---



---

**Note:** Only CA 1 and 2 and Platform 1 and 2 are valid for Wi-Fi.

---

If you set `device.wifi.wpa2Ent.clientCert.name` to `none`, the phone user must choose the certificate when they connect to a wireless network.

**Procedure**

1. Install the certificates.

```
sec.TLS.customDeviceCert1="<value>"
sec.TLS.customDeviceCert2="<value>"
```

2. Choose the certificate to use.

```
device.wifi.wpa2Ent.clientCert.name = "<Platform 1 or Platform 2>"
```

## Encryption

Encryption ensures that information remains secure. Configure your phone to encrypt configuration files before sending them to the provisioning server over your network.

### Encrypt Files for Upload

Configure the phone to encrypt files you upload to the provisioning server.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable encryption for the following file types:

- Configuration file:

```
sec.encryption.upload.config="1"
```

- Call lists:

```
sec.encryption.upload.callLists="1"
```

- Contact directory:

```
sec.encryption.upload.dir="1"
```

- MAC address configuration file:

```
sec.encryption.upload.overrides="1"
```

## Change the Encryption Key from the Local Interface

Change the encryption key on the phones to maintain secure files.

Set `device.set="1"`.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Place all encrypted configuration files that you want to update on the provisioning server.  
The phone may reboot multiple times.
2. Enter the new key into the configuration file included in the list of files downloaded by the phone, specified in `000000000000.cfg` or `<MACaddress>.cfg`.

3. Specify a new encryption key:

```
device.sec.configEncryption.key.set="1"
device.sec.configEncryption.key="<encryption key>"
```

4. Provision the phone.
5. After you update the encryption key, you must decrypt the files on the server with the old encryption key, then encrypt again it with the new key. Alternatively, you can make the files available in unencrypted format.
6. Delete any configuration override files from the provisioning server so that the phone replaces them when it successfully boots.

The phone automatically reboots another time to use the new encryption key.

## Web Proxy

Use a web proxy to securely communicate outside your network with increased performance. For example, you can direct your phone's outbound requests through an enterprise proxy.

---

**Note:** Web proxy authentication is not supported for Microsoft Teams and Zoom base profiles.

---

- **Automatic** - Specify only the proxy credentials (if needed). Using DHCP or DNS-A, your system obtains a URL to automatically download a proxy auto-configuration (PAC) file.
- **Manual** - Specify the proxy address and port or the PAC URL.
- **Disabled** - You can't configure web proxy settings.

## Supported HTTP/HTTPS Web Proxy Services

When you successfully configure the web proxy server, Poly phones route specific HTTP and HTTPS services to the web proxy server.

The phones route the following services to the web proxy server:

- Generic services
- HTTP/HTTPS provisioning
- Core file upload
- Skype for Business Services
  - Registration services
  - Address Book Service (ABS)
  - Location Information Server (LIS)
  - Device update (To ensure reliable software updates, device update is direct in case a proxy isn't available.)
  - Exchange web services

## Manually Configure Web Proxy Access

Manually configure web proxy access for Poly phones that can't use automatic web proxy discovery.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the web proxy.

```
feature.wpad.enabled="1"
```

2. Enter the web proxy server address.

The default is Null. The maximum string length is 255 characters.

```
feature.wpad.proxy="<string>"
```

3. Enter the web proxy username and password.

The default is Null. The maximum string length is 255 characters.

```
feature.wpad.proxy.username="<string>"
feature.wpad.proxy.password="<string>"
```

## Disable Unused External Ports

Disable unused external ports to increase the device security.

Set `device.set="1"`.

You can disable the following ports:

- Computer connection port
- Headset connection ports
- USB ports

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Ignore any steps instructing you to disable a port you need to use.

### Procedure

1. Disable the computer connection port.

```
device.net.etherModePC="0"
device.net.etherModePC.set="1"
```

2. Disable the headset connection ports.

```
device.auxPort.enable="Disabled"
device.auxPort.enable.set="1"
```

3. Disable the USB ports.

On Poly CCX 500, CCX 600, and CCX 700 business media phones, set:

```
feature.usb.host.enabled="0"
```

On Poly CCX 400 business media phones, set:

```
feature.usb.host.enabled="1"
```

## Enable Voice over Secure IP

Enable Voice over Secure IP (VoSIP) to increase the level of security for calls over certain lines. When you enable VoSIP, the voice signals travel securely between endpoints without the need to introduce multiple lines in the Session Description Protocol (SDP).

The following are advantages for using VoSIP:

- The voice signals are encrypted, enabling safe and secure signal transmission between phones.
- Signaling and media to the cloud-hosted product are encrypted.

Configure your phones to dynamically select either Secure Real Time Protocol (SRTP) or Real Time Protocol (RTP) when making a call. The choice depends on the media security protocols negotiated between the phone and outbound proxy server using VoSIP.

### Procedure

- » Enable the VoSIP protocol. Replace *x* with the desired line key value.

```
reg.x.rfc3329MediaSec.enable="1"
```

## Enable and Configure 802.1X Security

Configure your phone to work on a network secured with 802.1X authentication. With this feature enabled, you can configure credentials the phone provides to authenticate on your secured network. Poly phones support IEEE 802 standards.

Set `device.set="1"`.

To set up an EAP method requiring a device or CA certificate, configure a TLS Platform Profile 1 or TLS Platform Profile 2 to use with 802.1X. For more information on EAP authentication protocol, see [RFC 3748: Extensible Authentication Protocol](#).

The phone supports the following 802.1X 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

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---



**Procedure**

1. Enable 802.1X authentication.

```
device.net.dot1x.enabled="1"
device.net.dot1x.enabled.set="1"
```

2. Set the username and password for 802.1X authentication. You don't need to set a password if you set EAP-TLS for the 802.1X EAP method.

```
device.net.dot1x.identity="<username>"
device.net.dot1x.password="<password>"
device.net.dot1x.identity.set="1"
device.net.dot1x.password.set="1"
```

3. Set an 802.1X EAP method. Available EAP methods are:

- EAP-None - No authentication
- EAP-TLS
- EAP-PEAPv0-MSCHAPv2
- EAP-PEAPv0-GTC
- EAP-TTLS-MSCHAPv2
- EAP-TTLS-GTC
- EAP-FAST
- EAP-MD5

```
device.net.dot1x.method="<EAP method>"
device.net.dot1x.method.set="1"
```

4. If you set the 802.1X method as EAP-FAST, you can set the following parameters as well:

```
device.net.dot1x.eapFastInBandProv="<0> or <1>"
device.pacfile.data="<Optional PAC file name>"
device.pacfile.password="<Password for PAC file if needed>"
device.net.dot1x.eapFastInBandProv.set="1"
device.pacfile.data.set="1"
device.pacfile.password.set="1"
```

## Enable FIPS 140-2 Encryption

The Federal Information Processing Standard (FIPS 140-2) compliance is a cryptographic function. Enable phones to use the FIPS 140-2 compliant cryptography.

Set `device.set="1"`.

**Procedure**

- » Enable FIPS 140-2 encryption.

```
device.sec.TLS.FIPS.enabled="1"
device.sec.TLS.FIPS.enabled.set="1"
```

# Configuring Audio Settings

---

## Topics:

- [Automatic Gain Control](#)
- [Enable AEC for Headsets](#)
- [Noise Suppression](#)
- [Comfort Noise](#)
- [Audio Codecs](#)

Configure modifications to the default audio configurations to optimize the audio quality of your phones.

## Automatic Gain Control

Automatic gain control (AGC) boosts the volume of near-end conference participants. AGC is enabled by default to ensure far-end audio clarity.

---

**Note:** You can't disable this feature. Changing the default settings may cause accessibility concerns for people who use audio augmentation assistive technology.

---

If you are running an application that also provides AGC through the software, Poly recommends that you disable the application AGC.

## Enable AEC for Headsets

The default configuration enables acoustic echo cancellation (AEC) for both the handset and speakerphone. Enable AEC for connected Poly Bluetooth headsets to reduce echo during calls.

AEC includes the following features:

- Talk state detector: Determines whether the near-end user, far-end user, or both are speaking.
- Linear adaptive filter: Adaptively estimates the loudspeaker-to-microphone echo signal and subtracts that estimate from the microphone signal.
- Nonlinear processing: Suppresses any echo remaining after the linear adaptive filter.

### Procedure

- » Enable AEC for headsets.

```
voice.aec.bt.hd.enable="1"
```

# Noise Suppression

Poly phones offer multiple options to suppress background noise during calls. Some options are integrated into the phone itself, but you can configure others.

Integrated noise suppression reduces background noise caused by items such as fans, projectors, and air conditioners.

## Poly NoiseBlock

The default configuration enables Poly NoiseBlock on Poly phones.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

## Disable Poly NoiseBlock

Disable Poly Noiseblock and Poly NoiseBlockAI on your phones.

Poly NoiseBlock automatically mutes the microphone when a user stops speaking. It reduces interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter.

### Procedure

- » Disable Poly NoiseBlock.

```
voice.ns.hf.block="0"
```

## Enable Poly NoiseBlockAI

Enable Poly NoiseBlockAI on your phones.

Poly NoiseBlockAI suppresses background noise while a call participant actively speaks. It also reduces interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter. Call recipients hear only the intended speaker's voice.

---

**Note:** You can't enable both Poly NoiseBlock and Poly NoiseBlockAI at the same time. The same parameter configures both modes.

---

### Procedure

- » Enable Poly NoiseBlockAI.

```
voice.ns.hf.block="2"
```

## Acoustic Fence

Acoustic Fence technology suppresses background noise sent to the far end. This feature is particularly useful in call center environments where background noise can impact far-end audio quality.

Acoustic Fence works with the following devices:

- Phone handsets
- Wired headsets connected to the headset port

- USB headsets connected to the phone

---

**Note:** Acoustic Fence doesn't support Bluetooth headsets.

---

## Enable Polycom Acoustic Fence for Handset Calls

Enable Polycom Acoustic Fence for handset calls to remove unwanted background noise from calls.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable noise suppression for handset calls.

```
voice.ns.hs.enable="1"
```

2. Enable Polycom Acoustic Fence for handset calls.

```
voice.ns.hs.enhanced="1"
```

3. Optional: Configure the Polycom Acoustic Fence threshold for handset calls.

A lower number removes less background noise, while a higher number removes more background noise. The default value is 8.

```
voice.ns.hs.nonStationaryThresh="<1 to 10>"
```

## Enable Polycom Acoustic Fence for Headset Calls

Enable Polycom Acoustic Fence for headset calls to remove unwanted background noise from calls.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable noise suppression for headset calls.

```
voice.ns.hd.enable="1"
```

2. Enable Polycom Acoustic Fence for headset calls.

```
voice.ns.hd.enhanced="1"
```

3. Configure the Polycom Acoustic Fence threshold for headset calls.

A lower number removes less background noise while a higher number removes more background noise. The default value is 8.

```
voice.ns.hd.nonStationaryThresh="<1 to 10>"
```

## Add Acoustic Fence Options to the Local Interface

Add the Polycom Acoustic Fence menu items to the phone's **Basic** menu.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

- » Enable the **Acoustic Fence** menu item on the phone's local interface.

```
feature.acousticFenceUI.enabled="1"
```

## Dynamically Deactivate Acoustic Fence in Full-Screen Mode

Enable the phone to dynamically deactivate Acoustic Fence when users change the view to full screen mode in a video call.

Enable this setting to optimize CCX 600 phone performance while using a Polycom EagleEye Mini USB camera with Acoustic Fence.

### Procedure

- » Enable the phone to dynamically deactivate Acoustic Fence when in full-screen mode.

```
video.disableAFOnFullScreen="1"
```

## Configure VAD

Set the threshold for determining what is considered background noise using Voice activity detection (VAD).

Voice activity detection (VAD) conserves network bandwidth. VAD detects periods of silence in the transmit data path so the phone doesn't transmit unnecessary data packets for outgoing audio.

For compression algorithms without an inherent VAD function, such as G.711, the phone uses the codec-independent processing specified in [RFC 3389](#).

G.711 Appendix II, in [RFC 3389](#), defines the payload format for G.711 use in packet-based multimedia communication systems.

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

For more information about VAD, see Voice Activity Detection parameters in the *Parameter Reference Guide*.

### Procedure

1. Enable VAD.

```
voice.vadEnable="1"
```

2. Set the VAD threshold in decibels.

The default value is 25. Sounds louder than the VAD threshold are considered voice. Sounds below the threshold are considered background and muted from the call.

```
voice.vadThresh="<0 to 30>"
```

## Comfort Noise

Comfort noise ensures a consistent background noise level to provide a natural call experience for speakerphone and handset calls.

Comfort noise is enabled by default on Poly phones, and the payload type is negotiated in the Session Description Protocol (SDP) with a default of 13 for 8 kHz codecs and 122 for 16 kHz codecs and higher.

---

**Note:** Comfort noise isn't related to the comfort noise packets the phone generates when you enable VAD.

---

## Configure Comfort Noise for Speakerphone Calls

Add comfort noise to a hands-free call to ensure that the line isn't completely silent when callers aren't talking.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Comfort noise provides a minimal level of audio on the line to ensure callers that the call is still connected. You can add and adjust the level of comfort noise for speakerphone and headset calls.

### Procedure

1. Enable comfort noise for speakerphone calls.

```
voice.cn.hf.enable="1"
```

2. Optional: Adjust the comfort noise level.

The phone's default value of 30 is quite loud. Enter a higher number to reduce the comfort noise. A lower number increases the comfort noise.

```
voice.cn.hf.attn="<0 to 90>"
```

## Configure Comfort Noise for Handset Calls

Add comfort noise to a handset call to ensure that the line isn't completely silent when callers aren't talking.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable comfort noise for handset calls.

```
voice.cn.hs.enable="1"
```

2. Optional: Adjust the comfort noise level.

The default value is 35.

```
voice.cn.hs.attn("<0 to 90>")
```

## Audio Codecs

Configure the audio codecs for your phones.

This section provides basic information for configuring audio codecs. For more information on configuring audio codecs, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

## Supported Audio Codec Specifications

Specifications for audio codecs supported on Poly phones.

**Note:** The network bandwidth necessary to send encoded voice is typically 5% to 10% higher than the encoded bit rate due to packetization overhead. For example, a G.722.1C call at 48 Kbps consumes about 100 Kbps of network bandwidth for both the receive and transmit signals (two-way audio).

### Audio Codec Specifications

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
All systems	G.711 $\mu$ -law	RFC 1890	64 Kbps	80 Kbps	8 ksps	20 ms	3.5 kHz
All systems	G.711 a-law	RFC 1890	64 Kbps	80 Kbps	8 ksps	20 ms	3.5 kHz

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
All systems	G.711	RFC 1890	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722 Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16 ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.	RFC 3551	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1	RFC 3047	24 Kbps 32 Kbps	40 Kbps 48 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 ksps	20 ms	14 kHz
All systems	G.729AB	RFC 1890	8 Kbps	24 Kbps	8 ksps	20 ms	3.5 kHz
All systems	Opus	RFC 6716	8 to 24 Kbps	24 to 40 Kbps	8 ksps 16 ksps	20 ms	3.5 kHz 7 kHz
All systems	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



Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
All systems	Siren 7	SIREN7	16 Kbps	32 Kbps	16 ksps	20 ms	7 kHz
			24 Kbps	40 Kbps			
			32 Kbps	48 Kbps			
All systems	Siren14	SIREN14	24 Kbps	40 Kbps	32 ksps	20 ms	14 kHz
			32 Kbps	48 Kbps			
			48 Kbps	64 Kbps			
All systems	iLBC	RFC 3951	13.33 Kbps	31.2 Kbps	8 ksps	20 ms	3.5 kHz
			15.2 Kbps	24 Kbps		30 ms	
All systems	SILK	SILK	6 to 20 Kbps	36 Kbps	8 ksps	20 ms	3.5 kHz
				41 Kbps	12 ksps		5.2 kHz
			7 to 25 Kbps	46 Kbps	16 ksps		7 kHz
			8 to 30 Kbps	56 Kbps	24 ksps		11 kHz
			12 to 40 Kbps				

## Set Audio Codec Priority

Set the codec priority to improve consistency and reduce workload on the phones.

Note the following about audio codec priority:

- Permitted values to set audio codec priority are 1 to 35.
- 1 is the highest priority.
- A value of 0 or Null disables the codec.
- A change to the default value doesn't cause a phone to restart or reboot.

**Note:** The Opus codec isn't compatible with G.729 and iLBC. If you set Opus to the highest priority, G.729 and iLBC don't publish.

If you set G.729 and iLBC to the highest priority, Opus doesn't publish.

The phone doesn't answer calls using unsupported codecs. If the phone receives a call using an unsupported codec, the phone answers the call with the first supported codec priority.

The following values represent the configuration defaults. The default configuration sets the priority values from 1 to 8. All codecs **not** listed in the following table have a default priority value of 0 (disabled).

**Audio Codec Priority Default Values**

Parameter	Default Priority
voice.codecPref.Siren22.64kbps	1
voice.codecPref.G7221_C.48kbps	2
voice.codecPref.Siren14.48kbps	3
voice.codecPref.G722	4
voice.codecPref.G7221.32kbps	5
voice.codecPref.G711_Mu	6
voice.codecPref.G711_A	7
voice.codecPref.G729_AB	8

**Procedure**

- » Set audio codec priority.

```
voice.codecPref.AMRNB="<priority value>"
voice.codecPref.AMRWB="<priority value>"
voice.codecPref.G711_A="<priority value>"
voice.codecPref.G711_Mu="<priority value>"
voice.codecPref.G719.32kbps="<priority value>"
voice.codecPref.G719.48kbps="<priority value>"
voice.codecPref.G719.64kbps="<priority value>"
voice.codecPref.G722="<priority value>"
voice.codecPref.G7221.16kbps="<priority value>"
voice.codecPref.G7221.24kbps="<priority value>"
voice.codecPref.G7221.32kbps="<priority value>"
voice.codecPref.G7221_C.24kbps="<priority value>"
voice.codecPref.G7221_C.32kbps="<priority value>"
voice.codecPref.G7221_C.48kbps="<priority value>"
voice.codecPref.G729_AB="<priority value>"
voice.codecPref.iLBC.13_33kbps="<priority value>"
voice.codecPref.iLBC.15_2kbps="<priority value>"
voice.codecPref.Lin16.8ksps="<priority value>"
voice.codecPref.Lin16.16ksps="<priority value>"
voice.codecPref.Lin16.32ksps="<priority value>"
voice.codecPref.Lin16.44_1ksps="<priority value>"
voice.codecPref.Lin16.48ksps="<priority value>"
voice.codecPref.Opus="<priority value>"
voice.codecPref.SILK.8ksps="<priority value>"
voice.codecPref.SILK.12ksps="<priority value>"
voice.codecPref.SILK.16ksps="<priority value>"
voice.codecPref.SILK.24ksps="<priority value>"
voice.codecPref.Siren7.16kbps="<priority value>"
voice.codecPref.Siren7.24kbps="<priority value>"
voice.codecPref.Siren7.32kbps="<priority value>"
voice.codecPref.Siren14.24kbps="<priority value>"
voice.codecPref.Siren14.32kbps="<priority value>"
voice.codecPref.Siren14.48kbps="<priority value>"
voice.codecPref.Siren22.32kbps="<priority value>"
```

```
voice.codecPref.Siren22.48kbps="<priority value>"
voice.codecPref.Siren22.64kbps="<priority value>"
```

## Configure the SILK Audio Codec

Configure the SILK audio codec settings.

### Procedure

1. Set the maximum average encoder output bit rate in kbps for the supported SILK sample rate. Replace x with the sample rate.

```
voice.audioProfile.SILK.xksp.encMaxAvgBitrateKbps="<value>"
```

2. Specify the SILK encoder complexity. The higher the number, the more complex encoding is allowed.

The default is 2. The value range is 0 to 2.

```
voice.audioProfile.SILK.encComplexity="<value>"
```

3. Optional: Enable inband forward error correction (FEC) in the SILK encoder.

---

**Note:** When you enable this parameter, perceptually important speech information is sent twice: once in the normal bit stream and again at a lower bit rate in later packets. This results in an increased bit rate.

---

```
voice.audioProfile.SILK.encInbandFECEnable="1"
```

4. Set the SILK encoder expected network packet loss percentage.

The default is 0. The value range is 0 to 100.

---

**Note:** Configuring this value enables less interframe dependency encoded into the bit stream. This results in increasingly larger bit rates but with an average bit rate less than that configured with `voice.audioProfile.SILK.*`.

---

```
voice.audioProfile.SILK.encExpectedPktLossPercent="<value>"
```

5. Optional: Enable discontinuous transmission (DTX) in the SILK encoder.

---

**Note:** DTX reduces the encoder bit rate to 0 bps during silence.

---

```
voice.audioProfile.SILK.encDTXEnable="1"
```

## Configure the Opus Audio Codec

Configure the Opus audio codec settings.

### Procedure

1. Assign the Opus encoder's application type.
  - VoIP (Default) - Process signal for improved speech intelligibility

- Audio - Favors faithfulness to original input audio
- LowDelay - Configures the minimum possible coding delay by disabling certain modes of operation

```
voice.audioProfile.Opus.appType="<value>"
```

**2.** Set the preferred encoder transmit bit rate mode.

- CVBR (Default) - Constrained variable bit rate
- CBR - Constant bit rate
- VBR - Variable bit rate

```
voice.audioProfile.Opus.BitrateMode="<value>"
```

**3.** Set the maximum average encoder output bit rate in kbps.

```
voice.audioProfile.Opus.encMaxAvgBitrateKbps="<value>"
```

**4.** Optional: Enable decoding of forward error correction (FEC) information sent from the far end.

```
voice.audioProfile.Opus.decInbandFECEnable="1"
```

**5.** Optional: Enable inband forward error correction (FEC) in the Opus encoder.

---

**Note:** When you enable this parameter, perceptually important speech information is sent twice: once in the normal bit stream and again at a lower bit rate in later packets. This results in an increased bit rate.

---

```
voice.audioProfile.Opus.encInbandFECEnable="1"
```

**6.** Optional: Set the Opus encoder expected network packet loss percentage.

The default is 0. The value range is 0 to 100.

---

**Note:** This parameter helps the Opus encoder decide what amount of redundant information to send when you enable inband FEC using `voice.audioProfile.Opus.encInbandFECEnable`.

---

```
voice.audioProfile.Opus.encExpectedPktLossPercent="<value>"
```

**7.** Optional: Enable discontinuous transmission (DTX) in the Opus encoder.

---

**Note:** DTX skips packet transmission during periods of silence and only sends periodic frames with comfort noise information.

---

```
voice.audioProfile.Opus.encDTXEnable="1"
```

# Configuring Video Settings

---

## Topics:

- [Camera Options](#)
- [Configuring the Call Mode for Outgoing Calls](#)
- [I-Frames](#)

Poly CCX 600 and CCX 700 business media phones support video calls.

---

**Note:** Poly CCX 600 business media phones require an optional Polycom EagleEye Mini USB camera to send video.

---

## Camera Options

Configure the camera the phone uses for video calls.

Control where the **Camera** settings appear and whether users can access it without administrative permissions.

If your phone connects to a PTZ camera, you can configure several camera presets for the camera's position.

## Disable Far End Camera Control

Disable Far End Camera Control (FECC) to stop far-end participants from controlling the framing and angle of the local camera.

FECC enables participants to adjust the pan, tilt, zoom (PTZ) of the camera. When disabled, only the meeting host can control the PTZ camera.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

## Procedure

- » Disable FECC.

```
feature.fecc.enabled="0"
```

## Enable the Camera Button in the Main Menu

Enable the **Camera** button on the main menu, which enables users to control a connected pan, tilt, zoom (PTZ) camera.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable the **Camera** button in the main menu.

```
homeScreen.camera.enable="1"
```

## Remove Camera Settings from the Basic Menu

By default, camera settings, including preset storage and modifications, are available under the **Basic** menu, which is available for all users. You can move camera settings to the **Advanced** menu so only administrators have access to them.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Move camera settings to the **Advanced** menu.

```
video.camera.menuLocation="Advanced"
```

## Configure a Camera Home Preset

Configure the home preset for your pan, tilt, zoom (PTZ) camera.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the camera to move to its home position when it's idle.

```
video.camera.preset.home.uponIdle.enabled="1"
```

2. Set the number of minutes the camera remains idle before moving to its home position. The range in minutes is 0-3600.

```
video.camera.preset.home.uponIdle.delay="<# of minutes>"
```

3. Set the pan coordinates for the home position. The value range is 0-1000.

```
video.camera.preset.home.pan="<x>"
```

4. Set the tilt coordinate for a camera home preset. The value range is from 0-1000.

```
video.camera.preset.home.tilt="<x>
```

5. Set the zoom coordinate for a camera home preset. The value range is from 0-1000.

```
video.camera.preset.home.zoom="<x>"
```

## Configuring the Call Mode for Outgoing Calls

Configure video-enabled phones to place audio-only or audio-video calls by default.

All outgoing calls on video-enabled phones start in audio-video mode. If you mute your video signal, the phone displays a video-muted image instead of the video feed. Audio-only calls don't transmit any video signal, but users can add video to the active audio-only call.

---

**Note:** Incoming video calls display video even when you set the system default to audio-only.

---

- **Set the Default Call Mode:** Change the default call mode for outgoing calls to audio-only calls.
- **Mute Video:** Start audio-video calls with muted video.
- **Enable the Audio Call Button:** Give users the option to place an audio-only call from the **Home** screen, when the phone places audio-video calls by default.
- **Retain Call Mode Preferences:** Enable the phone to remember the last call mode setting for the next outgoing call.

### Set the Default Call Mode to Audio-Only

Configure your video-enabled phone to place audio-only calls by default.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

In an audio-only call, you can add video to the call. You can mute video after you add it, but you can't turn it off.

#### Procedure

- » Set the default call mode to audio.

```
video.callMode.default="audio"
```

### Mute Video at the Start of Video Calls

Starting a call with muted video helps prevent sending video feed before all call participants are ready to appear on camera.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Start the video transmission with muted video.

```
video.autoStartVideoTx="0"
```

**Enable the Audio Call Button**

On phones set to place audio-video calls by default, add the **Audio Call** button to the **Home** screen so users can directly place an audio-only call..

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable the **Audio Call** button on the **Home** screen.

```
up.homeScreen.audioCall.enabled="1"
```

**Enable Call Mode Persistence**

Configure the phone to maintain the last call mode setting (audio-only video) and use the same setting for the next call.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable call mode persistence.

```
audioVideoToggle.callMode.persistent="1"
```

**I-Frames**

When video streams initialize, devices transmit video packets called I-frames (reference frames) that contain information to display a complete image.

The phones send smaller and less complete frames, known as P-frames, to consume less bandwidth. Due to packet loss, jitter, or corruption, phones occasionally must make multiple requests for a complete I-frame to reset the full frame. Devices can then revert to P-frame updates.

You can set parameters to control an I-frame request. The following table indicates parameter dependencies and messaging behavior when setting an I-frame request method.



**I-Frame Parameter Dependencies**

<code>video.forceRtcpVideoCodecControl</code>	<code>video.dynamicControlMethod</code>	<code>voIpProt.SDP.offer.rtcpVideoCodecControl</code>	<b>Behavior when requesting video I-frame updates</b>
0	0 (n/a)	0	The phone sends only SIP INFO messages. No RTCP-FB is offered in SDP.
0	1 (n/a)	0	The phone sends only SIP INFO messages. No RTCP-FB is offered in SDP.
0	0 (n/a)	1	RTCP-FB is offered in SDP. If SDP responses don't contain the required RTCP-FB attribute, then the phone uses only SIP INFO requests.
0	1 (N/A)	1	RTCP-FB is offered in SDP. If SDP responses don't contain the required RTCP-FB attribute, then the phone uses only SIP INFO requests.
1	0	0	The SDP attribute <code>a=rtcp-fb</code> isn't included in SDP offers. The phone attempts both RTCP-FB and SIP INFO messages.
1	1	0	The SDP attribute <code>a=rtcp-fb</code> isn't included in SDP offers. The phone attempts both RTCP-FB and SIP INFO messages. If the phone receives no RTCP-FB messages, the phone sends only SIP INFO messages. If the phone receives no response for SIP INFO messages, then the phone attempts both RTCP-FB and SIP INFO messages again.
1	0	1	RTCP-FB is offered in SDP. Even if the SDP response doesn't include an accepted <code>a=rtcp-fb</code> attribute, the phone sends both RTCP-FB and SIP INFO messages.
1	1	1	RTCP-FB is offered in SDP. Even if the SDP response doesn't include an accepted <code>a=rtcp-fb</code> attribute, the phone initially sends both RTCP-FB and SIP INFO messages. If the phone doesn't receive a RTCP-FB response, the phone sends only SIP INFO messages.

# Configuring Call Controls

---

## Topics:

- [Do Not Disturb](#)
- [Call Hold](#)
- [Configure Default Call Transfer Type](#)
- [Call Forwarding](#)
- [Convert the Call Timer to Display in Seconds](#)
- [Call Waiting Alerts](#)
- [Use Network Signaling for Caller ID](#)
- [Enable the Remote Party Disconnect Alert](#)
- [Configure Directed Call Pickup](#)
- [Configure the Call Park and Retrieve Star Code](#)
- [Voicemail](#)
- [Enable Local Call Recording](#)
- [Missed Call Notifications](#)
- [Configure Last Call Return](#)
- [Enable the Conference Meeting Dial-In Options List](#)
- [Conference Call Host Management](#)
- [Configure Hot Dialing](#)
- [Multiple Call Appearances](#)
- [Flexible Call Appearances](#)
- [Busy Lamp Field](#)
- [Configure Key System Emulation](#)
- [Enable Instant Messaging](#)
- [Shared Lines](#)
- [Configure Bridged Line Appearance](#)
- [PTT and Group Paging](#)
- [Enable SIB-B Group Call Pickup](#)
- [Intercom Calls](#)
- [Configure E.911](#)

You can configure calling features for the Poly phone once it's connected to your VoIP network.

# Do Not Disturb

Disable Do Not Disturb on one or more phones. You can also configure your phones to automatically enter Do Not Disturb when the lines on your call server enter Do Not Disturb.

## Related Links

[Enable Do Not Disturb When the Phone Locks](#) on page 75

## Disable Do Not Disturb

Prevent the user from enabling Do Not Disturb on the phone.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Open the configuration file.
2. Disable DND on the phone.

```
feature.doNotDisturb.enable="0"
```

3. Save the configuration file.

## Enable Call Server-Based Do Not Disturb

Poly phones can enter Do Not Disturb (DND) in sync with the call server using an as-feature-event SIP subscription.

Ensure `reg.x.serverFeatureControl.localProcessing.dnd` is disabled before configuring DND.

The following conditions apply for call server-based DND:

- Shared lines don't support call server-based DND.
- If you enable call server-based DND, but don't turn it on with DND enabled on the phone, the `Do Not Disturb` message displays on the phone but incoming calls continue to ring.
- Call server-based DND disables local call forwarding and DND. However, if an incoming call doesn't route through the server, an audio alert may play on the phone.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the phone to enter DND based on the call server status.

```
voIpProt.SIP.serverFeatureControl.dnd="1"
```

2. Prevent the phone from allowing a user to enable DND locally. This configures the phone to enable DND via the server only.

```
voIpProt.SIP.serverFeatureControl.localProcessing.dnd="0"
```

3. Optional: There is a DND SIP layer modifier applicable to local DND (this is not applicable if `serverFeatureControl` is enabled). When enabled, the phone rejects inbound calls when DND is on with a **486 Busy** response. When disabled, the phone rejects calls with a **603 Decline** response.

```
call.rejectBusyOnDnd="1"
```

## Enable Call Server-Based Do Not Disturb on a Registered Line

Configure the phone to enter Do Not Disturb (DND) in sync with the call server using an as-feature-event SIP subscription on a registered line.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable the phone to enter DND based on the call server status. Replace *x* with the desired line key value.

```
reg.x.serverFeatureControl.dnd="1"
```

## Call Hold

Enables users to pause activity on an active call so that they can use the phone for another task.

When an active call is placed on hold, a message displays informing the held party that they are on hold.

Poly phones use the preferred call holding protocols by default, and typically don't require additional configuration.

## Configure Call Hold Reminders

Configure the phone to send an audible alert after a call is on hold for a specified amount of time.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Open the configuration file.
2. Enable call hold reminders.

```
call.hold.localReminder.enabled="1"
```

3. Set how long the phone waits, in seconds, after placing the call on hold before sounding the reminder. The default is 90 seconds.

```
call.hold.localReminder.startDelay="<number of seconds>"
```

4. Set the amount of time, in seconds, the phone repeats the reminder after the initial reminder sounds. The default is 60 seconds.

```
call.hold.localReminder.period="<number of seconds>"
```

5. Save the configuration file.

## Configure Hold Music

Configure the phone to play streaming music for callers while they wait on hold.

If supported by the call server, you can enter a music-on-hold URI. For more information, see [RFC Music on Hold draft-worley-service-example](#).

- Note the URI of your media stream service.
- Set `reg.x.musicOnHold.uri="NULL"`.

### Procedure

- » Configure the URI for the media streaming service.

```
voIpProt.SIP.musicOnHold.uri="<SIP URI>"
```

## Change the Reinvite Method

Configure the phone to send an `inactive` stream mode parameter when placing a call on hold.

By default, the phone sends a reinvite message with a stream mode parameter of `sendonly` when placing a call on hold.

---

**Note:** The phone ignores the value of this parameter if you set `voIpProt.SIP.useRFC2543hold="1"`.

---

### Procedure

- » Configure the phone to send an `inactive` stream mode parameter when placing a call on hold.

```
voIpProt.SIP.useSendonlyHold="0"
```

## Configure Default Call Transfer Type

Set the default call transfer type to **Blind Transfer**.

The following call transfer types are available to the phone's users:

- **Blind Transfer:** Complete a call transfer without speaking with the recipient first.
- **Consultative Transfer (Default):** Complete a transfer after speaking with the recipient.

### Procedure

- » Set the default call transfer type to blind transfer.

```
call.defaultTransferType="Blind"
```

# Call Forwarding

Enable users to automatically forward incoming calls to another contact or phone line.

## Forward Calls While Busy

Configure the phone to forward incoming calls to a specified contact when the phone is busy.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable the phone to forward calls while busy, and Replace the x with the desired line key value.

```
divert.busy.x.enabled="1"
```

2. Specify the contact you want to forward calls to. Replace the x with the desired line key value.

```
divert.busy.x.contact="<contact address>"
```

## Forward Calls While DND Is Active

Configure the phone to forward incoming calls to a specified contact when Do Not Disturb (DND) is active.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable the phone to forward calls while DND is active, and specify the contact you want to forward calls to. Replace the x with the desired line key value.

```
divert.dnd.x.enabled="1"
```

2. Replace the x with the desired line key value.

```
divert.dnd.x.contact="<contact address>"
```

## Forward Unanswered Calls

Configure the phone to forward unanswered incoming calls to a specified contact after a specified amount of time.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the phone to forward an unanswered call. Replace the *x* with the desired line key value.

```
divert.noanswer.x.enabled="1"
```

2. Specify how long the phone can ring (in seconds) before forwarding the call. The default is 55 seconds.

```
divert.noanswer.x.timeout="<number of seconds>"
```

3. Specify the contact you want to forward calls to.

```
divert.noanswer.x.contact="<contact address>"
```

## Disable Call Forwarding

Remove the **Call Forward** option from the **Features** menu, preventing users from forwarding incoming calls.

### Procedure

1. Open the configuration file.
2. Disable call forwarding.

```
feature.forward.enable="0"
```

3. Save the configuration file.

## Convert the Call Timer to Display in Seconds

Convert the call timer from HH:MM:SS to only seconds.

A call timer displays on the phone's screen during calls, and a separate call duration timer displays the hours, minutes, and seconds for each call in progress.

### Procedure

- » Configure the call time to display in seconds.

```
up.timerDisplayInSeconds="1"
```

## Call Waiting Alerts

By default, the phone alerts users to incoming calls during an active call. Disable these call waiting alerts or specify ringtones for incoming calls.

### Silence the Ringtone for Call Waiting

If the phone receives an incoming call while in an active call, configure the phone to display the incoming call options on the screen but not to play a ringtone.

#### Procedure

1. Open the configuration file.
2. Silence the call waiting ringtone.

```
call.callWaiting.ring="silent"
```

3. Save the configuration file.

### Disable Call Waiting Alerts

Disable call waiting alerts so that incoming calls don't disrupt the active call.

The phone alerts you to an incoming call while you are in an active call. Enabling the default (1) notifies the user of a second incoming call after ending the first call.

#### Procedure

1. Open the configuration file.
2. Disable call waiting alerts.

```
call.callWaiting.enable="0"
```

3. Save the configuration file.

### Configure Call Waiting for a Specific Line

Distinctive call waiting allows you to configure call waiting for a specific line uses the available ringtones.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---



---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

#### Procedure

1. Open the configuration file.
2. Set the ring class for line 1.

```
voIpProt.SIP.alertInfo.1.class="custom1"
```



### 3. Set the ring value for line 1.

```
voIpProt.SIP.alertInfo.1.value="<ringtone name set by  
se.rt.custom1.name value>
```

## Use Network Signaling for Caller ID

Configure the phone to get caller identification information from network signaling.

By default, the phone checks an incoming call against the local contact directory for caller identification. If the phone finds a match, the matching contact's name displays. Otherwise, the phone displays the incoming phone number.

The phone can't pull caller ID information from an LDAP corporate directory integration.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable the phone to use network signaling to get caller ID information.

```
up.useDirectoryNames="0"
```

## Enable the Remote Party Disconnect Alert

Enable the phone to audibly notify users when callers on the far end disconnect from an active call.

### Procedure

- » Enable the remote party disconnect alert. Set any of the following values:

- messageWaiting
- instantMessage
- remoteHoldNotification
- localHoldNotification
- positiveConfirm
- negativeConfirm
- welcome
- misc1 through misc7
- custom1 through custom10

```
call.remoteDisconnect.toneType="<audio tone value>"
```

## Configure Directed Call Pickup

Enable users to pick up incoming calls to another phone by dialing the extension of that phone.

This feature requires support from a SIP server, and the setup 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.

### Procedure

1. Enable directed call pickup.

```
feature.directedCallPickup.enabled="1"
```

2. Specify the directed call pickup method. The default value is legacy, which uses the star code configured in `call.directedCallPickupString`.

Set this parameter to native for the phone to use a native protocol method.

```
call.directedCallPickupMethod="<call pickup method>"
```

3. Specify the star code for directed call pickup.

For call servers other than BroadWorks, change the call pickup string from default. The default string is \*97.

```
call.directedCallPickupString="<star code>"
```

## Configure the Call Park and Retrieve Star Code

Enable users to park an active call and retrieve parked calls from the call orbit on any phone.

This feature requires support from a SIP server, and the setup 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. Call park moves the call to a separate address where any phone can retrieve the call.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Configure the star code to initiate the call park, placing the call into park orbit. The default setting is \*68.

Choose a value based on your SIP server settings.

```
call.parkedCallString="<value>"
```

## Voicemail

When you configure the phone with voicemail, it provides a visual and audible alert when a new voicemail message is available.

### Configure Voicemail Settings

Configure the phone's voicemail server and voicemail settings.

Note the address for the voicemail server.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

#### Procedure

1. Set the URI for the voicemail server. The phone sends a SUBSCRIBE request when it boots up. Replace *x* with the desired line key value.

```
msg.mwi.x.subscribe("<message center server URI>")
```

2. Optional: Configure an address to reach out to for message retrieval and notifications. Replace *x* with the desired line key value.

By default, the phone places a call to itself.

```
msg.mwi.x.callBackMode="contact"
msg.mwi.x.callBack("<message center server URI>")
```

3. Optional: Enable the phone's screen backlight to light up when a user receives a voice message.

```
up.mwiVisible="1"
```

### Disable Voicemail

Disable the voicemail feature if you don't use voicemail in your deployment. Disabling voicemail also removes the **Voicemail** button from the main menu.

#### Procedure

- » Disable voicemail.

```
feature.voicemail.enabled="0"
```

## Enable Local Call Recording

Local call recording enables the phone to record audio calls to a connected USB device.

---

**Note:** Federal, state, and local laws may legally require that you notify some or all of the call parties when a call recording is in progress.

---

When users record their calls, the phone saves the recorded audio calls in WAV format and includes a date/time stamp. Users can then playback the recorded audio on the phone itself or a computer.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable local call recording.

```
feature.callRecording.enabled="1"
```

## Missed Call Notifications

By default, a counter with the number of missed calls displays on the **Recent Calls** icon on the phone.

For missed call configuration options, see the *Poly Trio Parameter Reference Guide*.

## Configure Last Call Return

Poly phones support the ability to quickly dial the last received call using a star code.

This feature requires support from a SIP server. Many SIP servers implement this feature using a specific star code sequence. When enabled, the phone displays an **LCR** softkey that enables users to call the phone address that last called them.

### Procedure

1. Enable the last call returned feature.

```
feature.lastCallReturn.enabled="1"
```

2. Specify the star code to dial the last returned call. The default is \*69.

```
call.lastCallReturnString="<star code>"
```

## Enable the Conference Meeting Dial-In Options List

Reminders for upcoming meetings include options to easily dial in and join the meeting.

When a meeting invite includes a dial-in number, the **Join** button displays on the meeting and the meeting reminder. By default, the **Join** button dials the first available number if the meeting invite includes more than one possible dial-in number.

When enabled, the phone provides multiple dial-in options when the user taps the **Join** button on the onscreen meeting reminder. The phone displays the following dial-in options to join a meeting:

- SIP URI
- Tel URI
- PSTN number
- IP dial

**Procedure**

- » Enable the phone to present a list of dial-in numbers when users select **Join** on meeting reminders.

```
exchange.meeting.join.promptWithList="1"
```

## Conference Call Host Management

Configure the phone to offer additional call controls when it hosts a conference call.

Note the following:

- By default, when the phone hosting a three-party conference call leaves the call, the remaining call participants transfer to a point-to-point call. You can configure the phone to end the call for all call participants if it's the host and leaves the call.
- If the host of a four-party local conference leaves the conference, all parties disconnect 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 [Conference Management](#).

## Enable Conference Host to Place Participants on Hold

Enable the conference host to place call participants on hold during the conference call.

**Procedure**

- » Enable the conference host to place participants on hold.

```
call.localConferenceCallHold="1"
```

## End a Conference Call When the Host Disconnects

Configure the phone to end a conference call if the phone is the host and it disconnects from the call.

**Procedure**

- » Enable the phone to end a conference call if it disconnects.

```
call.transferOnConferenceEnd="0"
```

## Disable Conference Management Options

Disable the conference management options on the phone so users can only attend meetings as participants. Users can still hold three-way conferences, but conference management options aren't available.

### Procedure

- » Disable conference management options.

```
feature.nWayConference.enabled="0"
```

## Configure Hot Dialing

Configure the phone to automatically call a specified number when it goes off-hook.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable automatic off-hook dialing.

```
call.autoOffHook.x.enabled="1"
```

2. Specify the call recipient for automatic off-hook dialing.

```
call.autoOffHook.x.contact="<contact address>"
```

3. Optional: Set the calling protocol for the call.

```
call.autoOffHook.x.protocol="<SIP> or <H323>"
```

## Multiple Call Appearances

With multiple call appearances, users can place one call on hold, and switch to another call while both calls display on the phone.

This feature is one of several features associated with flexible call appearances. If you assign a registered line to multiple line keys, the default number of concurrent calls applies to all line keys.

## Configure the Number of Line Keys Per Registration

Configure the number of line keys allowed per phone line registration.

### Procedure

- » Set the number of line keys allowed for the registered line. You can set from 1 to 48 line keys per registered line. The default value is 1. Replace x with the desired line key value.

```
reg.x.lineKeys="<positive integer>"
```

## Configure the Maximum Number of Concurrent Calls Per Registration

Configure how many concurrent calls the phone allows per registered line.

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

You can set the value for the `reg.x.callsPerLineKey` parameter to a value higher than 1, for example, 3. After you set the value to 3, you can have three call appearances on line 1. By default, any additional incoming calls automatically go to voicemail.

If you set more than two call appearances, a call appearance counter displays at the top-right corner of the phone's screen.

### Procedure

- » Set the maximum number of concurrent calls for a single registration, *x*. This parameter applies to all line keys using registration *x*.

**Note:** If registration *x* is a shared line, an active call counts as a call appearance on all phones sharing that registration. This parameter overrides the setting for `call.callsPerLineKey`.

```
reg.x.callsPerLineKey="<positive integer>"
```

## Flexible Call Appearances

A number of features associate with flexible call appearances, including multiple line registrations, multiple line keys per registration, and multiple call appearances. Flexible line keys (FLK) support static busy lamp field (BLF) and enhanced feature keys (EFK).

The following table includes the following types of call appearances:

- **Registrations:** The maximum number of user registrations
- **Line Keys:** The maximum number of line keys
- **Line Keys Per Registration:** The maximum number of line keys per user registration
- **Calls Per Line Key:** The maximum number of concurrent calls per line key
- **Concurrent Calls (including Conference Legs):** The runtime maximum number of concurrent calls, and the number of conference participants minus the conference initiator.

Phone Model	Registration s	Line Keys	Line keys Per Registration	Calls Per Line Key	Concurrent Calls
CCX 400	34	48	48	24	24 (2)
CCX 500	34	48	48	24	24 (2)
CCX 600	34	48	48	24	24 (2)
CCX 700	34	48	48	24	24 (2)

## Busy Lamp Field

The busy lamp field (BLF) attendant console feature enhances support for phone-based monitoring.

When you enable BLF, a BLF line key icon displays on the phone screen for users monitoring remote phones. The BLF line key displayed indicates that BLF-related features are available.

The BLF feature enables the following user functions:

- Monitor the status of lines on remote phones
- Display remote party information
- Answer incoming calls to remote phones (directed call pickup)
- Park and retrieve calls

You can configure the following feature options for BLF:

- Line key labels
- Enhanced feature keys
- Call appearances display
- Call waiting audio notifications
- Caller ID information display
- One-touch call park and retrieve
- One-touch directed call pickup

This feature requires support from a SIP server, and the setup depends on the SIP server. When using BLF with a call server, the initial BLF subscription can receive large responses as the number of monitored resources increases. You may need to consult your SIP server partner or Poly channel partner to find out how to configure BLF feature options.





Typically, call servers support one of two methods of BLF configuration:

- Subscribing to a BLF resource list set up on your call server
- Entering BLF resources to a configuration file and the call server directs the requests to those BLF resources

## Busy Lamp Field Icons

The phone displays certain icons to indicate line status to the users.

### BLF icons

States	Line Icons
Monitored line is idle	
Monitored line is busy	
Monitored line is in hold	
Monitored line is unregistered	



---

**Note:** For information on how to manage calls to monitored phones, see the Handling Remote Calls on Attendant Phones section in *Technical Bulletin 62475: Using Statically Configured Busy Lamp Field with Polycom SoundPoint IP and VVX Phones* at the [Poly Online Support Center](#).

---

## Subscribe to a Busy Lamp Field Resource List on a Call Server

To subscribe a phone to a BLF resource list on a call server, access the call server and set up a list of monitored resources. Add a phone to the resource list by providing it with the call server address.

---

**Note:** When you set this parameter, the phone ignores individually addressed users configured by `attendant.resourceList` and `attendant.behaviors`.

---

### Procedure

1. Add a phone to the BLF resource list on the call server.

```
attendant.uri="<SIP URI>"
```

2. Optional: To ensure secure transmission, Poly recommends using Transmission Control Protocol (TCP) for BLF. Add TCP encryption to the attendant URI.

```
attendant.uri="<SIP URI>;transport=tcp"
```

## Configure a Busy Lamp Field Resource in the Configuration File

To specify BLF resources, enter the address of the BLF resource of the monitored contact, the label that displays beside the line key on the phone, and the resource's type.

A single SIP server has multiple registrations available. Your call server must support dialog to configure BLF resources using this method, even packages defined in [RFC 4235](#).

---

**Note:** This process covers the basic setup steps for a single BLF resource entry. See the *Poly CCX Parameter Reference Guide* for more information on the available configuration parameters.

---

You can configure up to 50 BLF resources.

### Procedure

1. Specify an index number for the new resource. Use any unused positive integers. The default index is 1.

```
attendant.reg="<index number>"
```

2. Specify the new resource address. Replace *x* with the resource's BLF index number.

```
attendant.resourceList.x.address="<SIP URI address>"
```

3. Optional: Configure the resource call signaling address if it's different than the one configured in `attendant.resourceList.x.address`. Replace *x* with the resource's BLF index number.

```
attendant.resourceList.x.callAddress="<SIP URI calling address>"
```

4. Configure a label to display adjacent to the associated line key. The default value is null. Replace *x* with the resource's BLF index number.

If you leave this value as null, the label displays as the user portion of the address set in `attendant.resourceList.x.address`.

```
attendant.resourceList.x.label="<label>"
```

5. Configure the resource type (the type of resource being monitored and the default action to perform when pressing the line key). Replace *x* with the resource's BLF index number.

The default type is normal for users' phones, but you can set the type as automata if the resource is something like a call orbit.

```
attendant.resourceList.x.type="<resource type>"
```

## Configure Key System Emulation

Key system emulation (KSE) enables one-touch call park and call retrieve from any phone within the user group.

You must enable busy lamp field (BLF) and enhanced call park features on the phone for KSE to work seamlessly.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

BLF and KSE are mutually exclusive. If you enable KSE, BLF is no longer available to monitor calls.

Key system emulation includes the following behavior:

- An audio notification plays on the phones in the user group when someone parks a call.
- A reminder tone continuously plays after a designated time interval if no one answers the call.
- There are no audio and reminder notifications for a self-parked call.
- The LED patterns and the line icons for a self-parked call are different from a call parked by other users in the group. This helps to differentiate between a self-parked call and a remote-parked call.
- The LED indicator turns solid red for a self-parked call and turns blinking red for a remote-parked call.

---

**Note:** Key system emulation is applicable to only the BroadSoft call control platform. You can't configure the yellow LED indicator for parked calls with an expansion module connected to a VVX phone.

---

### Procedure

1. Enable KSE.

```
attendant.keylineEmulation.enabled="1"
```

2. Enter the address for the registered line. Replace *x* with the desired line key value.

```
reg.x.address="<line registration>"
```

3. Enter the address for the SIP server accepting registrations. Replace x with the desired line key value. Replace y with the desired server key value.

```
reg.x.server.y.address="<server SIP URI>"
```

4. Enter the SIP URI for your attendant call server.

```
attendant.uri="<attendant server SIP URI>"
```

5. Specify an index number for the new BLF resource. Use any unused positive integers. The default index is 1.

```
attendant.reg="<index number>"
```

6. Set the call action behavior for an active call to Park.

```
attendant.CallAction="Park"
```

7. Enable the phone to display **Attendant Call Action** on the phone when you configure dynamic BLF on the phone.

```
attendant.callActionMenu.enabled="1"
```

8. Enable an audible call park notification for BLF-monitored lines.

```
feature.enhancedCallPark.allowBLFAudioNotification="1"
```

9. Configure a delay, in seconds, before the first call park notification plays, and then the delay, in seconds, that subsequent notifications play.

```
attendant.callParkBLFReminder.StartDelay="<delay in seconds>"
attendant.callParkBLFReminder.RepeatTime="<delay in seconds>"
```

10. Optional: Configure the call park notification ringtone. Replace x with the resource's BLF index number.

The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFReminderTone.inst.x.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.x.value="cs4"
se.pat.misc.callParkBLFReminderTone.inst.x.param="0"
se.pat.misc.callParkBLFReminderTone.inst.x.atten="0"
```

11. Optional: Configure the reminder ringtone. Replace x with the resource's BLF index number.

The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFAudioNotification.inst.x.type="chord"
se.pat.misc.callParkBLFAudioNotification.inst.x.value="cs4"
se.pat.misc.callParkBLFAudioNotification.inst.x.param="0"
se.pat.misc.callParkBLFAudioNotification.inst.x.atten="0"
```

## Related Links

[Configure Ringtones](#)

## Enable Instant Messaging

Send and receive instant text messages through your phone.

Support for instant messaging varies by call server. Consult your SIP server partner to find out if it supports this feature.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable instant messaging.

```
feature.messaging.enabled="1"
```

## Shared Lines

Configure phones to use shared lines and options available to phones on a shared line.

Some office layouts require numerous phones to ring for incoming calls. Shared lines are helpful for teams that handle a high volume of incoming calls, such as a customer service call center.

The following features are available with shared lines.

- **Line-Seize:** The answering phone has sole access to the incoming call. If the original answering phone places the call on hold, that call becomes available for any phone in that group to pick up. Line-seize is enabled by default.
- **Barge-In:** Configure phones within the group to enter an active call with other group phones.

### Related Links

[Configure LED Behavior for Held Calls on Shared Lines](#) on page 197

## Enable a Shared Line

Add a line to multiple phones for teams that benefit from a shared line, such as a call centers.

### Procedure

1. Specify the user or the user and host part of the registration SIP URI or the H.323 ID/extension. Replace x with the desired line key value.

The default is Null.

```
reg.x.address="<string>"
```

2. Set the call signaling type to Shared. Replace x with the desired line key value.

```
reg.x.type="shared"
```

## Shared Call Appearances

Shared call appearance (SCA) enables calls to display all call states—active, inactive, and hold—simultaneously on multiple phones in a group.

To enable SCA on your phone, you must obtain a shared line address from your SIP service provider or configure a shared line address on your phones. SCA is dependent on support from a SIP call server. Poly devices support SCA using the SUBSCRIBE-NOTIFY method specified in [RFC 6665](#).

---

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

---

## Configure Line-Seize on Shared Lines

Enable a shared line user to take control of a line before placing a call.

### Procedure

1. Configure the number of line-seize retries.  
The default is 10. The value range is 3 to 10.

```
voIpProt.SIP.lineSeize.retries="<value>"
```

2. Configure the line to immediately provide a dial prompt without waiting for the 200 OK registration message. Replace *x* with the registered line number.

```
reg.x.strictLineSeize="1"
```

3. Configure the line-seize timeout, in seconds. After the timeout period a seized line returns to an idle state. Replace *x* with the registered line number. Replace *y* with the desired server key value.  
The default is 30. The value range is 0 to 65535. A value of 0 means the line-seize doesn't expire.

```
reg.x.server.y.expires.lineSeize="<line-seize timeout>"
```

## Enable Barge-in on a Shared Line

Configure phones sharing a line to barge-in on active call.

### Procedure

- » Enable call barge-in on a specific line. Replace *x* with the registered line number.

```
reg.x.bargeInEnabled="1"
```

## Enable Call Diversion on Shared Lines

Enable users to divert incoming shared line calls to another line.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Enable call diversion for shared lines. Replace x with the registered line number.

```
divert.x.sharedDisabled="0"
```

**Enable Private Hold on Shared Lines**

Private hold enables users to hold a call, transfer a call, or initiate a conference call. The shared line displays as busy to other users sharing the line.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Enable private hold on the shared line. Replace x with the registered line number.

```
reg.x.enablePvtHoldSoftKey="1"
```

2. Enable the phone to send a re-INVITE to the server when setting up a conference on a shared line.

```
call.shared.exposeAutoHolds="1"
```

**SIP-B Automatic Call Distribution**

SIP-B automatic call distribution enables you to use your phones in a call center agent/supervisor role on a supported call server.

This feature supports automatic call distribution (ACD) agent availability, which depends on support from a SIP server.

**Enable ACD**

Enable the automatic call distribution (ACD) feature on a phone and registered lines.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Enable ACD login/logout.

```
feature.acdLoginLogout.enabled="1"
voIpProt.SIP.acd.signalingMethod="0"
```

2. Enable ACD login/logout on a registered line. Replace x with the registered line number.

```
reg.x.acd-login-logout="1"
reg.x.acd-agent-available="1"
```

## Simplify ACD State Controls

Configure the phone to hide the ACD softkeys and certain menu options to simplify how users interact with their phone.

The phone hides the following softkeys:

- **ASignIN**
- **ASignOut**
- **Available**

Enabling this parameter also hides menu items found in **Menu > Settings > Feature > ACD**.

### Procedure

- » Hide the ACD softkeys and menu options.

```
acd.simplifiedAgentStateControl="1"
```

## Configure Bridged Line Appearance

Connect calls and lines to multiple phones.

You must get a registered address dedicated for use with your call server provider. In the configuration files, shared lines configure bridged lines. Bridged line appearances don't support the barge-in feature.

---

**Important:** Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The methods you use vary with the SIP call server you use.

---

With bridged line appearance enabled, an active call displays simultaneously on multiple phones in a group. By default, the answering phone has sole access to the incoming call. If the answering phone places the call on hold, that call becomes available to all phones of that group. The call state, active, inactive, and held, displays on all of the phones.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Assign your registered address to the correct phone line and third-party name. Replace x with the desired line key value.

```
reg.x.address="<registered address>"
reg.x.thirdPartyName="<registered address>"
```

# PTT and Group Paging

Push-to-talk (PTT) and group paging enable users to transmit messages and announcements to configured and subscribed channels.

## PTT

PTT is a collaborative tool that enables users to exchange broadcasts to users subscribed to any of the 25 PTT channels, much like a two-way radio. Users transmit pages and PTT broadcasts using a handset, headset, or speakerphone. PTT broadcasts play on the speakerphone, handset, and headset.

In PTT mode, the phone behaves like a walkie-talkie. Users can broadcast audio to a PTT channel and recipients subscribed to that channel can respond to messages.

## Group Paging

Group paging enables users to send announcements to recipients subscribed to any of the 25 paging groups. Announcements play through the phone's speakerphone.

Administrators must enable paging before users can subscribe to a page group. You can specify the same IP multicast address in the parameter `ptt.address` for both PTT and group paging modes.

## Configure Phones to Receive Group Pages

Configure phones to receive pages sent from certain specified phone groups.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable group paging.

```
ptt.pageMode.enable="1"
```

2. Subscribe the phone to a specific group, and enable it to receive pages. Repeat these parameters for each group that you want the phone to receive pages from.

```
ptt.pageMode.group.x.subscribed="1"
```

3. Enable the phone to receive pages from subscribed groups.

```
ptt.pageMode.group.x.allowReceive="1"
```

4. Optional: Add a label to a specific group. Repeat this parameter for each group label.

```
ptt.pageMode.group.x.label="<string>"
```

5. Optional: Specify the group the phone uses for emergency pages. The default is group 25.

```
ptt.pageMode.emergencyGroup="<group number>"
```



## Configuring PTT

Configure the push-to-talk (PTT) settings and channels for your phone.

### Enable and Configure PTT

Enable push-to-talk (PTT) and configure how the phone uses available channels.

#### Procedure

1. Enable PTT on the phone.

```
ptt.pttMode.enable="1"
```

2. Subscribe the phone to a channel. Channel numbers are 1 to 25. Replace *x* with the number of the channel.

For example, channel 1 is `ptt.channel.1.subscribed`. All phones subscribed to the same channel can receive PTT messages from other phones subscribed on a channel.

```
ptt.channel.x.subscribed="1"
```

3. Set the default channel to use for PTT transmissions. Channel numbers are 1 to 25.

---

**Note:** The default emergency channel is 25.

---

```
ptt.defaultChannel="<channel number>"
```

4. Optional: Set the volume of the page without changing normal call volume. The default is -20.

```
ptt.volume="<number between -57 and 0>"
```

5. Optional: Enable the phone to play PTT messages while in an active call. By default, the PTT message plays after the user accepts it.

```
ptt.allowOffHookPages="1"
```

### Block a Phone from Sending Outgoing PTT Calls

Prevent a phone from sending out PTT calls on certain channels. Phones can still receive PTT messages on the channel.

This feature is useful for phones placed in common areas where users may need to hear PTT messages from a certain channel but not send any.

#### Procedure

- » Block the phone from sending PTT calls on a certain channel. Replace *x* with the number of the channel.

```
ptt.channel.x.allowTransmit="0"
```

## Add a Label to a PTT Channel

The channel's label displays on the phone when it sends or receives PTT calls.

### Procedure

- » Add a label to a channel. Replace x with the number of the channel. You can enter up to 64 characters in your label.

```
ptt.channel.x.label="<channel name>"
```

## Configure an Emergency PTT Channel

Specify a channel to use for emergency PTT messages.

---

**Note:** The default emergency channel is 25.

---

### Procedure

1. Specify the emergency PTT channel.

```
ptt.emergencyChannel="<channel number>"
```

2. Set the emergency page audio volume relative to the maximum speakerphone volume of the phone.

Positive values are louder than the maximum and negative values are quieter. The gain to use for emergency page/PTT is the maximum termination gain plus this parameter.

```
ptt.emergencyChannel.volume="<volume variance value>"
```

## Change the IP Multicast Address

Specify the IP multicast address for both PTT and group paging.

---

**Note:** The PTT and group paging features use an IP multicast address. If you want to change the default IP multicast address, make sure that the new address doesn't already have an official purpose as specified in the [IPv4 Multicast Address Space Registry](#).

---

For more information on PTT and group paging multicast packets, see the *Polycom UC Software PTT/Group Paging Audio Packet Format Engineering Advisory 70568* at the [Poly Online Support Center](#).

### Procedure

- » Enter the new multitask IP address.

```
ptt.address="<IP address>"
```

## Enable SIB-B Group Call Pickup

This feature enables users to pick up incoming calls to any phone within a predefined group of phones, without dialing the extension of another phone.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

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.

### Procedure

- » Enable SIP-B group call pickup.

```
feature.groupCallPickup.enabled="1"
```

## Intercom Calls

When users place an intercom call, the dialed contact's phone automatically answers it.

Users can quickly pass information to others without interrupting their task to answer the incoming call. An example of useful intercom calls is to notify users that there's another call on hold for them.

### Enable Intercom Calls

Enable the phone to place intercom calls.

This is a server-independent feature provided the server doesn't alter the Alert-Info header sent in the INVITE.

### Procedure

1. Enable intercom calls.

```
feature.intercom.enable="1"
```

2. Add the **Intercom** icon to the phone's **Home** screen.

```
homeScreen.intercom.enable="1"
```

3. Optional: Enter the string for the Alert-Info header.

You can use the following special characters: @, -, \_, or . . The default is *Intercom*.

```
voIpProt.SIP.intercom.alertInfo="<alphanumeric string>"
```

## Creating a Custom Intercom Soft Key

Use a custom intercom softkey to initiate intercom calls directly to a specified contact using enhanced feature keys (EFKs).

The **Intercom** softkey displays on the phone by default. You don't have to disable the default **Intercom** softkey to create a custom softkey. You can create an intercom action string for a custom softkey in one of the following ways:

- `<number>$Tintercom$`

A T-type macro that enables you to specify a direct intercom button that always calls the number you specify in `<number>`. This doesn't require additional input.

- `$FIntercom$`

An F-type macro that behaves as a custom Intercom softkey. The softkey opens the **Intercom** dial prompt to place an intercom call by entering the destination's digits and using a speed dial or BLF button.

## Configure E.911

The Enhanced 911 (E.911) feature enables the phone to obtain location information to share with responders when users dial 911 to report an emergency. This ensures that the operator dispatches emergency services to the correct location.

The phones obtain location information from:

- LLDP-MED
- DHCP via option 99
- LIS compliant with RFC 5985

The steps in this process accommodate most configurations. For more information on E.911 configuration parameters, see the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable the E.911 feature.

---

**Note:** The INVITE sent for emergency calls from the phone includes the geolocation header defined in RFC 6442 and PIDF presence element as specified in RFC3863 with a GEOPRIV location object specified in RFC4119 for in OpenSIP environments.

---

```
feature.E911.enabled="1"
```

2. Optional: Configure the source of the phone's location information. You have the following options:
  - LLDP (default) – Use the network switch as the source of location information.
  - LIS - Use the location information server as the source of location information.
  - DHCP - Use DHCP as the source of location information.

```
locInfo.source="<location information source>"
```

# Configuring Phone Settings

---

## Topics:

- [Multiple Line Registrations](#)
- [Local Digit Map](#)
- [User Profiles](#)
- [Presence Status](#)
- [Power Saving on CCX Phones](#)
- [Microphone Mute](#)
- [Enable Persistent Call Volume](#)
- [Disable DTMF Tones](#)
- [Audible Notifications and Sounds](#)

Customize your phone using various applications and keysets.

## Multiple Line Registrations

Poly phones can have multiple line registrations. When multiple registrations are available, users can select which registration to use for certain features, including which registration to use for outgoing calls or when initiating new instant messages.

Each registration requires an address or phone number.

---

**Note:** You must use a unique address or a phone number for each registration. Using the same address or phone number for multiple registrations might cause unexpected behavior.

---

The maximum number of registrations vary by phone and are listed in the following table.

**Maximum Number of Registrations Per Phone**

Phone Model Name	Maximum Registrations
CCX 400	34
CCX 500	34
CCX 600	34
CCX 700	34

## Local Digit Map

The local digit map feature assists with off-hook dialing and helps the phone conform to a dial plan.

Digit maps consist of a single string or a list of strings. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of [RFC 3435](#).

When dialing a number, the digit map behavior is based on the following:

- Any string of a digit map matches: The phone places the call automatically.
- No string matches: You can specify the phone's behavior.
- The number ends with #: You can specify the phone's behavior.

You can specify digit map timeout. This is the time between the caller dialing a number and the phone placing the call.

## Configure a Local Digit Map

Specify the digit map used for the dial plan.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

The default digit map is as follows:

```
[2-9]11|0T|+011xxx.T|0[2-9]xxxxxxxx|+1[2-9]xxxxxxxx|[2-9]xxxxxxxx|
[2-9]xxxT
```

### Procedure

- » Configure the local digit map according to your dial plan.

```
dialplan.digitmap="<digit map string>"
```

## Change the Dialing Timeout

Specify a timeout in seconds for each segment of the digit map. After a user presses a key, the phone waits this many seconds before matching the digits to a dial plan and dialing the call.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Specify the timeout, in seconds, for the digit map. Provide the timeout in a string with positive integers separated by a vertical bar (|).

```
dialplan.digitmap.timeOut="< n | n | n | n | n | n >"
```

## Change the International Dialing Prefix

By default, users enter a plus (+) symbol before dialing an international phone number to identify to the switch that they placed an international call. Change the international call prefix to 0 instead of the plus symbol.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Set 0 as the international call prefix.

```
call.internationalPrefix.key="1"
```

2. Require your local country's exit code to place an international call.

```
call.internationalDialing.enabled="0"
```

## User Profiles

Users can access their personal phone settings from any phone on the network with user profiles.

Remote and mobile workers who don't have a dedicated work space to conduct their business in more than one location can benefit from this feature. Offices with a common conference phone where multiple users need to access their personal settings can also use user profiles.

---

**Note:** You can configure all company phones so that anyone can call authorized and emergency numbers when not logged in to a phone. For more information, see `dialplan.routing.emergency.outboundIdentity`.

---

Users can change their own password on any phone on the network. If a user changes any settings while logged into a phone, the settings save and display the next time that user logs in to another phone. When the user logs out, the corresponding user options clear from the device until someone enables the user profile-related configuration on the phone again.

## Enable Multiple User Profiles on the Phone

Configure the phone so that it can accept multiple user profiles.

### Procedure

- » Enable the phone to accept multiple users other than the default user.

```
prov.login.defaultOnly="1"
```

## User Profile Authentication

Authenticate users with phone-based or server-based authentication methods.

Phone-based authentication authenticates credentials entered by the user against the credentials in the `<user>.cfg` file. Server-based authentication passes user credentials to the provisioning server for authentication.

## User Profile Server Authentication

Enable users to log in to any phone on the network with their user profile.

To enable server authentication, set up user accounts on the provisioning server so users can authenticate their phones by entering correct server credentials.

The phone downloads log files (`app.log` and `boot.log`) from the generic profile on the provisioning server regardless of user logins.

## Enable the Phone to Use Server Authentication

Configure the phone to use its provisioning server for user authentication.

Enable the phone to use multiple user profiles.

### Procedure

- » Enable server authentication.

```
prov.login.useProvAuth="1"
```

## Create a Generic User Profile for Server Authentication

Create a user profile to use with a provisioning server or locally on a shared phone.

If you enable server authentication of user profiles, the following parameters don't apply:

- `prov.login.defaultUser`
- `prov.login.defaultPassword`
- `prov.login.defaultOnly`
- `prov.login.localPassword`
- `prov.login.localPassword.hash`

### Procedure

1. On the server, create an account and directory for the generic profile.  
`Generic_Profile`
2. In the directory, create a configuration file for the generic profile the phone uses by default.  
`genericprofile.cfg`
3. Open the generic profile configuration file.
4. Include registration and server details, and set the following phone feature parameters:

```
prov.login.enabled="1"
prov.login.useProvAuth="1"
prov.login.persistent="1"
```



---

**Note:** If you enable `prov.login.enabled` and don't enable `prov.login.useProvAuth`, the phone authenticates users by matching with credentials you store in the `<user>.cfg` user configuration file.

---

5. Save the generic profile configuration file.
6. Create a primary configuration file `00000000000000000000.cfg` for all the phones or a `<MACAddress>.cfg` for each phone, and add the generic profile configuration file to the **CONFIG\_FILES** field.
7. Set the provisioning server address and provisioning server username and password credentials for the generic user account on the phone at **Settings > Advanced > Provisioning Server**.

The following override files upload to the generic profile directory:

- Log files
- Local interface settings
- System web interface settings
- Call logs
- Contact directory file

## Create User Profiles for Server Authentication

Create user profiles in the **Home** directory of each user with a specific configuration file that you store on the provisioning server. User profiles have unique names as well as specific files such as settings, directory, and call lists.

When a user logs in with credentials, the phone downloads the user profile from the provisioning server. When the user logs out, the phone downloads the default user profile using the generic credentials.

The following override files upload to the generic profile account on the server:

- Log files
- System web interface settings

The following override files upload to the user profile account on the server:

- Local interface settings
- Contact directory file

## Procedure

1. On the server, create an account and a directory for each user.  
`User1` and `User2`
2. In each user directory, create a configuration file for each user that contains the user's registration details and feature settings.  
`User1.cfg` and `User2.cfg`
3. Open the user profile configuration file.
4. Enable the user profile.

```
prov.login.enabled="1"
```

5. Optional: Set the user's default password. The default is 123 until the user changes it.

```
prov.login.localPassword="<string>"
```

6. Save the user profile configuration file.

## User Profile Phone Authentication

Enable multiple users to log in to one phone.

Users can provide their credentials on the phone without using a server. This is helpful for shared phones in common areas without a connection to a provisioning server.

### Create a User Configuration File

Create a configuration file for each user that you want to enable to log in to the phone.

Some things to note about user configuration files:

- If users update their password or other user-specific settings on the phone, the updates save to `<user>-phone.cfg`, not `<MACaddress>-phone.cfg`.
- If users update their contact directory while logged in to a phone, the updates save to `<user>-directory.xml`.
- Directory updates display each time users log in to a phone. For certain phones, the `<user>-calls.xml` contains an up-to-date call list history. This list updates each time users log in to their phone.

The following list provides configuration parameter precedence (from first to last) for a phone with the user profile feature enabled:

1. `<user>-phone.cfg`
2. System web interface
3. Configuration files listed in the primary configuration file (including `<user>.cfg`)
4. Default values

### Procedure

1. On the provisioning server, create a user configuration file for each user. Specify the user's login ID in the name of the file.  
If the user's login ID is `user100`, name the user configuration file `user100.cfg`.
2. Open the user configuration file.
3. In each `<user>.cfg` file, you must add and set values for the user's login password.
4. Optional: Add and set values for any user-specific parameters you want to add:
  - Registration details, such as the number of lines the profile displays and line labels.
  - Feature settings, such as microbrowser settings.

**Note:** If you add optional user-specific parameters to `<user>.cfg`, only add parameters that don't force the phone to restart or reboot to complete the update.

5. Save the user configuration file.

## Convert a Phone to User-Based Deployment

Configure a phone in a deployment that depends on user login instead of a traditional phone deployment.

### Procedure

1. Copy the `<MACaddress>-phone.cfg` file to `<user>-phone.cfg`.
2. Copy the `phoneConfig<MACaddress>.cfg` file to `<user>.cfg`.

## Create Default Credentials and a Profile for a Phone

Create a default user profile for the phone to automatically log in to each time a user logs out or the phone restarts.

The default user profile is like any other user profile, except it's designated as the phone's own profile. When the phone logs in using the default login credentials, a default phone profile displays. Users retain the option to log in and view their personal settings.

---

**Important:** Poly recommends that you create a single default user password for all default user profiles.

---

### Procedure

- » Enter the default user login credentials.

```
prov.login.defaultUser="<Default User Profile Username>"
prov.login.defaultPassword="<Account User Profile Password>"
```

## Require a User Login

Configure the phone to require a user to log in to the phone to use it.

### Procedure

- » Require a user to log in to use the phone.

```
prov.login.required="1"
```

## Mask the User Password Entry

Use pound signs (#) to mask the user's password on the phone's screen as they enter it.

Password entries on the phone's screen to prevent prying eyes from seeing user's password. For example, password displays as #####.

### Procedure

- » Mask the user's password entry with pound signs.

```
prov.login.localPassword.hasheds="1"
```

## Enable User Login Persistence

Enable the phone to maintain the last user logged in following a phone reboot.

### Procedure

- » Enable the phone to retain the last user login when it reboots.

```
prov.login.persistent="1"
```

## Presence Status

Enable users to monitor the status of other remote users and phones. Poly phones support a maximum of 64 buddies.

By adding remote users to a buddy list, users can monitor changes in the status of remote users in real time or they can monitor remote users as speed-dial contacts. Users can also manually specify their status to override or mask automatic status updates to others and can receive notifications when the status of a remote line changes.

### Enable Presence Status to Display on the Phone

Enable phone users to see the presence of other users.

#### Procedure

1. Enable presence status to display on the phone. The **MyStatus** and **Buddies** softkeys display on the phone.

```
feature.presence.enabled="1"
```

2. Set the line used for presence. Select lines 1 through 34. The phone's default line is line 1.

```
pres.reg="<line number>"
```

### Disable Presence Softkeys

Remove the **MyStatus** and **Buddies** softkeys from the phone's local interface to prevent users from manually updating their presence.

#### Procedure

- » Remove the **MyStatus** and **Buddies** softkeys.

```
pres.idleSoftkeys="0"
```

## Power Saving on CCX Phones

The power-saving feature automatically turns off the phone's LCD display when it's not in use. Power saving is enabled by default.

Configure the following power-saving options for the phone:

- Power-saving during workdays
- Power-saving during off days
- Idle or inactivity time after which the phone enters power-saving mode

---

**Note:** When you enable power-saving mode and the phone is in low-power state, the red LED indicator slowly blinks to show that the phone still has power.

---

**Related Links**

[Disable Message Waiting Indicator in Power Saving Mode](#) on page 198

**Configure Power Saving**

Configure power-saving mode for office hours and off hours on your phone.

The phone remains in office hours mode until it completes the duration, after which it enters off hours mode. You configure office hours on a certain workday by setting a start hour and duration in hours. You can also configure the allowed period of idle time in minutes before the system enters power-saving mode.

For more information on permitted values, see the *Poly CCX Business Media Phone Parameter Reference Guide*.

**Procedure**

1. Configure office hours for each workday.

Repeat this step for each workday, as set by the value for *<Day>*. For example, Monday.

```
powerSaving.officeHours.startHour.<Day>="<Hour value>"
powerSaving.officeHours.duration.<Day>="<Hour value>"
powerSaving.idleTimeout.officeHours="<Minute value>"
```

2. Configure the allowed period of idle time in minutes before the phone enters power-saving mode during off hours.

When the system isn't in office hours mode, it's in off hours mode.

```
powerSaving.idleTimeout.offHours="<Minute value>"
```

3. Configure how long user input, such as touching the screen or pressing a button, extends the period of idle time in minutes.

Incoming calls, whether the user answers them or not, resets the idle timeout. This applies for both office hours and off hours.

```
powerSaving.idleTimeout.userInputExtension="<Minute value>"
```

**Disable Power Saving**

Disable power saving so the phone never enters a low-power state.

**Procedure**

- » Disable power saving on the phone.

```
powerSaving.Enable="0"
```

# Microphone Mute

Microphone mute is an embedded feature on your phone, and you can't configure or disable it. However, you can configure supporting features related to muting the microphone.

## Enable Microphone Mute/Unmute Alert

Configure the phone to play a tone when a user mutes or unmutes the microphone.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable the microphone mute alert.

```
se.touchFeedback.enabled="1"
```

## Configure Mute Reminder Alert Interval

Set the microphone mute reminder alert interval to play tones at a specified amount of time to remind users that their microphone is muted.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Configure the interval, in seconds, to play a tone while the phone is muted. Enter a value between 5 and 3600.

```
call.mute.reminder.period="<interval period in seconds>"
```

## Disable Microphone Mute Persistence

By default, the microphone mute status is persistent. If an active call ends with the microphone muted, it remains muted for subsequent calls until a user manually changes it. Disable microphone mute persistence so that the microphone unmutes when an active call ends.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Disable microphone mute persistence.

```
feature.persistentMute.enabled="0"
```

## Enable Persistent Call Volume

By default, the phone resets the call volume to the default level for each new call. Configure the phone to retain the call volume set during a call for subsequent calls.

In some countries, regulations state that a phone's receiver volume must reset to a nominal level for each new call. Make sure any changes you make here don't violate local laws or regulations.

Set `device.set="1"`.

Transmit levels are fixed according to the TIA/EIA-810-A standard.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Set any or all of these parameters for particular devices to enable the call volume to persist between calls.

### Procedure

1. Configure the handset volume to persist between calls.

```
voice.volume.persist.handset="1"
```

2. Configure the speakerphone volume to persist between calls.

```
voice.volume.persist.handsfree="1"
```

3. Configure USB headset volume to persist between calls.

```
voice.volume.persist.usbHeadset="1"
```

4. Configure volume for a connected Bluetooth headset to persist between calls.

```
voice.volume.persist.bluetooth.headset="1"
```

## Disable DTMF Tones

Prevent the phone from playing DTMF tones through the speakerphone

The phone can encode DTMF tones using the active voice codec or using [RFC 2833](#) compatible encoding. The remote endpoints capabilities determine the coding format decision. The phone generates [RFC 2833](#) tones but doesn't regenerate or use DTMF tones received from the remote end of the call.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

DTMF tones are encoded in the Real-time Transport Protocol (RTP) stream by default. When you disable `tone.dtmf.viaRtp`, DTMF isn't encoded in the RTP stream.

**Procedure**

- » Disable DTMF tones from playing through the speakerphone.

```
tone.dtmf.chassis.masking="1"
tone.dtmf.viaRtp="0"
```

## Audible Notifications and Sounds

Configure how audible notifications and sounds play on your phones. Audible notifications and sounds play through the speakerphone by default.

Audible notifications include call progress tones and ringtones, as well as the sound effect patterns or files they play.

### Set the Audible Notification and Sound Output

Determine where the audible notifications and sounds play during a call.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Set the output location for audible notifications and sounds.
  - chassis (Default) - All notifications and sounds play through the speakerphone, regardless of the active location.
  - handset - All notifications and sounds play through the handset when it's in use. If it's not in use, notifications and sounds play through the speakerphone.
  - headset - All notifications and sounds play through an active headset. If the headset is not active, no notifications or sounds play.
  - active - All notifications and sounds play through the handset or headset if they are in use. Otherwise, notifications and sounds play through the speakerphone.

```
se.destination="<value>"
```

### Disable the Phone's Welcome Sound

Disable the welcome sound on your phone.

**Procedure**

- » Disable the welcome sound.

```
up.welcomeSoundEnabled="0"
```



## Disable Audible Notifications and Sounds

Disable audible notifications and sounds so they don't play on your phones.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

- » Disable audible notifications and sounds.

**Note:** Disabling this parameter doesn't affect the voicemail stutter dial tone configured in `se.stutterOnVoiceMail`.

```
se.appLocalEnabled="0"
```

## Disable the Voicemail Stutter Dial Tone

By default, phones use a stuttered dial tone to indicate a user has voicemail messages. Configure the phone to use a normal dial tone instead.

### Procedure

- » Disable the voicemail stutter dial tone.

```
se.stutterOnVoiceMail="0"
```

## Ringtones and Visual Incoming Call Indicators

Use ringtones to define a simple ring class that the phone applies based on credentials carried within the network protocol.

The ring class includes parameters such as call-waiting and ringer index (if appropriate), and it can use one of the following ring types:

- Ring: Plays an audible ring pattern or call waiting indication.
- Visual: Provides a visual-only indication of an incoming call.
- Answer: Auto-answers incoming calls when no incoming calls are in progress. Auto-answer continues to work during outgoing calls.
- Ring-answer: Provides auto-answer on an incoming call after a certain number or rings.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

## Supported Ring Classes

The following table provides the available ring classes to create or assign ringtones.

### Ring Classes

Ring Class	Definition
Default	The phone rings for all call types.
Visual	The phone's LED flashes to indicate an incoming call.
AnswerMute	The phone mutes the microphone when you answer a call.
AnswerAuto	The phone auto answers incoming calls.
RingAnswerMute	The phone rings audibly and answers with mute active.
RingAnswerAuto	The phone rings audibly and auto-answers the call.
Internal	The phone rings for internal calls.
External	The phone rings for external calls.
Emergency	The phone rings for emergency calls.
Precedence	
Splash	
Custom y	Link to a custom ringtone uploaded to the phone. y can be any value from 1 to 17.

### Related Links

[Call Progress Tone Patterns](#) on page 150

[Configure the Call Waiting Tone](#) on page 146

[Assign a Distinctive Ringtone Based on Alert-Info Headers](#) on page 147

## Disable Ringtones

Disable your phones from playing ringtones.

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

- » Disable ringtones on your phones.

```
se.rt.enabled="0"
```

## Disable the Ability to Change the Ringtone

Don't allow users to modify the predefined ringtone from the phone's local interface.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Disable the ability for users to modify the ringtone through the local interface.

```
se.rt.modification.enabled="0"
```

## Configure the Call Waiting Tone

Configure the call waiting tone used for the specified ring class.

The call waiting pattern must match those defined in the call progress tone pattern list.

### Procedure

- » Set the call waiting tone type. Replace *<ringClass>* with the desired ring class.
  - callWaiting (default)
  - callWaitingLong
  - precedenceCallWaiting

```
se.rt.<ringClass>.callWait="<tone pattern>"
```

### Related Links

[Supported Ring Classes](#) on page 145

[Call Progress Tone Patterns](#) on page 150

## Distinctive Ringtones

Apply a distinctive ringtone to a specific contact, type of call, or registered line, including internal or external calls.

You can set up distinctive ringing using more than one method. However, the phone uses the highest priority method based on the following:

- Assign ringtones to specific contacts in the contact directory. This option is the first and highest in priority.
- Use parameters to map calls to specific ringtones based on call server settings. This option requires server support and is second in priority.
- Users can select a ringtone for each registered line on the phone from the phone's local interface. This option has the lowest priority.

### Assign a Distinctive Ringtone to a Registered Line

Assign a specific ringtone to a line to identify calls received from a specific line.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Assign a ringtone directly to a registered line. Replace *x* with the registered line number.

```
reg.x.ringType="<ringtone name>"
```

**Related Links**

[Ringtone Patterns](#) on page 151

**Assign a Distinctive Ringtone Based on Alert-Info Headers**

Use parameters to map calls to specific ringtones based on Alert-Info headers and call server settings. This option requires server support.

**Procedure**

1. Specify a ring class to apply when the phone compares the Alert-Info header from INVITE requests to parameters as specified. Replace *x* with the registered line number.

```
voIpProt.SIP.alertInfo.x.class="<ring class>"
```

2. Specify a ringtone for a single registered line using a string to match the Alert-Info header in the incoming INVITE request. Replace *x* with the registered line number.

The string has a max length of 128 characters.

```
voIpProt.SIP.alertInfo.x.value="<Alert-Info header string>"
```

**Related Links**

[Supported Ring Classes](#) on page 145

**Sound Effects**

Customize the audio sound effects that play for incoming calls and other alerts. Patterns, sequences of chord-sets, silence periods, and wave files define sound effects.

The phones use synthesized tones or sampled audio files with `.wav` files that you download from the provisioning server or internet. Phones support the following sampled audio `.wav` file formats:

- Mono 8 kHz G.711 u-Law - Supported on all phones
- Mono G.711 (13-bit dynamic range, 8-khz sample rate)
- G.711 A-Law - Supported on all phones
- Mono L16/8000 (16-bit dynamic range, 8-kHz sample rate) - Supported on all phones
- Mono 8 kHz A-law/mu-law - Supported on all phones
- L8/16000 (16-bit, 8 kHz sampling rate, mono) - Supported on all phones
- Mono L16/16000 (16-bit dynamic range, 16-kHz sample rate)
- L16/16000 (16-bit, 16 kHz sampling rate, mono - Supported on all phones

Phones store ringtone files in volatile memory that allows a maximum size of 600 KB (614,400 B) for all ringtones.

## Add a Sample Audio File

Add a link to a sample audio file (SAF) to use as a ringtone.

---

**Note:** If you use TFTP, the URL must be in the following format: `tftp://<host>/<pathname><filename>`. For example: `tftp://somehost.example.com/sounds/example.wav`.

---

### Procedure

- » Enter the filename and file path or URL. Include the name of the file and the `.wav` extension in the path. Replace `x` with the custom audio file's filename.
  - Null (Default) - The phone uses a built-in file.
  - `filepath` - Location in the provisioning server where the audio file is located. During startup, the phone attempts to download the file.
  - `URL` - Location of the audio file on the internet. During startup, the phone attempts to download the file. The URL must be compliant with RFC 1738 and go to an HTTP, FTP, or TFTP `.wav` file resource.

```
saf.x="<string>"
```

## Configure Sound Effect Patterns

Specify the sound effects, patterns, and category that play for different phone functions.

Note the following when configuring these parameters:

- `x` is the pattern name.
- `y` is the instruction number.
- Both `x` and `y` must be sequential.
- `cat` is one of the following pattern categories:
  - `callProg` - Call progress tones
  - `ringer` - Ringtones
  - `misc` - Miscellaneous tones

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Set the sound effect name. Replace `cat` with the pattern category name. Replace `x` with the pattern name. Replace `y` with the instruction number.
  - `sample`
  - `chord`
  - `silence`
  - `branch`

The default is Null. The maximum string length is 255 characters.

```
se.pat.cat.x.inst.y.type="<string>"
```

2. Set the sound effect instruction. Replace *cat* with the pattern category name. Replace *x* with the pattern name. Replace *y* with the instruction number.

- sampled - Sampled audio file number
- chord - Type of sound effect
- silence - Silence duration in ms
- branch - Number of instructions to advance

The default is Null. The maximum string length is 50 characters.

```
se.pat.cat.x.inst.y.value="<string>"
```

## Sound Effect Pattern Examples

Specify the sound effects, patterns, and category that play for different phone functions.

Patterns use a simple script language that enables you to string different chord sets or .wav files together with periods of silence. The script language uses the instructions shown in the following table.

### Sound Effect Pattern Instruction Types

Instruction	Definition	Example
sampled ( <i>n</i> )	Play sampled audio file <i>n</i>	se.pat.misc.custom1.inst.1.type="sampled" - Sampled audio file instruction type se.pat.misc.custom1.inst.1.value="2" - Specifies sampled audio file 2
chord ( <i>n</i> )	Play chord set <i>n</i>	se.pat.callProg.busyTone.inst.2.type="chord" - Chord set instruction type se.pat.callProg.busyTone.inst.2.value="busyTone" - Specifies sampled audio file busyTone
silence ( <i>d</i> )	Play silence for <i>d</i> milliseconds  This option doesn't mute Rx audio.	se.pat.callProg.bargeIn.inst.3.type="silence" - Silence instruction type se.pat.callProg.bargeIn.inst.3.value="300" - Specifies silence lasts 300 milliseconds
branch ( <i>n</i> )	Advance <i>n</i> instructions and execute that instruction  <i>n</i> must be negative and must not branch beyond the first instruction.	se.pat.callProg.alerting.inst.4.type="branch" - Branch instruction type se.pat.callProg.alerting.inst.4.value="-2" - Step back 2 instructions and execute that instruction

## Call Progress Tone Patterns

Poly phones play call progress tones including busy signals, ringback sounds, and call waiting tones.

The built-in call progress tones match standard North American tones. If you want to customize your phone's call progress tones to match the standard tones in your region, contact [Poly Technical Support](#).

The following table lists the call progress patterns and their descriptions.

### Call Progress Tones

Call Progress Pattern	Description
bargeIn	Barge-in tone
busyTone	Busy tone
callWaiting	Call waiting tone
callWaitingLong	Call waiting tone long (distinctive)
confirmation	Confirmation tone
dialTone	Dial tone
howler	Howler tone (off-hook warning)
intercom	Intercom announcement tone
msgWaiting	Message waiting tone
precedenceCallWaiting	Precedence call waiting tone
precedenceRingback	Precedence ringback tone
preemption	Preemption tone
precedence	Precedence tone
recWarning	Record warning
reorder	Reorder tone
ringback	Ringback tone
secondaryDialTone	Secondary dial tone
stutter	Stuttered dial tone
alerting	Alerting

### Related Links

[Supported Ring Classes](#) on page 145

[Configure the Call Waiting Tone](#) on page 146

## Ringtone Patterns

The following table lists the ring pattern names and their default descriptions.

Sampled audio files 1 to 10 all use the same built-in file unless you replace that file with a downloaded file.

### Ringtone Pattern Names

Parameter Name	Ringtone Name	Description
ringer1	Silent Ring	Silent ring
		<b>Note:</b> Silent ring provides a visual indication of an incoming call, but no audio indication.
ringer2	Low Trill	Long single A3 Db3 major warble
ringer3	Low Double Trill	Short double A3 Db3 major warble
ringer4	Medium Trill	Long single C3 E3 major warble
ringer5	Medium Double Trill	Short double C3 E3 major warble
ringer6	High Trill	Long single warble 1
ringer7	High Double Trill	Short double warble 1
ringer8	Highest Trill	Long single Gb3 A4 major warble
ringer9	Highest Double Trill	Short double Gb3 A4 major warble
ringer10	Beeble	Short double E3 major
ringer11	Triplet	Short triple C3 E3 G3 major ramp
ringer12	Ringback-style	Short double ringback
ringer13	Low Trill Precedence	Long single A3 Db3 major warble Precedence
ringer14	Ring Splash	Splash
ringer15	N/A	Sampled audio file 1
ringer16	N/A	Sampled audio file 2
ringer17	N/A	Sampled audio file 3
ringer18	N/A	Sampled audio file 4
ringer19	N/A	Sampled audio file 5
ringer20	N/A	Sampled audio file 6
ringer21	N/A	Sampled audio file 7
ringer22	N/A	Sampled audio file 8



Parameter Name	Ringtone Name	Description
ringer23	N/A	Sampled audio file 9
ringer24	N/A	Sampled audio file 10

### Related Links

[Assign a Distinctive Ringtone to a Registered Line](#) on page 146

## Miscellaneous Sound Effect Patterns

The following table lists the miscellaneous sound effect patterns and their descriptions.

### Miscellaneous Sound Effect Pattern Parameters

Parameter Name	Pattern Name	Description
instantmessage	instant message	New instant message
localHoldNotification	local hold notification	Local hold notification
messageWaiting	message waiting	New message waiting indication
negativeConfirm	negative confirmation	Negative confirmation
positiveConfirm	positive confirmation	Positive confirmation
remoteHoldNotification	remote hold notification	Remote hold notification
welcome	welcome	Welcome (boot up)
callParkBLFReminderTone	call Park BLF Reminder Tone	Cadence of parked call reminder tone
callParkBLFAudioNotification	call Park BLF Audio Notification	Cadence of parked call audio notification

# Third-Party Servers

---

## Topics:

- [Microsoft Exchange Integration](#)
- [Ribbon Communications Server](#)
- [BroadSoft BroadWorks Server](#)
- [Enable uaCSTA on a Dedicated Line](#)

This section provides information on configuring your phones with features from third-party servers.

## Microsoft Exchange Integration

Integrate your OpenSIP phones with a Microsoft Exchange server to join meetings, make calls to Outlook contacts, and access Outlook calendars.

### Related Links

[Enable Exchange Call Logs](#) on page 183

## Configuring the Microsoft Exchange Server

Configure the phone to use Microsoft Exchange server services on your phone.

These options are available once you connect to a Microsoft Exchange server:

- **Visual Voicemail:** Enable unified messaging and enable messages to play on the phone for each user.
- **Synchronizing Call Logs:** Enable the option to save calls logs to each user's conversation history in Outlook.
- **Outlook Address Book Search:** Enables users to search their Outlook contacts from the phone.

After you configure the Exchange server and features, users can log into their accounts in the **Basic** settings menu on the phones local interface. Users can also log in from the system web interface under **Settings > Applications > Exchange Sign in**.

## Manually Connect to a Microsoft Exchange Server

Manually configure the phone to use a specific Microsoft Exchange server address.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

By default, the phone uses autodiscovery to determine the Microsoft Exchange server address, which relies on local DNS records and login domain information. The phone prioritizes the setting in `exchange.server.url`, even if you keep autodiscovery enabled.

**Procedure**

- » Enter the Microsoft Server address.

```
exchange.server.url="<server address>"
```

**Enable Exchange Voicemail**

Configure your OpenSIP phone to access voicemails left for a Microsoft Exchange account.

Set `feature.exchangeCalendar.enabled="1"`.

**Procedure**

- » Enable Exchange Voicemail.

```
feature.exchangeVoiceMail.enabled="1"
```

**Enable Exchange Call Logs**

Enable an OpenSIP phone to synchronize with the logged in user's Exchange account.

Set `feature.exchangeCalendar.enabled="1"`.

**Procedure**

- » Enable the Exchange call log feature.

```
feature.exchangeContacts.enabled="1"
```

**Configure Exchange Address Book Service**

Enable an OpenSIP phone to search with the logged in user's Exchange address book.

Set `feature.exchangeCalendar.enabled="1"`.

**Procedure**

1. Enable the Exchange Skype for Business address book service.

```
feature.lync.abs.enabled="1"
```

2. Optional: Set the maximum number of contacts displayed when searching through the Exchange address book. The default is 12 results.

```
feature.lync.abs.maxResult="<integer>"
```

3. Optional: Set the phone's access to the Exchange address book to read only. This prevents users from making any changes to their address book from the phone.

```
feature.lync.abs.maxResult="<integer>"
```

## Microsoft Exchange Calendar

For phones connected to an Exchange calendar, a **Calendar** icon displays on the phone **Home** screen.

Users can view and join Outlook calendar events directly from the phone. The phone displays the day and meeting view for scheduled events. However, the phone doesn't support the ability to schedule calendar events or view email from the phone.

### Provision a Microsoft Exchange Calendar

Enable a phone to access a Microsoft Exchange Calendar using a configuration file.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

#### Procedure

1. Enable the Microsoft Exchange Calendar feature.

```
feature.exchangeCalendar.enabled="1"
```

2. Enter the Microsoft Exchange server URL.

```
exchange.server.url="<Exchange server address>"
```

### Enable Microsoft Exchange Calendar Using the System Web Interface

Use the system web interface to configure one phone at a time with the Microsoft Exchange calendar.

#### Procedure

1. Log in to the system web interface using admin credentials.
2. Go to **Settings > Applications > Exchange Applications**.
3. In the **Exchange Calendar** field, select **Enable**.
4. Enter the exchange web services URL using a Microsoft Exchange Server URL.  
`https://<mail.com>/ews/exchange.asmx`
5. Select **Save**.
6. Select **Yes**.

The **Calendar** icon displays on the phone screen.

### Verify the Microsoft Exchange Integration

After you configure your phone for Microsoft Exchange services, confirm that the services work properly.

Integrate the phone with the Microsoft Exchange server.

#### Procedure

- » On the phone's local interface, go to **Settings > Status > Diagnostics > Warnings**.  
If the phone doesn't display any warnings, then the services work correctly.

## Configure Calendar Meeting Details

Configure the information that displays in Exchange meeting details with the `exchange.meeting.show*` parameter.

Configure the following:

- **Subject:** Displayed by default. A brief description of the meeting's purpose.
- **Location:** Displayed by default. Where the meeting takes place.
- **Invitee(s):** Displayed by default. A list of meeting participants.
- **Agenda/Notes:** Displayed by default. When you hide Agenda/Notes, a message indicates that the meeting is private.
- **Meeting Organizer:** Displayed by default. The organizer doesn't display for meetings displayed on the monitor.
- **Show More Actions:** Displayed by default. If users can dial multiple numbers to join a meeting, the **Show More Actions** option displays in **Meeting Details** to enable users to choose the dial-in number.
- **Show Only Current or Next:** Deactivated by default. When enabled, the phone only displays either the current or next meeting on the calendar.
- **Show Tomorrow:** Enabled by default. Allows the phone to display meetings scheduled for the next day as well as the current day.

---

**Note:** This process is optional, depending on the desired configuration.

---

### Procedure

1. Hide the list of meeting attendees.

```
exchange.meeting.showAttendees="0"
```

2. Hide the **Agenda/Notes**.

```
exchange.meeting.showDescription="0"
```

3. Hide the meeting location.

```
exchange.meeting.showLocation="0"
```

4. Hide the **Show More Actions** option.

```
exchange.meeting.showMoreActions="0"
```

5. Configure the phone to display only the current or next meeting on the calendar.

```
exchange.meeting.showOnlyCurrentOrNext="0"
```

6. Hide the meeting organizer.

```
exchange.meeting.showOrganizer="0"
```

7. Hide meeting's subject.

```
exchange.meeting.showSubject="0"
```

8. Configure the phone to only show the current day's meetings on the calendar.

```
exchange.meeting.showTomorrow="0"
```

## Enable Calendar Month View

Enable the **Month View** option for users to retrieve calendar events for all the days in the month.

### Procedure

- » Enable the **Month** view option.

```
calendar.monthView.enabled="1"
```

## Ribbon Communications Server

Ribbon Communications application server, also called EXPERiUS™ A2, provides full-featured, IP-based multimedia communications applications for business and consumers.

Deploy EXPERiUS A2 as a standalone server or in combination with a Ribbon Communications CONTINUUM™ C20 server. Note that feature availability varies depending on your chosen deployment.

The following features are available for phones registered with the Ribbon Communications servers:

- **MADN-SCA:** A shared group feature that provides support for conference barge in, privacy, and remote call appearance. MADN-SCA requires you to deploy EXPERiUS A2 and CONTINUUM C20 server.
- **Global Address Book:** The global address book (GAB) feature is a corporate directory application managed by the Ribbon Communications server.
- **Personal Address Book:** The personal address book (PAB) feature, managed by the Ribbon Communications server, allows multiple clients (phones, computer software) to read and modify a user's personal directory of contacts. When one client changes a contact, all other clients immediately receive a notification of the change by the Ribbon Communications server.
- **E.911:** Enhanced 911 services specific to Ribbon Communications C20 server implementation.

## Multiple Appearance Directory Number - Single Call Appearance

Multiple appearance directory number-single call appearance (MADN-SCA) enables a group of users to share a single directory number that displays as a single line to each member of the group.

When you enable this feature on your users' phones, they can initiate or receive calls on this shared line. MADN-SCA requires you to deploy EXPERiUS A2 and CONTINUUM C20 servers.

Only one call can be active on the MADN-SCA shared line at a time. When a call is in progress, any incoming calls to the line receive a busy tone.

### Configure MADN-SCA

Configure MADN-SCA on a registered line.

Note the following:

- If you configure the line-specific parameter `reg.x.server.y.address`, you must also configure values in the line-specific parameter `reg.x.server.y.specialInterop`.

- If you configure the global parameter `voIpProt.server.x.address`, you must also configure values in the global parameter `voIpProt.server.x.specialInterop`.
- For all deployments, including Ribbon Communications, line-specific configuration parameters override global configuration parameters. If you set values in both line-specific and global parameters, line-specific parameters apply and global parameters don't apply.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

## Procedure

1. Configure the shared line. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

```
reg.x.type="shared"
reg.x.address="<registered line SIP URI>"
reg.x.server.y.address="<SIP server address>"
```

2. Limit the number of concurrent active calls allowed on the registered line. Replace *x* with the desired line key value.

```
reg.x.callsPerLineKey="1"
```

3. Specify the server-specify feature as `GENBAND`. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

```
reg.x.server.y.specialInterop="GENBAND"
```

4. Optional: Enable barge-in for the registered line. Replace *x* with the desired line key value.

```
reg.x.bargeInEnabled="1"
```

5. Optional: Enter the line's authentication credentials. Replace *x* with the desired line key value.

```
reg.x.auth.userId="<line authentication username>"
reg.x.auth.password="<line authentication password>"
```

6. Optional: Configure the SIP server's proxy server. Replace *x* with the desired line key value.

```
reg.x.outboundProxy.address="<SIP proxy server address>"
reg.x.outboundProxy.address="<transport method for SIP server>"
```

## Configuring Privacy on a MADN-SCA Line

Configure privacy settings for shared MADN-SCA lines.

When you set the line to shared, an incoming call alerts all the members of the group simultaneously, and any group member can answer it. On the server, you can configure a privacy setting that determines if other members of the group can barge into the same call after another member answers it. You can also configure if members of the group can pick up a call on hold regardless of who put it on hold.

Optionally, configure star codes on the server that you can dial on the phone to toggle the privacy setting during a single active call. Star codes apply in the following scenarios:

- If you configure the line for privacy by default, users can use a star code to toggle privacy on or off during an active call. When the call ends, the line resets to privacy settings.

- If you configure the line on the server with privacy off, users can use a star code to toggle the privacy on during an active call. However, users can't toggle back to privacy off during the call. When the call ends, the line resets privacy to off.

## Configure the Global Address Book

Enable and configure the phone to use a Ribbon Communications global address book (GAB). Ribbon Communications GAB is a read-only global directory set up by an administrator and can co-exist with other corporate directories on the phone.

### Procedure

1. Enable the GAB feature.

```
feature.corporateDirectory.alt.enabled="1"
```

2. Configure the connection to the Ribbon Communications GAB server.

```
dir.corp.alt.address="<URL address for Ribbon GAB>"
dir.corp.alt.port="<port for Ribbon GAB>"
dir.corp.alt.user="<Ribbon GAB username>"
dir.corp.alt.password="<Ribbon GAB password>"
```

---

**Note:** You may not need to provide a port if you provide a full URL for the Ribbon Communications server.

---

## Configure the Personal Address Book

Enable and configure the phone to use a Ribbon Communications personal address book (PAB). The PAB enables users to read and modify a personal directory of contacts on their phone.

When users modify contact information using any soft client, desk phone, or mobile client registered to the same line, the change updates all other clients. The Ribbon Communications server then immediately notifies users of the change.

### Procedure

1. Enable the PAB.

```
feature.corporateDirectory.alt.enabled="1"
```

2. Enable the GENBANDSOPI protocol on the phone to get the PAB service from the Ribbon Communications server.

```
dir.local.serverFeatureControl.method="GENBANDSOPI"
```

3. Specify the phone line on which to enable the personal address book.

```
dir.local.serverFeatureControl.reg="<line key>"
```

4. Optional: Specify the maximum number of contacts available for the Ribbon Communications PAB contact directory.



The default is 100. The value range is 1 to 100.

```
dir.genband.local.contacts.maxSize="<max number of contacts>"
```

## Configuring 911 Location for Ribbon Communications

Enhanced 911 (E.911) is disabled by default in a Ribbon Communications environment. Users can still manually set their location for emergency services.

By default, users can make a 911 call on a locked phone, regardless of the call state, or when other features are in use. During an active 911 call, the call control option doesn't display, users can't use the hard keys to control a call, and DND and call forwarding don't display.

### Manually Set the Phone's Location for Emergency Calls

Users can manually set their location for emergency calls on the phone's local interface.

Register the phone.

#### Procedure

1. Go to **Settings > Status > Diagnostics > Warnings**.
2. Select **Details** to enter a location to the location tree navigation menu.
3. Choose a location and press **Save**.
4. To confirm the setting, go to **Status > Location Information**.

The location information displays in the **Status** menu.

### Change the Location XML Schema Protocol for Location

Change the location XML schema sent during the SIP invite.

#### Procedure

- » Set the XML schema used during the SIP invite to comply with RFC 5139.

---

**Note:** Default setting is *RFC4119*.

---

```
feature.E911.locationInfoSchema="RFC5139"
```

## Configure Emergency Instant Messages

Enable incoming emergency instant messages and configure how long they display.

Messages display until one of the following occurs:

- The phone times out.
- The phone receives another instant message.
- A dialog message displays.
- The phone receives an incoming call.
- The user presses any key or message on the phone.

**Procedure**

1. Enable the phone to display emergency instant messages.

```
feature.instantMessaging.enabled="1"
```

2. Optional: Configure the timeout, in minutes, the emergency instant messages display on the phone's screen.

The default is 1. The value range is 1 to 60.

```
feature.instantMessaging.displayTimeout="<# of minutes>"
```

3. Optional: Silence the emergency instant message ringtone.

```
feature.instantMessaging.ring="Silent"
```

## BroadSoft BroadWorks Server

Integrate your phone with BroadSoft BroadWorks R18 and BroadWorks R20 features.

Some BroadSoft features include:

- Anonymous call rejection
- Simultaneous Ring
- Line ID blocking
- BroadWorks Anywhere
- Remote Office
- BroadSoft Server-Based call forwarding

---

**Note:** You can't register lines with the BroadWorks R18 server and the R20 and later simultaneously. You must register all lines on the phone to the same BroadWorks server.

---

## Authentication with BroadWorks XSP Service Interface

Some BroadSoft features require the phone to authenticate with the BroadWorks Xtended Service Platform (XSP) service interface. Configure your phones to use advanced features available on the BroadSoft BroadWorks server.

The phones support the following advanced BroadSoft features:

- BroadSoft Enhanced Call Park
- Executive-Assistant
- BroadSoft UC-One directory, favorites, and presence
- BroadSoft UC-One personal call control features

## Authenticate for BroadWorks XSP R19 or Earlier

Use this process to authenticate your phone if your server runs BroadWorks R19 or earlier.

### Procedure

1. Configure the server address for your BroadSoft XSP directory.

```
dir.broadsoft.xsp.address="<server address>"
```

2. Require the phone to use BroadSoft XSP credentials. Replace x with the desired line key value.

```
reg.x.broadsoft.useXspCredentials="1"
```

3. Configure your user ID for BroadSoft XSP services. Replace x with the desired line key value.

```
reg.x.broadsoft.userId="<user ID>"
```

4. Configure your password for Broadsoft XSP services. Replace x with the desired line key value.

```
reg.x.broadsoft.xsp.password="<password>"
```

## Authenticate for BroadWorks XSP R19 Service Pack 1 or Later

Authenticate your phone if your server runs BroadWorks R19 SP1 or later.

BroadWorks R19 SP1 and up enable you to authenticate using your BroadSoft XSP user ID and SIP credentials.

### Procedure

1. Configure the server address for your BroadSoft XSP directory.

```
dir.broadsoft.xsp.address="<server address>"
```

2. Enter your BroadSoft XSP user ID.

```
reg.x.broadsoft.userId="<XSP user ID>"
```

3. Enter your SIP user ID.

```
reg.x.auth.userId="<user ID>"
```

4. Enter your SIP password.

```
reg.x.auth.password="<password>"
```

## Polycom BroadSoft UC-One Application

The Polycom BroadSoft UC-One application integrates with BroadSoft Enterprise Directory and BroadCloud services—a set of hosted services by BroadSoft.

The BroadSoft UC-One application provides the following features:

- **BroadSoft Directory:** Displays information for all users in the enterprise. For example, work and mobile phone numbers.

- **BroadSoft Self-Presence:** Displays the user's aggregated presence received from the BroadSoft Messaging Server (UMS) on the phone.
- **BroadCloud Presence:** Enables users to share presence information with the BroadTouch Business Communicator (BTBC) client application.
- **BroadCloud Favorites:** Enables users to mark contacts as favorites with the BroadTouch Business Communicator (BTBC) client application.

## Enable the BroadSoft UC-One Application

Configure the phone to use the BroadWorks BroadSoft UC-One Application.

Configure the phone's authentication on your BroadSoft XSP server.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the BroadSoft UC-One feature.

```
feature.broadsoftUcOne.enabled="1"
```

2. Enable the QML viewer on the phone. This is required for the UC-One directory user interface.

```
feature.qml.enabled="1"
```

3. Enable simple search for Enterprise Directories.

```
feature.broadsoftdir.enabled="1"
```

4. Enable the presence feature, which includes buddy management and user status.

```
feature.presence.enabled="1"
```

## Hide the BroadSoft UC-One Settings in the Home Screen

Disable the **UC-One Settings** icon on the phone's **Home** screen to prevent unauthorized access to the settings.

### Procedure

- » Hide the **UC-One Settings** icon in the **Home** screen.

```
homeScreen.UCOne.enable="0"
```

## Configure UC-One Directory on BroadSoft R20 Server or Later

For the BroadSoft R20 server or later, configure the BroadSoft UC-One phone directory.

### Procedure

1. Prevent the phone from using the BroadSoft XSP credentials.

```
dir.broadsoft.useXspCredentials="0"
```

2. Enter the SIP credentials to retrieve the UC-One directory.

```
dir.broadsoft.regMap="<SIP credentials>"
```

## Enable Anonymous Call Rejection

Enable users to automatically reject incoming calls from anonymous parties with restricted caller identification.

When enabled, the **Anonymous Call Rejection** option displays in the **UC-One Settings** on the phone. Users can then activate the function to automatically reject incoming anonymous calls.

### Procedure

- » Display the **Anonymous Call Rejection** menu on the phone.

```
feature.broadsoft.xsi.AnonymousCallReject.enabled="1"
```

## Enable BroadWorks Call Decline on a Shared Line

Enable the phones to reject incoming calls on a shared line in a BroadSoft BroadWorks environment.

When enabled, a user can reject an incoming call on the shared line using the **Reject** softkey, preventing the call from ringing on all phones registered with the shared line.

### Procedure

- » Enable call decline on shared lines in the BroadSoft BroadWorks environment.

```
call.shared.reject="1"
```

## Enable and Configure Hoteling

Hoteling enables users to log in to a guest profile to use any available shared phone in the BroadSoft BroadWorks environment.

To enable hoteling, you must configure the phones with the BroadSoft BroadWorks R17 platform.

After logging in, users have access to their own guest profile and settings on the shared phone. When hoteling is enabled, the Guest In soft key displays for users to log in to the phone.

---

**Note:** For additional details on configuring the hoteling feature, see *Using Hoteling on Poly Phones (FP 76554)* at [Poly Engineering Advisories and Technical Notifications](#).

---

**Procedure**

- » Enable hoteling, and configure the hoteling line key value.

```
feature.hoteling.enabled="1"
hoteling.reg "<line key value>"
```

**Flexible Seating**

Flexible Seating enables a user of an assigned primary phone to simultaneously access a registered line as a guest from an alternate host phone.

The user's primary registration is active on the primary and host phone. Users can access the BroadSoft UC-One contact directory and favorites on the host phone, but the Poly contact directory and favorites aren't available.

---

**Note:** Flexible Seating differs from the hoteling feature in that it provides only the primary registration's label on the host phone without any synchronization of features or settings.

---

The following conditions apply to the Flexible Seating feature:

- The primary phone and host phone don't sync automatically, but you can manually sync the phones on the BroadSoft BroadWorks server.
- The phone configured for the host user can't accept incoming calls. The host user can make only emergency outgoing calls as defined by the BroadWorks server.
- With the Phone Lock enabled, the phone can't place outgoing calls to numbers defined in the authorized call list, except the emergency numbers set on the BroadWorks server.
- The host user account is a placeholder account that supports guest users.
- The guest user can't change the user password. You can change the host phone's user password from the system web interface at any time. You can change the host phone's user password from the phone screen only after the guest user logs out.

Flexible Seating doesn't support the following features:

- Hoteling
- Visitor Desk Phone (VDP)
- User Profile Feature
- Local Call Forwarding
- Local DND

On the BroadWorks server, you can set a period of time when the server automatically logs out a user from a phone in case a user doesn't log out.

**Related Links**

[Securely Store LDAP Credentials](#) on page 181

**Configure Flexible Seating**

Configure a phone to support Flexible Seating.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

To configure a host phone to support the primary phone's line registration, you must configure a host user profile and a guest user profile on the BroadSoft BroadWorks server.

### Procedure

1. Specify the phone line on the host phone which hosts the guest line.

```
hoteling.reg="<line key value>"
```

2. Enable the Flexible Seating on the phone and put it into a state where a guest isn't logged in.

**Note:** This parameter overrides  
voIpProt.SIP.specialEvent.checkSync.downloadDirectory.

```
hotelingMode.type="2"
```

## BroadSoft BroadWorks Configuration Tags

The following table shows the Poly parameters you can map to the corresponding BroadSoft tags.

Poly Configuration Parameter	BroadSoft Tag
hoteling.reg	%BWHOTELINGLINE-x%
hotelingMode.type	%BWHOTELINGMODE-x%

## Guest Profile PIN

You can configure a PIN for each guest profile, which enables users to access their guest profile on a host phone by providing their PIN.

Using a PIN prevents other users from logging into a guest phone without the phone password or guest PIN. The guest profile PIN takes precedence over the local phone password and the guest user must log out of the phone with the PIN before another user can log in with their password.

## Executive-Assistant Lines

Enable the BroadSoft Executive-Assistant feature on lines registered with the BroadWorks R20 or later server and assign the lines as either an executive or an assistant.

**Note:** All corresponding executive and assistant lines must register to the same server.

After you enable the feature, users can set filters to control whether calls route to an assistant or the executive line first. Executives can also enable screening, which enables the executive's phone to display the incoming call notification for all filtered calls.

In addition, depending on the role you assign the user, an **Executive** or **Assistant** icon displays on the phone's home screen. You can also simplify the Executive and Assistant menus by adding or removing **Pick Call** and **Barge-in** softkeys from the menu.

The BroadWorks server allows the following configuration options:

- A private executive line with an assistant with a private line

- Shared executive line with an assistant with a private line
- Shared executive line with a shared line alias on the assistant's phone
  - You must configure the shared line as a shared location with the Executive Service on the BroadWorks server.
  - In this option, the main line registration is a private line for the assistant, and the secondary registration is a shared line for the executive.

## Enhanced Feature Keys for Executive-Assistant Menus

You can create Enhanced Feature Keys (EFK) which allow users to quickly access the **Overview Executives** menu for assistants or the **Executive Settings** menu for executives.

You can create an **Executive** or **Assistant** line key, softkey, or speed dial that displays on the **Lines** screen.

- When a user presses the **Executive** EFK on the executive's phone, the **Executive Settings** menu displays.
- When a user presses the **Assistant** EFK on the assistant's phone, the **Overview Executives** menu displays.

Configure a line or softkey for this feature using the following EFK macros:

- Executive menu: "\$FExecutiveMenu\$"
- Assistant menu: \$FAssistantMenu\$

## Configure a Phone for Executive or Assistant Lines

Configure two phones as either an executive phone or as an assistant phone for the BroadWorks Executive-Assistant feature.

In the BroadWorks Web Portal, you must enable the Executive Service for private and shared executive lines, and the Executive-Assistant Service for private and shared assistant lines. You must also authenticate the phone with the BroadSoft XSP service interface.

### Procedure

1. Enable the BroadSoft Executive-Assistant feature on the phone.

```
feature.BSExecutiveAssistant.enabled="1"
```

2. Configure the registered line the phone uses for BroadSoft Executive-Assistant feature.

```
feature.BSExecutiveAssistant.regIndex="<line key value>"
```

3. Optional: If you're configuring an assistant phone, change its role. Phones default to the executive role.

```
feature.BSExecutiveAssistant.userRole="AssistantRole"
```

4. Optional: Remove the **Pick Call** and **Barge-in** softkeys from the Executive or Assistant menu options on the phone's home screen.

If you're configuring an executive phone:

```
feature.BSExecutiveAssistant.SimplifiedExec.enabled="1"
```



If you're configuring an assistant phone:

```
feature.BSExecutiveAssistant.SimplifiedAssistant.enabled="1"
```

## Configure Enhanced Call Park

Enhanced Call Park enables softkeys on the phone to park a call and retrieve a parked call in a BroadWorks BroadSoft environment.

The following features are available for Enhanced Call Park:

- You can configure Enhanced Call Park only using configuration files; you can't configure the feature on the system web interface or from the local interface.
- You can configure Enhanced Call Park for private lines and shared lines. No configuration is necessary to enable the call park notification for monitored BLF lines.
- The default star code set for the `call.parkedCallRetrieveString` parameter is \*88.

### Procedure

1. Enable BroadWorks Enhanced Call Park on a registered or shared line. Replace x with the registered line number.

```
reg.x.enhancedCallPark.enabled="1"
```

2. Optional: If you're configuring a shared line, enter the line extension. Replace x with the registered line number.

```
reg.x.lineAddress="<extension>"
```

3. Enable audio notifications for parked calls.

```
feature.enhancedCallPark.allowAudioNotification="1"
```

4. Optional: Configure a star code to initiate parked call retrieval. The default star code is \*88.

```
call.parkedCallRetrieveString="<star code>"
```

## Enable BroadSoft Directories

BroadSoft directories enable users to search and view their personal, group, or enterprise contacts.

When you integrate BroadSoft directories with the Polycom BroadSoft UC-One Application, users can access the different types of directories and search for contacts. There are five types of BroadSoft Directories:

- **Enterprise Directory:** This directory enables users to search and view Active Directory global address list of an enterprise. Users can query by first name, last name, phone number, extension, mobile number, and access contact information.
- **Group Directory:** This directory enables users to view the contact details such as work, extension, and mobile numbers of contacts. Users can place a call to anyone in their group.
- **Group Common Directory:** This directory enables users to view the contact details such as names and phone numbers of common contacts listed in the Group Common Directory.
- **Enterprise Common Directory:** This directory enables users to view the contact details such as names and phone numbers of common contacts listed in the Enterprise Common Directory.

- **Personal Directory:** This directory enables users to view the contact details such as names and phone numbers of the contacts in their personal directory stored on the BroadSoft server. You must enable this feature to allow users to add, delete, or edit the contacts in the BroadSoft Personal Directory.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the BroadSoft Enterprise and Enterprise Common Directories.

```
feature.broadsoftdir.enabled="1"
```

2. Enable the Group and Group Common Directories.

```
feature.broadsoftGroupDir.enabled="1"
```

3. Enable the Personal Directory and allow users to manage theirs on the phone's local interface.

```
feature.broadsoftPersonalDir.enabled="1"
```

## Centralized Call Recording

Centralized Call Recording allows users to record audio and video calls and control call recording directly from phones registered with BroadSoft BroadWorks r20 server.

Users can manage recorded audio and video files on a third-party call recording server.

By default, far-side participants don't receive an alert when the near side records a call. The BroadWorks r20 server provides administrators can enable an announcement, which sounds at the beginning of a call when recording begins. The recording continues for the new call if the user transfers the call.

---

**Note:** You can record calls using a central server or locally using the phone's USB call recording feature - you can't use both at the same time. By default, both features are disabled. If you enable one call recording feature, ensure you disable the other. Use either centralized or the local call recording; don't use both.

---

### Call Recording Modes

On the BroadSoft BroadWorks R20 server, set a call recording mode to one of the following:

- **Never Mode:** Call recording never initiates and the phone never displays call recording softkeys.
- **Always Mode:** The server records all incoming and outgoing calls without user initiation. Users have no call recording control options. During active calls, the phone display indicates the status of the call recording state. Call recording stops when the call ends and the server stores the recording.
- **Always with Pause/Resume Support Mode:** Call recording starts automatically when the call connects and **Pause** and **Resume** softkeys display on the phone. The phone display indicates the status of the call recording state. Call recording stops when the call ends and the server stores the recording.
- **On Demand Mode:** Call recording starts on the server when the call connects, but the recorded file saves only if the user initiates the recording. When the user presses the **Start** softkey, the recording saves to the server and the phone displays the **Pause** and **Resume** softkeys.

- **On Demand Mode with User-Initiated Start Mode:** Call recording doesn't begin automatically and the **Record** softkey displays on the phone. If users want to record an active call, they need to press **Record > Start** to start recording and save it to the server. While recording, the phone displays the **Pause**, **Resume**, and **Stop** softkeys.
- **Recording two separate calls and creating a conference:** This mode enables users to record two participants as separate call sessions when connected in a conference call. The server stores the conference call as two separate recording sessions.

## Enable Centralized Call Recording

Enable a phone to support BroadSoft BroadWorks Centralized Call Recording.

To use Centralized Calling, you must enable this feature on the BroadSoft BroadWorks r20 server and on the phone.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable Centralized Calling on the phone.

```
voIpProt.SIP.serverFeatureControl.callRecording="1"
```

## Block Call Recording on a Registered Line

Prevent a Centralized Call Recording on specific registered lines.

### Procedure

- » Specify the lines to block Centralized Call Recording. Replace x with the desired line key value.

```
reg.x.serverFeatureControl.callRecording="0"
```

## Enable Simultaneous Ring

Enable users to add phone numbers to a list of contacts whose phones ring simultaneously when they receive an incoming call.

When enabled, the **Simultaneous Ring** menu option displays in the **UC-One Settings** on the phone. Users can then turn the feature on or off from the phone and define which numbers to include in the simultaneous ring group.

### Procedure

- » Configure the **Simultaneous Ring** to display on the phone menu .

```
feature.broadsoft.xsi.SimultaneousRing.enabled="1"
```

## Enable Line ID Blocking

Enable users to conceal their phone number when making calls.

When enabled, the **Line ID Blocking** menu option displays in the **UC-One Settings** on the phone. Users can activate the feature to hide their phone number before making a call.

**Procedure**

- » Configure the **Line ID Blocking** menu to display on the phone.

```
feature.broadsoft.xsi.LineIdblock.enabled="1"
```

**Enable BroadWorks Anywhere**

Enable users to use one phone number on multiple phones, such as their desk phone, mobile phone, and home office phone.

When enabled, the **BroadWorks Anywhere** menu option displays in the **UC-One Settings** on the phone. Users can then turn the feature on or off and add BroadWorks Anywhere locations, which enable them to move calls between phones and perform phone functions from any phone.

**Procedure**

- » Configure the **BroadWorks Anywhere** menu to display on the phone.

```
feature.broadsoft.xsi.BroadWorksAnywhere.enabled="1"
```

**Enable Remote Office**

Enable users to set up a phone number on their office phone to forward incoming calls to a mobile device or home office number.

When enabled, the **Remote Office** menu option displays in the **UC-One Settings** on the office phone. When activated, the office phone forwards incoming calls to another phone configured by the user. Calls placed from the other phone display the office phone number on the far end.

**Procedure**

- » Configure the **Remote Office** menu to display on the phone.

```
feature.broadsoft.xsi.RemoteOffice.enabled="1"
```

**BroadSoft Server-Based Call Forwarding**

The BroadSoft server forwards incoming calls instead of the phone forwarding incoming calls.

To enable server-based call forwarding, you must enable the feature on both the server and the registered phone. If you enable server-based call forwarding on one registration, it only affects that registration.

The phone doesn't forward calls if you enable server-based call forwarding and leave it inactive, even if a user presses the **Forward** softkey.

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

## Enable Visual Security Classification Display

Enable the phone to display visual security classifications for all lines or for specific phone lines. The participant with the lowest security classification determines the security classification for a call.

Configure security classification settings on the BroadSoft BroadWorks server v20 or later.

For example, a **Top Secret** classification displays when all participants in a call have at least a **Top Secret** classification level.

---

**Note:** You can safely exchange information classified no higher than the call's security classification. For example, when a **Top Secret** participant calls a **Restricted** level participant, don't exchange information higher than **Restricted**.

---

Participants can adjust their security classification level to a lower value during a call. The participant's classification level resets to the higher value once the call is complete.

If a phone has multiple registered lines, you can assign a different security classification to each line. Configure security classifications as names or strings, then set the priority of each classification on the server in addition to the default security classification level **Unclassified**. The default security classification **Unclassified** displays until you set classifications on the server. When a user establishes a call to a phone not connected to this feature, the phone displays as **Unclassified**.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

- » Enable visual security classifications.

- For all lines:

```
voIpProt.SIP.serverFeatureControl.securityClassification="1"
```

- For specific lines Replace x with the desired line key value.:

```
reg.x.serverFeatureControl.securityClassification="1"
```

## Enable Feature-Synchronized Automatic Call Distribution

Feature-synchronized automatic call distribution (ACD) helps organizations handle a large number of incoming phone calls, such as a call center with users in agent and supervisor roles.

Feature-synchronized ACD is available in the following services tiers:

- **Standard:** Standard service enables call center agents to sign in to a shared phone. After an agent signs in, the phone displays their availability to take new calls.
- **Premium:** Premium service offers two additional features in addition to the Standard service:
  - Hoteling enables agents to use their agent credentials to log in to any available phone.
  - Queue status notification enables agents to view the queue status of a call center so that agents can adjust their call response.

The capabilities of this feature vary with the SIP call server. Consult your call server provider for information and for documentation. You can find information on the SIP signaling used for this

implementation in the BroadSoft BroadWorks document *Device Key Synchronization Requirements Document*; Release R14 sp2; Document version 1.6.

---

**Note:** For more information on standard and premium ACD as well as the hoteling and queue status notification enhancements, see *Feature Profile 76179: Using Premium Automatic Call Distribution for Call Centers - Hoteling and Queue Status* at [Poly Engineering Advisories and Technical Notifications](#).

---

## Procedure

1. Enable feature-synchronized on the phone. This parameter also adds the **Trace**, **Emergency**, and **Disp Code** softkeys.

```
feature.enhancedFeatureKeys.enabled="1"
feature.acdServiceControlUri.enabled="1"
```

2. Enable the ability for agents to log in and out of their phones.

```
feature.acdLoginLogout.enabled="1"
```

3. Optional: If you have the Premium service, enable the Premium Unavailability feature.

```
feature.acdPremiumUnavailability.enabled="1"
```

## Enable uaCSTA on a Dedicated Line

You can configure only one User Agent Computer Supported Telecommunications Applications (uaCSTA) line on each phone.

When you configure phones for uaCSTA with a CSTA server, you can remotely control the phone and access phone services using a computer telephony integration (CTI) application on your computer.

Poly phones support two types of user agent configurations for CSTA:

To ensure CSTA works correctly, Poly recommends that you configure the CSTA line as the last among all registered lines on the phone.

- A dedicated line to control or monitor all the other lines on the phone.
- A single line to act as both SIP line and CSTA line.

Poly phones support the Minimum and Basic profiles compliant with “ECMA TR/087: Using CSTA for SIP Phone User Agents (uaCSTA).” For information, see [ECMA international](#).

---

**Note:** Poly phones don't support the Network Reached event.

---

Poly supports the following CSTA services

- MonitorStart
- MonitorStop
- MakeCall Without Prompt
- AnswerCall
- ClearConnection
- DeflectCall in alerting state

- HoldCall
- RetrieveCall
- SingleStepTransferCall
- SnapshotDevice
- Conference Call
- Transfer Call
- ConsultationCall
- SetForwarding
- GetForwarding
- SetDoNotDisturb
- GetDoNotDisturb
- GetSwitchingFunctionDevices


Poly supports the following CSTA events:


- ServiceInitiated
- Originated
- Delivered
- Diverted
- Established
- ConnectionCleared
- Held
- Retrieved
- Failed
- Transferred
- BackInService
- OutOfService
- Conferenced
- SwitchingFunctionDevices

### Procedure

- » Set the CSTA line registration. Replace x with the desired line key value. Replace y with the desired server key value.

```
reg.x.csta="1"
reg.x.server.y.specialInterop="CSTA"
```

When you correctly register a CSTA line on a Poly phone, the CSTA line displays on the phone with an icon  and the default label **CSTA**.

If you incorrectly register the CSTA line, an icon  shows that the line is unregistered.

---

**Note:** A CSTA-registered line has no functionality to users. If a user selects a CSTA line on the phone, a message displays stating that no action is available.

---

# Directories and Contacts

---

## Topics:

- [Local Contact Directory](#)
- [Corporate Directory](#)
- [Call Lists](#)

Configure your phones to use a local contact directory, a corporate directory, or both.

Call logs stored in the **Missed Calls**, **Received Calls**, and **Placed Calls** call lists enable users to view phone events. Events include remote party identification, time and date of call, and call duration.

## Local Contact Directory

Configure phones with a local contact directory and link contacts to speed dial buttons.

### Set the Maximum Number of Contacts in the Local Directory

Configure the maximum number of contacts the phones store.

Phones can store a maximum of 3000 contact entries in a contact directory file 4 MB or smaller.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

## Procedure

- » Enter the maximum number of contacts allowed in the local directory. The default value is 500 contacts.

```
dir.local.contacts.maxNum="<1 to 3000>"
```

## Creating Directory Files

Configure a contact directory file that Poly phones use to store frequently used contacts.

The UC Software package includes a contact directory template named 000000000000-directory~.xml. The contact directory file loads to the provisioning server the first time you boot up a phone or after a factory reset.

The phone looks for contact directories in the following order:

- An internally stored local directory
- A personal <MACaddress>-directory.xml file
- A global 000000000000-directory.xml file when the phone substitutes <000000000000> for its own MAC address



## Create a Per-Phone Personal Directory File

Create a personal directory file to load onto a single phone in an update file.

Any changes users make to the contact directory on the phone store on the phone. Upload the information to the provisioning server in the personal directory (`<MACAddress>-directory.xml`) file.

### Procedure

1. Locate the XML directory file in the phone's software update folder.  
The default file name is `000000000000-directory~.xml`.
2. Remove the tilde (~) from the end of the file name and replace the `000000000000` in the directory file name with the phone's MAC address.  
`<MACAddress>-directory.xml`

## Create a Global Directory File

Create a global directory file to provision to multiple phones.

When you update the global directory file on the provisioning server, the updates download to all phones. The downloaded directory file combines with the local directory on the phone.

### Procedure

1. Locate the XML directory file in the provisioning folder.  
The default file name is `000000000000-directory~.xml`.
2. Remove the tilde (~) at the end of the file name.  
`000000000000-directory.xml`

## Populate a Directory File with Contact Information

Create the contact entries for the directory files loaded onto your phones.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Open the `000000000000-directory~.xml` directory file.  
The directory file includes three sample contacts that can serve as templates for new contact entries.
2. Add contact information inside the `<item>` tag.

```
<item>
    <fn>First Name</fn>
    <ln>Last Name</ln>
    <ct>Numeric Contact ID</ct>
    <sd>Speed Dial Entry</sd>
    <rt>Ringtone</rt>
</item>
```

The following table lists the elements to use when configuring a contact directory file.

## Contact Directory XML Elements

Element	Description	Permitted Values
fn	First name	UTF-8 encoded string up to 40 bytes.
ln	Last name	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL.
ct	<p>Contact</p> <p>Used by the phone to address a remote party in the same way that a user manually dials a string of digits or a SIP URL. Also used to associate incoming callers with a particular directory entry.</p> <p>The maximum field length is 128 characters.</p>	<p>20</p> <p><b>Note:</b> You can't duplicate this field or leave it Null.</p>
sd	<p>Speed dial index</p> <p>Associates a particular entry with a speed dial key.</p>	20
lb	<p>Label for the contact</p> <p>The label of a contact directory item is by default the label attribute of the item. If the label attribute doesn't exist or is Null, then the first and last names form the label with a space between first and last names.</p>	UTF-8 encoded string up to 40 bytes.
pt	<p>Protocol</p> <p>The protocol to use when placing a call to the contact.</p>	SIP, H323, or Unspecified
rt	<p>Ringtone</p> <p>When incoming calls match a directory entry, this field specifies the ringtone to use.</p>	Null, 1 to 21
ad	<p>Auto divert</p> <p>Set to 1 to divert callers that match the directory entry to the address specified for the divert contact element.</p>	<p>0, 1</p> <p><b>Note:</b> If you enable auto-divert, it has precedence over auto-reject.</p>

Element	Description	Permitted Values
ar	Auto reject  Set to 1 to reject callers that match the directory entry specified for the auto reject element.	0, 1  <b>Note:</b> If you enable auto-divert, it has precedence over auto-reject.
bw	Buddy watching  Set to 1 to add this contact to the list of watched phones.	0, 1
bb	Buddy block  Set to 1 to block this contact from watching this phone.	0, 1
up	User photo  The contact's photo icon set by the <code>icons.x</code> parameter.	1 to 24

## Configure When Directory Files Update

Enable the phone to download the global directory file more frequently.

By default, a phone that uses a global directory file updates only after it receives a checksync NOTIFY message from the server. When you enable this parameter, the phone also downloads the global directory file following a reboot, configuration change, or software update.

When the phone updates, the following events happen:

- The phone downloads the global directory (`000000000000-directory.xml`) and per-phone (`<MACaddress>-directory.xml`) directory files.
- The directory files merge with the phone's directory.
- The phone ignores changes to the global directory that conflict with the phone's personal directory.

**Note:** Setting the `hotelingMode.type` parameter to 2 or 3 overrides this parameter.

## Procedure

- » Enable the phone to download the global directory file following a reboot, configuration change, or software update.

```
voIpProt.SIP.specialEvent.checkSync.downloadDirectory
="1"
```

## Disable the Local Contact Directory

If you don't want phone users to store contacts on a phone, disable the local contact directory.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

- » Disable the local contact directory.

```
feature.directory.enabled="0"
```

## Create a Speed Dial Entry in the Directory File

Poly phones support speed dial entries accessible from the phone interface.

Poly CCX business media phones can support up to 500 speed dial entries.

This example shows adding a speed dial to the main directory file 00000000000000-directory.xml used by all phones.

### Procedure

1. In the directory file, locate the contact entry.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<directory>
  <item_list>
    <item>
      <ln>last name</ln>
      <fn>first name</fn>
      <ct>contact entry #</ct>
      <rt>ringtone</rt>
    </item>
  </item_list>
</directory>
```

2. To assign a speed dial value, add the <sd> element with the assigned speed dial number.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<directory>
  <item_list>
    <item>
      <ln>last name</ln>
      <fn>first name</fn>
      <ct>contact entry #</ct>
      <rt>ringtone</rt>
      <sd>speed dial #</sd>
    </item>
  </item_list>
</directory>
```

When the phone polls the provisioning server, the new entry shows up on all phones.

## Disable Local Speed Dial Edits

Prevent users from editing the speed dial entries on their phones.

### Procedure

- » Disable local edits to speed dial entries.

```
dir.local.readonly="1"
```

## Corporate Directory

Connect your phones to a corporate directory server that supports LDAP version 3. Setting up the corporate directory on the phone enables users to search for and place calls to these directory contacts.

Poly phones support corporate directories with server-side sorting. If the directory doesn't support server-side sorting, the phone performs sorting locally.

---

**Note:** Use 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](#).

---

## Connect to a Corporate Directory Using LDAP

Connect to and download corporate directory contacts to your phones.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

Access to a corporate directory on the phone is read only. Phone users can't add or remove contacts to the corporate directory.

### Procedure

1. Enter the IP address or host name of the LDAP server.

```
dir.corp.address="<LDAP IP address or host name>"
```

2. By default, the phone uses the TCP transport protocol to transfer the LDAP file from the server. If your network requires it, change the transport protocol to TLS.

```
dir.corp.alt.transport="TLS"
```

3. Enable the login prompt if the phone doesn't log in to the LDAP server as part of the phone's configuration.

```
dir.corp.allowCredentialsFromUI.enabled="1"
```

## Securely Store LDAP Credentials

Enable multiple users to enter their LDAP user credentials directly in the phone to access the corporate (LDAP) directory and store those credentials on the phone.

Any LDAP credentials that users enter on the phone are encrypted and stored only on the phone. The credentials also persist after the phone restarts or reboots.

When you configure this feature for phones with BroadSoft Flexible Seating, the phones can store up to 50 user credentials. If the number of user credentials reaches 50, the phone removes the user who has the longest period of inactivity when additional users are added.

### Procedure

1. Enable the phone to securely store and encrypt LDAP directory user credentials.

```
dir.corp.persistentCredentials="1"
```

2. Enable the phone to accept user credentials on the local interface.

```
dir.corp.allowCredentialsFromUI.enabled="1"
```

### Related Links

[Flexible Seating](#) on page 165

## Call Lists

The phone records and maintains user phone events in call lists. Call lists contain call information such as remote party identification, time, and date.

The provisioning server stores the list as an XML file named `<MACaddress>-calls.xml`. If you want to route the call list to another server, use the `CALL_LISTS_DIRECTORY` field in the primary configuration file. All call lists are enabled by default.

The phone maintains all calls in three separate user accessible call lists:

- Missed calls
- Received calls
- Placed calls

## Disable the Missed Call List

Remove the missed call list on the **Home** screen and dialpad.

The missed call list lists all the incoming calls that the user doesn't answer.

### Procedure

- » Disable the missed call list.

```
feature.callListMissed.enabled="0"
```

## Disable the Placed Call List

Remove the placed call list on the **Home** screen and dialpad.

The placed call list displays all outgoing calls users make from the phone.

### Procedure

- » Disable the placed call list.

```
feature.callListPlaced.enabled="0"
```

## Disable the Received Call List

Remove the received call list on the **Home** screen and dialpad.

The received call list displays all incoming calls the user answers.

### Procedure

- » Disable the received call list.

```
feature.callListReceived.enabled="0"
```

## Disable All Call Lists

Remove the missed call list, placed call list, and received call list from the **Home** screen and dialpad.

Setting this parameter overrides the `feature.callListMissed.enabled`, `feature.callListPlaced.enabled`, and `feature.callListReceived.enabled` parameters.

### Procedure

- » Disable all call lists.

```
feature.callList.enabled="0"
```

## Disable Consultation Call Logging

Prevent the phone from logging consultation calls in call lists.

### Procedure

- » Disable consultation call logging so the phone doesn't log them in call lists.

```
callLists.logConsultationCalls="0"
```

## List Consecutive Calls Individually

By default, the phone call lists collapse consecutive calls to or from the same party into one call entry. Configure the phone to list each call instance individually.

### Procedure

- » Configure the phone to list each consecutive call instance individually.

```
callLists.collapseDuplicates="0"
```

## Enable Exchange Call Logs

Configure the phone to synchronize the current user's Exchange call logs with the server and display the call history of missed, outgoing, and received calls.

### Procedure

- » Enable the phone to display Exchange call logs.

```
feature.exchangeCallLog.enabled="1"
```

### Related Links

[Microsoft Exchange Integration](#) on page 153



# Configuring the Local Interface

---

## Topics:

- [Localizing the User Interface](#)
- [Configure the Phone's Display Name](#)
- [Configuring Labels](#)
- [Time and Date Display](#)
- [Set a Preferred Home Screen](#)
- [Change Colors for Display Elements](#)
- [Set Up a Custom Background](#)
- [Configure a Line Registration Key Icon](#)
- [Digital Picture Frame](#)
- [LED Indicators](#)

Configure the phone display with various features, functions, and customization options.

## Localizing the User Interface

Poly phones support multiple languages and keyboard layouts.

### Edit Phone Languages

Edit the language files included with the UC Software package to customize the localized user interface.

Before editing, familiarize yourself with the guidelines on basic and extended character support.

Poly phones support the following languages:

- Arabic
- Simplified Chinese
- Traditional Chinese
- Czech, Czech Republic
- Danish
- Dutch
- English
- French
- German
- Hungarian, Hungary
- Italian
- Japanese
- Korean

- Norwegian
- Polish
- Brazilian Portuguese
- Romanian, Romania
- Russian
- Slovenian
- International Spanish
- Swedish

---

**Note:** The updater is only available in English.

---

### Procedure

1. Go to the `VVXLocalization` folder in your UC Software package.
2. Open the language file in a Unicode-compatible XML editor.
3. Edit the dictionary as desired.

## Change the Keyboard Layout

Enable users to choose a keyboard layout based on languages other than the system language.

The phone uses the default keyboard assigned to the language you set the phone to. For example, setting the phone language to French tells the phone to use the AZERTY keyboard layout.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Press and hold the comma (,) key on the phone's keyboard for one second to access the **Input options** menu.
2. Select **Languages**.
3. Clear the **Use system language** check box.
4. Select one or more languages in the **Active input methods** list.
5. Select the back arrow.

When enable more than one language, a globe key displays next to the comma (,) key on the phone keyboard, which enables you to change the active keyboard.

6. Do one of the following:
  - Select and hold the globe key for 1 second to view and choose from a list of enabled languages. The phone uses the default keyboard layout for the language you choose.
  - Select the globe key to cycle through enabled languages. The space bar displays the current language and keyboard layout.

## Enable Pinyin Text on the Phone

Pinyin is the phonetic system used to transcribe spoken Mandarin Chinese into Latin characters.

### Procedure

- » Go to [Nuance XT9](#) and download a license key to the phone.

## Configure the Phone's Display Name

Configure the phone's name that displays on connected devices.

The default system name displays as **<phone name><model number>\_xxxx** where xxxx are the last four digits of the phone's MAC address.

Configure the system name using any of the following parameters:

- `system.name`
- `reg.x.displayname`
- `reg.x.label`
- `reg.x.address`
- Default system name

---

**Note:** This list displays the priority in which the system name is selected from highest priority to lowest priority.

---

If you set the system name using the `system.name` parameter, the value you set displays for the phone unless you configure a name to display for a specific feature. The system name you set using any of the following feature parameters takes precedence over the name set in `system.name`:

- **AirPlay:** `content.airplayServer.name`
  - **Bluetooth:** `bluetooth.device.name`
  - **Wireless Display:** `content.wirelessDisplay.name`
- 

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Change the system name.

```
system.name="<system name - maximum 96 characters>"
```

2. Optional: Set a name specifically for AirPlay-certified devices. This setting overrides the setting in `system.name` when searching for the phone from AirPlay-certified devices.

```
content.airplayServer.name="<UTF-8 encoded string>"
```

- Optional: Set a name specifically for Android and Windows devices. This setting overrides the setting in `system.name` when searching for the phone from Android or Windows devices.

```
content.wirelessDisplay.sink.name="<UTF-8 encoded string>"
```

- Optional: Set a name specifically for Bluetooth devices. This setting overrides the setting in `system.name` when searching for the phone from Bluetooth devices.

```
bluetooth.device.name="<UTF-8 encoded string>"
```

- Set the SIP URI registration/H.323 extension. Replace `x` with the desired line key value.

```
reg.x.address="<SIP URI / H.323 ID>"
```

- Set the name used in SIP signaling, the H.323 alias, or both. This appears as the caller ID on outgoing calls. Replace `x` with the desired line key value.

```
reg.x.displayname="<UTF-8 encoded string>"
```

- Set the text label that displays next to the line key for registration `x`. Replace `x` with the desired line key value.

```
reg.x.label="<UTF-8 encoded string>"
```

## Configuring Labels

You can choose to display a phone number, an extension, or a custom label on the **Home** screen below the time and date.

### Configure Labels in the Local Interface

Configure the phone number and labels that display on the **Home** screen through the phone's local interface.

#### Procedure

- Select **Settings > Advanced > Administration Settings**.
- Select **Home Screen Label**.
- Select the **Type**.

If you select **Custom** for the **Type**, enter a custom message to display in the **Label** field.

- Choose a **Location** for the phone number or label to display.
- Select **Save**.

### Create a Custom Label with a Configuration File

Use a configuration file to create and configure a custom message to display on the **Home** screen.

By default, all phones display their phone number in a label on the **Home** screen.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Change the label's type to a custom label and enter the custom message.

The custom message can be up to 255 characters.

```
homeScreen.labelType="Custom"
homeScreen.customLabel="<Custom message>"
```

2. Optional: Set the label so it displays below the date instead of at the top of the screen.

```
homeScreen.labelLocation="BelowDate"
```

**Configure Unique Line Labels for Registration Lines**

Configure a unique label for a line key on a registered line.

Ensure you enable at least two line keys for a registered line before configuring this feature. If `reg.x.linekeys="1"`, this configuration has no effect.

You must configure multiple line keys for a registration to configure unique line labels. For example, you can set different names to display for the registration *4144* that display on four line keys.

If you configure the line to display on multiple line keys without a unique label assigned to each line, the phone labels the lines automatically in numeric order. For example, if you have four line keys for line *4144* labeled *Poly*, the line keys are labeled as *1\_Poly*, *2\_Poly*, *3\_Poly*, and *4\_Poly*. This also applies to lines without labels.

**Procedure**

1. Enable the phone to use unique labels for line keys for a registered line.

```
up.cfgUniqueLineLabel="1"
```

2. Configure a unique line label for a line key on a registered line. Replace *x* with the registration index number starting from 1. Replace *y* with the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys.

The default is Null. The maximum string length is 255 characters.

```
reg.x.line.y.label="<string>"
```

3. Configure the alignment of the label.

- None (Default)
- Right
- Left

By default the line label aligns right for alphanumeric strings and it aligns left for numeric strings.

```
up.cfgLabelElide="<value>"
```

## Enable and Configure the Digital Phone Label

The digital phone label displays a custom message in the status bar. Enable the digital phone label and enter a brief message to display in the phone's status bar.

The message you enter for the digital phone label supports up to 14 digits. The phone supports letters, though it may truncate longer messages. The label is helpful for displaying the phone's number or other frequently contacted numbers on the **Home** screen.

### Procedure

1. Enable the digital phone label.

```
lcl.status.LineInfoAtTop="1"
```

2. Enter the message used for the digital phone label.

```
lcl.status.LineInfoAtTopText="<string>"
```

## Time and Date Display

Configure how the phone displays the time and date or disable the time and date display entirely.

Set the time and date format to display differently when the phone is in certain modes. For example, the display format can change when the phone goes from idle mode to an active call.

The time and date display on phones in PSTN mode in the following conditions:

- An incoming call with a supported caller ID standard
- The phone is connected to Ethernet and you enable the date and time display

Poly recommends synchronizing your phone with an SNTP server to display the most accurate time.

### Related Links

[Setting the Time and Date](#) on page 28

## Disable the Time and Date on the Idle Display

Prevent the time and date from displaying on the phone's screen when the phone is in idle mode.

### Procedure

- » Disable the time and date on the idle display.

```
up.localClockEnabled="0"
```

## Configure Time and Date Display Settings

Configure how the time and date display on your phone's screen.

### Procedure

1. Display the time in a 12-hour clock format.

The default displays the time in a 24-hour clock format.

```
lcl.datetime.time.24HourClock="0"
```

2. Configure the date to appear above the time display.

The default displays the time above the date.

```
lcl.datetime.date.dateTop="1"
```

## Change the Date Format

Configure how the date displays on the phone screen.

### Procedure

1. Configure how the day and date display on the phone.

By default, phones display the day and date as "Thursday, 3 July" with a value of D,dM.

```
lcl.datetime.date.format="<date format string>"
```

Use the following table to choose values for the `lcl.datetime.date.format` parameter. The table shows values for Friday, August 20, 2019 as an example.

**Date Format Table**

<code>lcl.datetime.date.format</code>	<code>lcl.datetime.date.longformat</code>	Date Displayed on Phone
dM,D	0	20 Aug, Fri
dM,D	1	20 August, Friday
Md,D	0	Aug 20, Fri
Md,D	1	August 20, Friday
D,dM	0	Fri, 20 Aug
D,dM	1	Friday, August 20
DD/MM/YY	N/A	20/08/19
DD/MM/YYYY	N/A	20/08/2019
MM/DD/YY	N/A	08/20/19
MM/DD/YYYY	N/A	08/20/2019
YY/MM/DD	N/A	19/08/20
YYYY/MM/DD	N/A	2019/08/20

2. Optional: Change the day and month display the short format (Fri/Nov) instead of the default long format (Friday/November).

```
lcl.datetime.date.longFormat="0"
```

## Set a Preferred Home Screen

Configure the page that displays as the phone's **Home** screen.

By default, the phone's **Home** screen displays the time, date, and icons to access **Settings** and to place a call. Depending on the phone's configuration, it may also display icons to forward calls, enable DND, and access messages.

### Procedure

- » Set the phone's preferred **Home** screen.
  - default (Default) - **Home** screen
  - line - **Lines** screen
  - meeting - **Meetings** screen

```
feature.preferredHomeScreen="<value>"
```

## Change Colors for Display Elements

Change the color for phone display elements using hex code format (#RRGGBB). Skip any steps for elements you don't need to adjust.

---

**Important:** Configuring these options can impact the accessibility of your phones for people who have low vision or are colorblind. It can also impact accessibility for people with seizure disorders.

---

You can adjust the colors for the following items:

- **Home** screen background
- **Menu** screen background and text
- Menu item background and text
- Softkey background and text
- Status bar background and text

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Change the background color for the **Home** screen.

```
ui.home.background="<#RRGGBB color code>"
```

2. Change the background color for the **Menu** screen.

```
ui.menu.background="<#RRGGBB color code>"
```

3. Change the background color for the **Menu** title.

```
ui.menu.title.background="<#RRGGBB color code>"
```



4. Change the background color for menu items.

```
ui.menu.item.background="<#RRGGBB color code>"
```

5. Change the text color for menu items.

```
ui.menu.item.text.color="<#RRGGBB color code>"
```

6. Change the background color for softkeys.

```
ui.softkey.background="<#RRGGBB color code>"
```

7. Change the text color for softkeys.

```
ui.softkey.text.color="<#RRGGBB color code>"
```

8. Change the background color for the status bar.

```
ui.statusBar.background="<#RRGGBB color code>"
```

9. Change the text color for the status bar.

```
ui.statusBar.text.color="<#RRGGBB color code>"
```

## Set Up a Custom Background

Replace the phone's default background image with a custom image or import multiple images that users can select from.

Poly phones support .jpeg, .bmp, and .png image file formats. The phone doesn't support progressive/multi-scan .jpeg images.

The custom background displays behind the time, date, and line and key labels on the **Home** screen. The phone looks for custom background image from a folder in your network.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable the phone to use a custom background.

```
bg.background.enabled="1"
```

2. Set the background images location on your network.

---

**Note:** If the file is missing or unavailable, a default solid pattern displays.

---

```
bg.color.bm.1.name="<custom background URL>"
```

- Optional: Make the line keys transparent to display more of the custom background.

```
up.transparentLines="1"
```

Refer to the following table for the maximum image size supported for each phone model.

**Maximum Phone Screen Image Size**

Phone	Screen Size (px)	Recommended Logo Size (px)
CCX 400	720 × 1280	135 × 135
CCX 500	720 × 1280	135 × 135
CCX 600	1024 × 600	135 × 135
CCX 700	1024 × 600	135 × 135

## Configure a Line Registration Key Icon

Configure your phone to display custom icons for registered lines or user photos for contacts in the local contact directory and favorites on the **Home** screen.

Poly recommends uploading .png images that are 106 × 106 pixels with a size of 100 KB or smaller. You can upload images as large as 200 × 200 pixels, however, the phone automatically scales the icons to 106 × 106 pixels.

---

**Note:** The phone only supports .png image files. It doesn't support other image filetypes, such as .jpg, .tiff, .bmp, .webp, and .gif.

---

You can configure icons for up to 24 registered lines and contacts.

You can add the icons to the root directory or a subdirectory on the provisioning server or specify the URL location for the icons. If you place icons in a subdirectory, specify the subdirectory in the `ICONS_DIRECTORY` attribute in the `<APPLICATION>` tag in the `MAC.cfg` file.

---

**Note:** Make sure that the icons configured and distributed through UC Software don't violate any Intellectual Property rights.

---

### Procedure

- Define the line registration key icon by mapping it to a .png image file in your FTP or provisioning server. Replace *y* with the icon index number.

```
icons.y="<icon filename>"
```

The first icon you define is `icons.1`. Define subsequent icons with the next available index number: the second and third icons you define are `icons.2` and `icons.3`, respectively.

- Assign the icon to a line registration. Replace *x* with the desired line key value.

```
reg.x.icon="icons.y"
```

## Digital Picture Frame

Users can use the digital picture frame feature to display a slide show on the phone's idle screen. You can map a different location for the photos, adjust the photo refresh duration, and disable the digital picture frame feature.

For images to display, users must save the images in .jpg, .bmp, or .png format in the root directory of the USB flash drive. The phone can display a maximum image size of 9999 × 9999 pixels and a maximum of 1000 images.

The maximum image size depends on the available memory in the phone.

Users can access the digital picture frame on the web using `PicFrame:// URL`.

### Map Digital Picture Frame Location

Configure the digital picture frame feature to use images not stored on the USB flash drive's root directory.

By default, the phone looks for the photos in the USB flash drive's root directory.

#### Procedure

- » Enter the filepath for the images on the USB flash drive. For example, if you want users to save the images in the `/images/phone` folder on the USB flash drive, configure `images/phone`.

```
up.pictureFrame.folder="<image filepath>"
```

### Adjust the Digital Picture Frame Refresh Duration

Set how long, in seconds, the phone displays one image before moving to the next one. By default, the phone displays an image for 5 seconds.

#### Procedure

- » Change how long the phone displays one image before refreshing.  
You can set the duration of the picture frame refresh from 3 to 300 seconds, the default is 5 seconds.

```
up.pictureFrame.timePerImage="<duration>"
```

### Disable the Digital Picture Frame

Prevent users from displaying images stored on a USB flash drive while idle.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

- » Disable the digital picture frame feature.

```
feature.pictureFrame.enabled="0"
```

## LED Indicators

LED indicators alert users to the different states of the phone and remote contacts.

**Important:** Configuring these options can impact the accessibility of your phones for people who have low vision or are colorblind. It can also impact accessibility for people with seizure disorders.

You can turn LED indicators on or off and set the pattern, color, and duration of a pattern for all physical keys on the phones and the following LED indicators:

- Line keys
- Message Waiting Indicator (MWI)
- Headset key

Use the following example configuration tasks to configure custom LED patterns.

For more LED pattern configurations, see the *Poly CCX Parameter Reference Guide*.

## LED Indicator Pattern Types

Use the values from the following table to indicate the LED indicator pattern type.

**LED Indicator Pattern Type**

Pattern Type	Function
powerSaving	Sets the behavior for the message waiting indicator when the phone is in power saving mode.
active	Sets the pattern for line keys during active calls.
on	Turns on the LED indicator pattern.
off	Turns off the LED indicator pattern.
offering	Sets the pattern for line keys during incoming calls.
flash	Sets the pattern for line keys during held calls and the message waiting indicator when there are unread voicemail messages.
lockedOut	Sets the pattern for line keys when a remote party is busy on a shared line.
held	Sets the pattern for line keys during a held call.
remoteBusyOffering	Sets the pattern for line keys for monitored BLF contacts when the BLF is in an active call and receives a new incoming call.

Pattern Type	Function
blfHold	Sets the pattern for BLF line keys when a call is on the hold. The default pattern is a slow flashing red LED.
parkedCallSelf	Sets the LED pattern for a self-parked call.
parkedCallRemote	Sets the LED pattern for remote-parked call.

## Set an LED Pattern for Active Calls

Configure the phone's LED to alternate colors during an active call.

### Procedure

1. Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.active.step.1.state="1"
ind.pattern.active.step.1.color="<LED color>"
ind.pattern.active.step.1.duration="<duration>"
```

2. Enable the LED, configure the second LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.active.step.2.state="1"
ind.pattern.active.step.2.color="<LED color>"
ind.pattern.active.step.2.duration="<duration>"
```

## Set an LED Pattern on BLF for Held Calls

Configure the LED indicator to flash when a monitored BLF line is on hold.

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

### Procedure

1. Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.blfHold.step.1.state="1"
ind.pattern.blfHold.step.1.color="<LED color>"
ind.pattern.blfHold.step.1.duration="<duration>"
```

2. Disable the LED and set how long the LED remains off, in milliseconds, before turning back on.

Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.blfHold.step.2.state="0"
ind.pattern.blfHold.step.2.duration="<duration>"
```

## Set an LED Pattern for Incoming Calls

Configure the phone's LED to flash a different color for incoming calls.

### Procedure

- » Change the LED indicator color for incoming calls.  
Set the LED color as Red, Green, or Yellow. The default is Green.

```
ind.pattern.offering.step.1.color="<LED color>"
```

## Set an LED Pattern for Self-Parked Calls

Set how the LED indicator behaves for self-parked calls.

### Procedure

- » Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.parkedCallSelf.step.1.state="1"
ind.pattern.parkedCallSelf.step.1.color="<LED color>"
ind.pattern.parkedCallSelf.step.1.duration="<duration>"
```

## Set an LED Pattern for Remote-Parked Calls

Set how the LED indicator behaves for remote-parked calls.

### Procedure

- » Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.parkedCallRemote.step.1.state="1"
ind.pattern.parkedCallRemote.step.1.color="<LED color>"
ind.pattern.parkedCallRemote.step.1.duration="<duration>"
```

## Configure LED Behavior for Held Calls on Shared Lines

Configure the LED to blink red and green for locally held calls and to blink only red for remotely held calls.

By default, the phone blinks red for both remotely and locally held calls. You can also create a custom pattern.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

#### Procedure

- » Configure a distinctive LED behavior for held calls on shared lines.

```
call.shared.distinctiveLedOnHold="1"
```

#### Related Links

[Shared Lines](#) on page 123

## Disable the Headset Key LED in Headset Memory Mode

Disable the flash pattern for the **Headset** key in Headset Memory Mode.

The **Headset** key flashes green for analog headsets and blue for USB headsets by default while in headset memory mode. Disable the key flashes if the user finds it distracting or bothersome.

#### Procedure

- » Disable the **Headset** key LED flashing in headset memory mode.

```
ind.pattern.flashSlow.step.1.state="0"
```

## Disable Message Waiting Indicator in Power Saving Mode

Disable the message waiting indicator while the phone is in power saving mode to conserve power.

#### Procedure

- » Disable the message waiting indicator in power saving mode.

```
ind.pattern.powerSaving.step.1.state="0"
```

#### Related Links

[Power Saving on CCX Phones](#) on page 139

# Phone Maintenance

---

## Topics:

- [Analytics Support for Poly Cloud Services](#)
- [VQMon Reports](#)
- [Monitoring the Phone's Memory Usage](#)
- [Capturing the Phone's Screen](#)
- [Rebooting the Phone](#)
- [Upgrading the Software](#)
- [Resetting a Phone to Factory Defaults](#)

Perform system management and maintenance tasks on your phone and upgrade the software.

## Analytics Support for Poly Cloud Services

Configure phones to accept commands from the cloud analytics service to perform specified operations on the device and retrieve device details.

Poly phones send the following details to the cloud:

- Device Asset
- Device Network
- Device Diagnostics

Poly phones send the device details to the cloud when the following occurs:

- Phone restarts or reboots
- On-demand request from the cloud
- Device details are updated or changed

### Importing and Exporting Configurations

When you enable Device Analytics and set the `da.supported.services` value to `all` or `config`, you can configure the following device options:

- Download a configuration file to a phone from the cloud
- Upload the configuration of a phone to cloud

## Busy Lamp Field Analytics

When you enable Device Analytics and set `da.supported.services` to `all` or `blf`, the phone sends certain BLF details to the cloud.

The phone sends the following details to the cloud:

- The total number of configured Busy Lamp Field (BLF) lines.
- The total number of dropped BLF line notification.



- The total number of actions/pickup on BLF line.
- The phone increments the BLF's line notification for every new notification for each BLF configured line.

## Shared Call Appearance Analytics

When you enable Device Analytics and set `da.supported.services` to `all` or `sca`, the phone sends certain information to the cloud.

The phone sends the following details are sent to the cloud:

- The total number of registered Shared Call Appearance (SCA) lines.
- The total number of action or resume/barge-in on SCA line.
- The phone increments the SCA line notification for every new notifications of call-info, line-seize, and dialog for each SCA configured line.

## User Interface Analytics

User Interface analytics enables you to upload phone activity to the cloud when you set `da.supported.services` to `all` or `uianalytics`.

### Key-Press Analytics

Key-press analytics enables you to track and maintain hard and soft key press count on the phone for each key.

You can upload key-press counts at intervals you configure. Counters per key are reset after each upload. You cannot record the sequence of the key presses on the phone.

### Feature Access Analytics

Feature access analytics enables you to track and maintain features that users access on the phone.

When a user accesses a feature, the corresponding feature counter is incremented. You can upload feature counts at an interval you configure. Feature counters are reset after each upload.

## UPtime Analytics

The phone keeps track of various services and uploads the active status to cloud periodically when `da.supported.services` value is set as `all` or `uptimeanalytics`.

The phone monitors and sends the following services details to the cloud:

- Exchange Services (Calendar, Call logs, and Contacts)
- Provisioning Server
- BroadSoft Directory
- Corporate Directory
- Ribbon Communications PAB-GAB Directory

The phone immediately sends the change in service connectivity status to the cloud. For example, if the Microsoft Exchange server gets an authentication failure, the failed authentication details are sent to cloud immediately.

If there's no change in the service connectivity status, the phone periodically sends the status to the cloud based on the configured interval. The phone also sends the last access time of the service to the server along with response codes and failure reason if any.

## Hardware Analytics

Poly phones send hardware analytics to the cloud at periodic intervals when you set the `da.supported.services` value to `all` or `hardwareanalytics`.

Poly phones send and upload the following hardware analytics and information to the cloud:

- **CPU Monitoring Service** – Sends CPU details for software processes along with total CPU consumed, Timestamp, and Monotonic time. You can set the values for trigger points such as `UpperCPUValue` and `LowerCPUValue` in percentage from the cloud. The following actions trigger the phone to send CPU details to the cloud:
  - The CPU usage value equals or goes above the `UpperCPUValue`.
  - The CPU usage value equals or goes below the `LowerCPUValue`.
  - The `UpperCPUValue` and `LowerCPUValue` are 0.

The phone collects the records at every defined time interval. On receiving a stop command from the cloud or after timeout, the phone sends the collected records to the cloud. However, if the number of records crosses the limit of 100, the records are sent to the cloud and the counter is reset.
- **Packet Loss Service** – Uploads L2 layer network statistics (received) to the cloud through Packet Loss Service. This service has the following Rx L2 parameters:
  - `rxDiscard`
  - `rxUnicastPkts`
  - `rxBroadcastPkts`
  - `rxMulticastPkts`

This service has the following fields:

- `eventMonotonicTime` – Time since DUT is up.
- `uploadTime` – Time at which DUT sends the packet to the cloud.
- `versionInfo` – Every INLINE message sent to cloud contains the `versionInfo` parameter to indicate version of that message. Minor or major version change depends on type of change with respect to particular message in subsequent releases.

The following action triggers the phone to send packet loss details to the cloud:

- Timeout
- Manually stopping service by issuing stop request

This service is applicable only for Ethernet.

- **Memory Monitoring Service** – Sends memory monitoring details for software processes along with total used, cached, and free memory to the cloud.

Memory metrics is controlled through two parameters: `UpperMemoryValue` and `LowerMemoryValue`. The following actions trigger the phone to send memory monitoring details to the cloud:

- Free memory is equal to and below `LowerMemoryValue` (Normal to Low memory)
- Free memory is equal to and above `UpperMemoryValue` (Low to Normal memory)

When you define `LowerMemoryValue` and `UpperMemoryValue` as 0, memory information is shared with the cloud periodically.

## Device Details Sent to the Cloud

When you enable device analytics, the phones can send various details regarding the device to the cloud service.

### Device Asset Details

Device asset details include details for a primary device and SIP service. A primary device consists of Poly phones, and a secondary device consists of Bluetooth or USB headsets, expansion modules (if supported), connected cameras, and a PC port.

When you enable device analytics, the phone sends the following primary device details to the cloud:

- Manufacturer
- Product Family
- Power Source
- MAC Address
- PCS Number
- PCS Account Code
- Region Code
- Version Information
- Hardware Model
- Hardware Revision
- Hardware Part number
- Serial Number
- OBi Number
- Offset GMT
- Reboot Type
- Mac Address
- Software Release
- Upload Time
- Updater Version

### Secondary Device Details

When you connect a secondary device to a Poly phone and enable device analytics with the parameter `da.supported.services` value set as `all` or `sdi`, the secondary device details are sent to the cloud.

The following table lists six secondary devices and the device details they send to the cloud:

## Secondary Device Details

Bluetooth Headset	USB Headset	Expansion Module	PC Port	Polycom EagleEye Mini USB Camera
<ul style="list-style-type: none"> <li>▪ Connection Type</li> <li>▪ Peripheral Type</li> <li>▪ Display Name</li> <li>▪ Bluetooth Address</li> </ul>	<ul style="list-style-type: none"> <li>▪ Display Name</li> <li>▪ Connection Type</li> <li>▪ Peripheral Type</li> <li>▪ Power Source</li> </ul>	<ul style="list-style-type: none"> <li>▪ Display Name</li> <li>▪ Connection Type</li> <li>▪ Serial Number</li> <li>▪ Peripheral Type</li> </ul>	<ul style="list-style-type: none"> <li>▪ Mac Address</li> <li>▪ Display Name</li> <li>▪ PC Port Status</li> <li>▪ PC Port Speed</li> <li>▪ PC Port Mode</li> <li>▪ Connection Type</li> <li>▪ Peripheral Type</li> <li>▪ Serial Number</li> </ul>	<ul style="list-style-type: none"> <li>▪ Connection Type</li> <li>▪ Display Name</li> <li>▪ Peripheral Type</li> <li>▪ Power Source</li> <li>▪ Software Version</li> <li>▪ Serial Number</li> </ul>

## Service Details

When you enable device analytics and set the `da.supported.services` parameter value to `all` or `service`, the phone sends certain information to the cloud.

The phone sends the following SIP service details to the cloud:

- Registration Type
- SIP Server Address
- SIP User Registration Address
- SIP User ID
- Transport Protocol
- SIP Port
- Outbound Proxy Address
- Outbound Proxy Transport Protocol
- Outbound Proxy Port
- Line Type
- Display Name
- Registration Status
- Registration Refresh Time
- Registration Failure Reason
- Server Platform
- Registration Line Index

## Device Network Details

When the phone's network boots up or when there's a change in network parameters, the phone sends device network details to Polycom Cloud Services.

Poly phones send network information for the Ethernet to the cloud when the phone is idle and send Wi-Fi information to the cloud at any time.

When you enable device analytics and set the `da.supported.services` parameter value to `all` or `ni`, the phone sends the following device network details for Ethernet to the cloud:

- Connection Type
- IPv4 Address
- IPv4 Subnet
- IPv4 Gateway
- VLAN
- IPv4 Address Source
- Interface Name
- DNS Primary Address
- DNS Alternative Address
- DNS Domain
- Connection Speed
- PC Port Status
- LLDP Status
- LLDP Neighbors
- LLDP Location Information
- CDP Status
- 802.1x Status
- NTP Server
- EAP Method
- Provisioning Protocol
- Connection Mode

When Poly phones are connected to a wireless network, the phones send the following network details for the wireless network to the cloud:

- IPv4 Subnet
- Upload Time
- Version Information
- Wifi Channel
- Connection Type
- Regulatory Domain
- IPv4 Address
- IPv4 Gateway
- DNS Primary Address
- DNS Alternative Address
- Interface Name
- IPv4 Address Source
- DNS Domain
- EAP Method
- Provisioning Protocol

- MIC Error Count
- EAP Error Count
- NTP Server

## VQMon Reports

Generate multiple types of performance metrics using the Voice Quality Monitoring (VQMon) parameters.

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.

Some reports 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. The phone generates some metrics using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

## Configure VQMon Alerts

Configure settings used to generate VQMon alert reports.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Specify the threshold value of listening MOS score (MOS-LQ) that causes the phone to send a critical alert quality report.

The default is 0. The value ranges from 0 to 40.

```
voice.qualityMonitoring.collector.alert.moslq.threshold.critical="x"
```

2. Specify the threshold value of listening MOS score (MOS-LQ) that causes phone to send a warning alert quality report.

The default is 0. The value ranges from 0 to 40.

```
voice.qualityMonitoring.collector.alert.moslq.threshold.warning="x"
```

3. Specify the threshold value of one way-delay, in milliseconds, that causes the phone to send a critical alert quality report.

The default is 0. The value ranges from 0 to 2000.

```
voice.qualityMonitoring.collector.alert.delay.threshold.critical="x"
```

---

**Note:** One-way delay includes both network delay and end system delay.

4. Specify the threshold value of one-way delay, in milliseconds, that causes the phone to send a critical alert quality report.

The default is 0. The value ranges from 0 to 2000.

```
voice.qualityMonitoring.collector.alert.delay.threshold.warning="x"
```

---

**Note:** One-way delay includes both network delay and end system delay.

---

## Configure VQMon Reports

Configure the settings used to generate periodic- and session-based VQMon reports.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

### Procedure

1. Enable periodically generated reports throughout the call.

```
voice.qualityMonitoring.collector.enable.periodic="1"
```

2. Enable reports to generate after the call.

```
voice.qualityMonitoring.collector.enable.session="1"
```

3. Configure the state that triggers the report.

- 0 (Default) - Alert states do not cause periodic reports to be generated.
- 1 - Periodic reports are generated if an alert state is critical.
- 2 - Period reports are generated when an alert state is either warning or critical.

---

**Note:** The phone ignores this parameter when you enable `voice.qualityMonitoring.collector.enable.periodic`, since reports are sent throughout the duration of a call.

---

```
voice.qualityMonitoring.collector.enable.triggeredPeriodic="<value>"
```

4. Configure the time interval, in milliseconds, between successive periodic quality reports.

The default is 20. The value range is 5 to 900.

```
voice.qualityMonitoring.collector.period="<value>"
```

## Monitoring the Phone's Memory Usage

If you're using a range of phone features, customized configurations, or advanced features, you might need to manage phone memory resources.

If your deployment includes a combination of phone models, consider configuring each phone model separately with its own features instead of applying all features to all models.

For best performance, the phone should use no more 95% of its available memory. When the phone memory runs low on resources, you may notice one or more of the following symptoms:

- The phone reboots or freezes up.
- The phone doesn't download all ringtones, directory entries, backgrounds, or XML dictionary files.

## Phone Memory Resources

If you need to free up memory on your phone, review the following table for the amount of memory each customizable feature uses. You can then reduce the amount of memory you need the feature to use.

### Phone Memory Resources

Feature	Typical Memory Size	Description
Custom idle display image	15 KB	The average size of the display image is 15 KB. Custom idle display image files should also be no more than 15 KB.
Local contact directory	42.5 KB	<p>The phones are optimized to display a maximum of 250 contacts. Each contact has four attributes and requires 170 B. A local contact directory of this size requires 42.5 KB.</p> <p>To reduce memory resources used by the local contact directory:</p> <ul style="list-style-type: none"> <li>▪ Reduce the number of contacts in the directory.</li> <li>▪ Reduce the number of attributes per contact.</li> </ul>
Corporate directory	Varies by server	<p>The phones are optimized to corporate directory entries with five to eight contact attributes each. The size of each entry and the number of entries in the corporate directory vary by server.</p> <p>If the phone can't display directory search results with more than five attributes, make additional memory resources available by reducing memory requirements of another feature.</p>
Ringtones	16 KB	<p>The ringtone files range in size from 30 KB to 125 KB. If you use custom ringtones, limit the file size to 16 KB.</p> <p>To reduce memory resources required for ringtones, reduce the number of available ringtones.</p>
Background images	8 KB to 32 KB	<p>The phones are optimized to display background images of 50 KB.</p> <p>To reduce memory resources required for background images, reduce the number and size of available background images.</p>
Local interface language	90 KB to 115 KB, depending on language	The language dictionary file used for the phone's user interface ranges from 90 KB to 115 KB for languages that use an expanded character set. To conserve memory resources, use XML language files for only the languages you need.
System web interface	250 KB to 370 KB	The system web interface (Web Configuration Utility) runs on a web browser.



## Check Memory Usage from the Local Interface

You can view a graphical representation of the phone's memory usage on the phone's local interface.

Before you check the memory usage, load and configure the features and files you want to make available on the phone's local interface.

### Procedure

1. Go to **Settings > Status > Diagnostics**.
2. Select **Graphs > Memory Usage**.

## Configure a Phone Memory Alert

Configure the alert when the phone's available memory falls below a percentage threshold.

If the phone's free memory falls below this threshold, the phone displays a warning message. The default setting is 20%. You can also configure the interval, in minutes, that the phone checks its available memory.

### Procedure

1. Adjust the available memory threshold percentage.

The default is 20. The value range is 20 to 40.

```
up.sysFreeMemThresholdPercent="<value>"
```

2. Set the interval, in minutes, that the phone checks its available memory.

The default is 0. The value range is 0 to 1440.

```
up.lowSysMemWarn.timeInMins="<value>"
```

## Memory Usage Errors in the Application Log

Each time the phone's minimum free memory goes below about 5%, the phone displays a message in the application log that the minimum free memory has been reached.

The application log file is enabled by default. The file is uploaded to the provisioning server directory on a configurable schedule. You can also upload a log file manually.

## Capturing the Phone's Screen

Capture the phone's current screen as a saved image on your computer.

This can be helpful when explaining a problem or providing instructions.

## Enable Screen Capture

Enable screen capture and the **Screen Capture** option in the **Basic** menu.

---

**Important:** Configuring the following parameter(s) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

**Procedure**

1. Enable the screen capture feature.

```
up.screenCapture.value="1"
```

2. Enable the **Screen Capture** option in the **Basic** menu.

```
up.screenCapture.enabled="1"
```

**Capture the Phone's Screen**

Capture and save a screenshot of the phone's display.

Before you capture the phone's screen, locate and record the phone's IP address at **Status > Platform > Phone > IP Address**.

**Procedure**

1. On the device, go to **Settings > Basic > Preferences > Screen Capture** and select **Enabled**.

**Note:** You must repeat this step each time the device restarts or reboots.

2. Set the phone to the screen you want to capture.
3. In a web browser, enter `https://<phoneIPAddress>/captureScreen`.
4. Enter the username `Polycom` and the phone's current administrator password.

The web browser displays an image showing the phone's current screen. You can save the image as a `.bmp` or `.jpg` file.

**Rebooting the Phone**

Reboot the phone when you want to send configuration changes that require a phone reboot.

Configure your phone to reboot in the following scenarios:

- At a scheduled time
- When paired to a network device

**Reboot the Phone**

Reboot the phone from the local interface when you want to send configuration changes that require a phone reboot.

Parameters that require a reboot are marked in this guide. If a configuration change doesn't require a reboot, you can update the configuration.

**Procedure**

- » Do one of the following:
  - Go to **Settings > Advanced > Reboot Phone**.
  - Go to **Settings > Basic > Update Configuration**.

If new software is available on the provisioning server, the phone downloads the software and immediately reboots.

## Reboot the Phone at a Scheduled Time

Configure your phones to reboot at a scheduled time, time period, or day.

### Procedure

1. Enable scheduled reboot on the phone.

```
prov.scheduledReboot.enabled="1"
```

2. Specify the time, in days, between scheduled reboots.

The default is 1. The value range is 1 to 365.

```
prov.scheduledReboot.periodDays="<value>"
```

3. Specify a time to reboot the phone. Use 24-hour time format (hh:mm).

The default is 03:00.

```
prov.scheduledReboot.time="<value>"
```

4. Optional: Set to a specific time to randomize the scheduled reboot between the time you set for `prov.scheduledReboot.time` and this parameter. Use 24-hour time format (hh:mm).

The default is Null.

```
prov.scheduledReboot.timeRandomEnd="<value>"
```

## Disable the Phone Boot Status Message

By default, the phone displays its status IP address, VLAN ID, provisioning status, and SNTP status in a dialog every time it reboots. Prevent the message from displaying.

---

**Note:** Reboot status may not be in sync or as expected due to limitation on network activity.

---

### Procedure

- » Disable the phone's boot status dialog.

```
up.phoneBootStatusPopupEnabled="0"
```

## Upgrading the Software

The upgrade process varies depending on the software version that is currently running on your phones and the version that you want to upgrade to.

New software versions may offer only small enhancements to improve the user experience, or they may be large software upgrades that offer new features.

## Upgrading the Software on a Single Phone

Use the **Software Upgrade** tool in the system web interface to update the software version on a single phone.

For instructions, see *Use the Software Upgrade Tool in the Web Configuration Utility: Feature Profile 67993* at [Poly Engineering Advisories and Technical Notifications](#).

Configuration changes made to individual phones using the system web interface override configuration settings made using central provisioning.

## Configure User-Controlled Software Updates and Polling

Upgrade software with the user-controlled software upgrade feature.

Set a polling policy and polling time period at which the phone polls the server for software updates and displays a notification on the phone to update software. For example, if you set the polling policy to poll every four hours, the phone polls the server for new software every four hours and displays a notification that says a software update is available. Users can choose to update the software right then, or they can postpone it a maximum of three times for up to six hours. The phone automatically updates the software after three postponements or after six hours, whichever comes first.

If a user postpones a software update, configuration changes and software version updates from both the server and the system web interface postpone as well. The server and system web interface send their configuration and software version changes to the phone when the user chooses to update.

You can send earlier or later versions of the software to your users' phones. User-controlled updates apply to configuration changes and software updates you make on the server and the system web interface.

This feature doesn't work if you enable ZTP.

### Procedure

1. Enable user-controlled software updates.

```
prov.usercontrol.enabled="1"
```

2. Display the **Ignore** and **Ignore until next Reboot/Sync** options during a software upgrade alert. This gives users the option to completely ignore software updates or defer them until the next reboot or sync event.

```
prov.usercontrol.optionToIgnore="1"
```

3. Optional: Adjust the postponement duration using the HH:MM format.

The default is 02:00 (2 hours).

```
prov.usercontrol.postponeTime="<HH:MM>"
```

## Upgrade UC Software Using a USB Flash Drive

Use a USB flash drive to upgrade the software on your phone.

---

**Note:** Changes you make using a USB flash drive override the settings you configure using a centralized provisioning server (if applicable).

---

## Procedure

1. Do one of the following:
  - Format a blank USB 2.0 USB flash drive using FAT32.
  - Delete all files from a previously formatted USB flash drive.
2. Download the UC software from the [Poly Online Support Center](#).
3. Copy the configuration files you want to use to the root of the USB flash drive.  
 You must copy at least the primary configuration file (00000000000000000000.cfg) and the product-specific configuration files to the USB flash drive:
  - Poly CCX 400: 3111-49700-001.sip.ld
  - Poly CCX 500: 3111-49710-001.sip.ld
  - Poly CCX 600: 3111-79770-001.sip.ld
  - Poly CCX 700: 3111-49740.001.sip.ld
4. Insert the USB flash drive into the USB port.  
 The phone detects the flash drive automatically.
5. Enter the administrator password.  
 The phone starts the update within 30 seconds of entering the correct administrator password.  
 The system may reboot several times during the update. The update is complete when the indicator lights stop flashing and the **Home** screen displays.

# Resetting a Phone to Factory Defaults

Reset the entire phone or some of the phone's configurations to factory defaults using the local interface.

## Reset the Phone and Configuration

You can reset the phone and phone configuration partially or completely.

## Procedure

1. Go to **Settings > Advanced > Administration Settings**.
2. Select **Reset to Defaults** and choose a reset option:
  - **Reset Local Configuration:** Clears the override file generated when you make changes using the phone's local interface.
  - **Reset Web Configuration:** Clears the override file generated by changes made using the system web interface.
  - **Reset Cloud Configuration:** Clears any configuration received from the configuration source identified by `cfgParamSourceCloud`.
  - **Reset Device Settings:** Resets the phone's flash file system settings not stored in an override file. These settings 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 phone's flash file system and deletes the software application, log, configuration, and override files. Note that if the override file is stored on the provisioning server, the phone redownloads the override file when you provision the phone again. Formatting the phone's file system doesn't delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the phone.

- **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.
- **Reset to Factory Partial:** 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, updater, and administrator password remain intact.
- **Reset User Data:** Resets the call list and removes all contacts from the phone and server.
- **Out-of-Box Wizard:** Resets the selections made during the initial out-of-box setup wizard. You can then make the selections again, and the phone reboots.

## Factory Reset the Phone at Power-Up

### Symptom:

You need to factory reset the phone but you don't have access to the phone menu or the system web interface.

### Workaround

Factory reset your phone using the phone's hardware (hard reboot).

Factory resetting the phone clears the flash parameters, removes user and cached data, and resets the administrator password.

---

**Note:** It may take several tries to get the timing right or to find the correct spots to press on the LCD display.

---

### Procedure

1. On a CCX 400 phone
  1. Disconnect the power, then power on the Poly phone.
  2. Do one of the following:
    - On a CCX 400, as soon as the message waiting light turns red, press all four corners of the display.
    - On a CCX 500, CCX 600, or CCX 700 phone, as soon as the Poly logo appears for the second time, double-tap all four corners of the display.
  3. Release the LCD when it displays "Recovery Mode Initiated..."
- The Poly logo appears, and then phone enters Recover Mode.

## Enable Users to Reset the Phone to Factory

By default, only administrators can initiate a factory reset. However, you can make the **Reset to Factory** setting available to users.

### Procedure

1. Display the **Reset to Factory** option under the **Basic** settings.

```
up.basicSettings.factoryResetEnabled="1"
```

2. Optional: Adjust which settings the phone resets when a user performs a factory reset. You can preserve just the administrator password or the administrator password and the provisioning settings.

To preserve just the administrator password, set the following parameters:

```
device.system.recoveryType="PreserveAdmin"
```

To preserve the administrator password and the provisioning settings, set the following parameters:

```
device.system.recoveryType="PreserveAdmin"
```

# Troubleshooting

---

## Topics:

- [Record Your Phone's Version Information](#)
- [System Logs](#)
- [View the Phone's Status](#)
- [Upload a Phone's Configuration Files](#)
- [Test Phone Hardware](#)
- [Perform Network Diagnostics](#)
- [Configure Remote Packet Capture](#)
- [Updater Error Messages and Possible Solutions](#)
- [Polycom UC Software Error Messages](#)
- [Network Authentication Failure Error Codes](#)
- [Power and Start-up Issues](#)
- [Screen and System Access Issues](#)
- [Calling Issues](#)
- [Display Issues](#)
- [Audio Issues](#)
- [Software Upgrade Issues](#)
- [Provisioning Issues](#)

The following sections address issues you might encounter when configuring phones, along with suggested actions to resolve them.

## Record Your Phone's Version Information

Record your phone's version information and save it in a safe place. You may need it when contacting technical support.

### Procedure

1. Go to **Settings > Status > System Information**.
2. In the **System Information** screen, record the following:
  - Model(s)
  - Updater signature
  - Version
  - Platform



# System Logs

System log files assist when troubleshooting issues.

System log files contain information about system activities and the system configuration profile. After you set up system logging, you can retrieve system log files.

The detailed technical data in the system log files can help Poly Global Services resolve problems and provide technical support for your system. Your support representative may ask you to download log archives and send them to Poly Global Services.

You must contact Poly Customer Support to obtain the template file (`techsupport.cfg`) that contains the parameters that configure log levels.

For information on configuring system log parameters, refer to the *Poly CCX Business Media Phone Parameter Reference Guide*.

## Configuring Log Files

Configure how the phone creates log files.

Log file names use the following format: `[MAC address]_[Type of log].log`. For example, if the MAC address of your phone is `0004f2203b0`, the app log file name is `0004f2203b0_app.log`.

The phone writes information into several different log files. The following list describes the type of information in each type of log file.

- **Boot Log** – The phone sends boot logs to the provisioning server in a `boot.log` file collected from the Updater/BootROM application each time the phone boots up. The BootROM/Updater application boots the application and updates with the new firmware if available.
- **Application Log** – The application log file contains complete phone functionality including SIP signaling, call controls and features, digital signal processor (DSP), and network components.
- **Syslog** – For more information about **Syslog**, see [Syslog on Polycom Phones - Technical Bulletin 17124](#).

## Logging Levels

The event logging system supports the classes of events listed in the table Logging Levels.

The phone supports two types of logging:

- Level, change, and render
- Schedule

---

**Note:** Logging parameter changes can impair system operation. Don't change any logging parameters without prior consultation with Technical Support.

---

### Logging Levels

Logging Level	Description
0	Debug only
1	High detail class event

Logging Level	Description
2	Moderate detail event class
3	Low detail event class
4	Minor error
5	Major error – will eventually incapacitate the system
6	Fatal error

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

- Time or time/date stamp, in one of the following formats:
  - 0 - 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
- 1-5 character component identifier (such as "so")
- Event class
- Cumulative log events missed due to excessive CPU load
- The event description

## Upload Logs to a USB Flash Drive

Configure your phones to copy application and boot logs to a USB flash drive connected to the phone.

You can configure the phone to copy the application logs to the USB flash drive when the log file size reaches the limit defined in the `log.render.file.size` parameter. Similarly, you can configure the phone to copy application logs to the USB flash drive periodically using `log.render.file.upload.period` parameter.

### Procedure

- » Enable the phone to upload logs to a connect USB flash drive.

```
feature.usbLogging.enabled="1"
```

## Retrieve Logs Using the System Web Interface

You can view and export log files using a phone's system web interface.

### Procedure

1. Log in to the system web interface as an administrator
2. Go to **Diagnostics > View & Download Logs > Audit**.

## Retrieve Logs from the Support Information Package

Export the **Support Information Package** (.tar file) using the system web interface.

The support information package includes the following log files:

- PBU file
- App log file
- Boot log file
- Audit log file

### Procedure

1. Log in to the system web interface as an administrator.
2. Go to **Diagnostics > Download Support Information Package** and download the support information package.
3. On your computer, unzip the .tar file to view the log files.

## View the Phone's Status

Troubleshoot phone issues by viewing the phone's **Status** menu.

### Procedure

1. Go to **Settings > Status** and select a status menu item.
2. View the following information:

Menu Item	Available Information
System Information	<ul style="list-style-type: none"> <li>• Model</li> <li>• Part Number</li> <li>• Platform (Profile)</li> <li>• MAC Address</li> <li>• Wi-Fi MAC Address (on supported models)</li> <li>• Bluetooth MAC Address (on supported models)</li> <li>• IP Address</li> <li>• Version</li> <li>• Updater Signature</li> <li>• System Name</li> </ul>
Platform	<ul style="list-style-type: none"> <li>• Phone's serial number or MAC address</li> <li>• Current IP address</li> <li>• Updater version</li> <li>• Application version</li> <li>• Names of the configuration files in use</li> <li>• Address of the provisioning server</li> </ul>

Menu Item	Available Information
Network	<ul style="list-style-type: none"> <li>• TCP/IP Setting</li> <li>• Ethernet port speed</li> <li>• Connectivity status of the PC port (if it exists)</li> <li>• Statistics on packets sent and received since last boot</li> <li>• Last time the phone rebooted</li> <li>• Call Statistics showing packets sent and received on the last call</li> </ul>
Lines	<ul style="list-style-type: none"> <li>• Detailed status of each of the phone's configured lines</li> </ul>
Diagnostics	<ul style="list-style-type: none"> <li>• Hardware tests to verify correct operation of the microphone, speaker, handset, and third-party headset, if present</li> <li>• Hardware tests to verify correct operation of the microphones and speaker</li> <li>• Tests to verify proper functioning of the phone keys</li> <li>• List of the functions assigned to each of the phone keys</li> <li>• Real-time graphs for CPU, network, and memory use</li> </ul>
Licenses	Reports licenses installed on the phone.
Location Information	Reports the phone's location information if it's available.
Calendar	<ul style="list-style-type: none"> <li>• Reports the calendar server, domain, user, and reminder status.</li> <li>• Provides an option to disconnect from the calendar server.</li> </ul>

## Upload a Phone's Configuration Files

Upload the phone's current configuration files from the local interface or the system web interface to the provisioning server to help debug configuration problems.

You can upload a configuration file for every active source as well as the current nondefault configuration set.

### Procedure

1. Go to **Settings > Advanced > Admin Settings > Upload Configuration**.
2. Choose the files to upload:
  - **All Sources**
  - **Configuration Files**
  - **Local**
  - **Web**
  - **SIP**
  - **Cloud**

If you select **All Sources**, the phone uploads the `<MACaddress>-update-all.cfg` file.

If you use the system web interface, you can also upload **Device Settings**.

### 3. Select **Upload**.

The phone uploads the configuration file to the location you specified in the `prov.configUploadPath` parameter.

## Test Phone Hardware

Test the phone's hardware directly from the phone's local interface.

### Procedure

1. Go to **Settings > Status > Diagnostics > Test Hardware**.
2. Choose from these tests:
  - **Audio Diagnostics**: Test the speaker, microphone, handset, and a third-party headset.
  - **Display Diagnostics**: Test the LCD for faulty pixels.
  - **Touch Screen Diagnostics**: Test the touchscreen response.
  - **Brightness Diagnostics**: Test the screen brightness.

## Perform Network Diagnostics

You can use ping and traceroute to troubleshoot network connectivity problems.

### Procedure

1. Go to **Settings > Status > Diagnostics > Network**.
2. Choose one of the following:
  - **Ping**
  - **Trace Route**
3. Enter a URL or IP address.
4. Press **Start**.

## Configure Remote Packet Capture

Configure the phone to capture data packets that may help troubleshoot issues.

---

**Important:** Dependencies and overrides may affect other parameters. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

---

The phone generates core files when errors occur by default.

### Procedure

1. Enable all onboard packet capture features.

```
diags.pcap.enabled="1"
```

2. Enable the remote packet capture server.

```
diags.pcap.remote.enabled="1"
```

3. Optional: Configure the remote packet capture password. The phone's MAC address is the default password.

```
diags.pcap.remote.password="<alphanumeric password>"
```

4. Optional: Configure the remote packet port number. The default is port 2002.

```
diags.pcap.remote.port="<TCP port>"
```

## Updater Error Messages and Possible Solutions

If a fatal error occurs, the phone doesn't boot up.

If the error isn't fatal, the phone boots up but its configuration might be changed. Most updater errors are logged to the phone's boot log. However, if the phone is having trouble connecting to the provisioning server, the phone is not likely to upload the boot log.

The following table describes possible solutions to updater error messages.

Error Message	Cause and Possible Solution
Failed to get boot parameters via DHCP	<p>The phone doesn't have an IP address and therefore can't boot.</p> <ul style="list-style-type: none"> <li>• Check that all cables are connected, the DHCP server is running, and that the phone has not been set to a VLAN that is separate from the DHCP server.</li> <li>• Check the DHCP configuration.</li> </ul>
Application <file name> is not compatible with this phone!	<p>An application file was downloaded from the provisioning server, but it cannot be installed on this phone.</p> <p>Install a compatible software image on the provisioning server. Be aware that there are various hardware and software dependencies.</p>
Could not contact boot server using existing configuration	<p>The phone cannot contact the provisioning server. Possible causes include:</p> <ul style="list-style-type: none"> <li>• Cabling issues</li> <li>• DHCP configuration</li> <li>• Provisioning server problems</li> </ul> <p>The phone can recover from this error so long as it previously downloaded a valid application BootROM image and all of the necessary configuration files.</p>

Error Message	Cause and Possible Solution
Error, application is not present!	<p>The phone does not have an application stored in device settings and cannot boot because an application could not be downloaded.</p> <ul style="list-style-type: none"> <li>Download compatible Polycom UC Software to the phone using one of the supported provisioning protocols.</li> </ul> <p>If no provisioning server is configured on the phone, enter the provisioning server details after logging in to the Updater menu and navigating to the Provisioning Server menu.</p>

## Polycom UC Software Error Messages

If an error occurs in the UC Software, an error message and a warning icon displays on the phone.

Find the warnings menu by going to **Settings > Status > Diagnostics > Warnings**.

The following table describes Polycom UC Software error messages.

### Polycom UC Software Error Messages

Error Message	Cause
<p>Config file error: Files contain invalid params: &lt;filename1&gt;, &lt;filename2&gt;,...</p> <p>Config file error: &lt;filename&gt; contains invalid params</p> <p>The following contain pre-3.3.0 params: &lt;filename&gt;</p>	<p>These messages display if the configuration files contain these deprecated parameters:</p> <ul style="list-style-type: none"> <li>tone.chord.ringer.x.freq.x</li> <li>se.pat.callProg.x.name</li> <li>ind.anim.IP_500.x.frame.x.duration</li> <li>ind.pattern.x.step.x.state</li> <li>feature.2.name</li> <li>feature.9.name</li> </ul> <p>This message also displays if any configuration file contains more than 100 of the following errors:</p> <ul style="list-style-type: none"> <li>Unknown parameters</li> <li>Out-of-range values</li> <li>Invalid values.</li> </ul> <p>To check that your configuration files use correct parameter values, refer to Using Correct Parameter XML Schema, Value Ranges, and Special Characters.</p>
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 on the phone: Status > Basic > Login Credentials.

Error Message	Cause
Missing files, config. reverted	This message displays when errors in the configuration and a failure to download the configuration files force the phone to revert to its previous (known) condition with a complete set of configuration files. This also displays if the files listed in the <MAC Address>.cfg file are not present on the provisioning server.
Network link is down	Indicates that the phone cannot establish a link to the network and persists until the link problem is resolved. Call-related functions, and phone keys are disabled when the network is down but the phone menu works.

## Network Authentication Failure Error Codes

Error messages display on the phone if 802.1X authentication fails.

The error codes display on the phone when you press the **Details** key. Error codes are also included in the log files.

Event Code	Description	Comments
1	Unknown events	An unknown event by '1' can include any issues listed in this table.
2	Mismatch in EAP Method type Authenticating server's list of EAP methods doesn't match with clients'.	
30xxx	TLS Certificate failure 000 - Represents a generic certificate error. The phone displays the following codes: <ul style="list-style-type: none"> <li>• 042 - bad cert</li> <li>• 043 - unsupported cert</li> <li>• 044 - cert revoked</li> <li>• 045 - cert expired</li> <li>• 046 - unknown cert</li> <li>• 047 - illegal parameter</li> <li>• 048 - unknown CA</li> </ul>	See section 7.2 of <a href="#">RFC 2246</a> for further TLS alert codes and error codes.



Event Code	Description	Comments
31xxx	<p>Server Certificate failure</p> <p>'xxx' can use the following values:</p> <ul style="list-style-type: none"> <li>• 009 - Certificate not yet Valid</li> <li>• 010 - Certificate Expired</li> <li>• 011 - Certificate Revocation List</li> <li>• (CRL) not yet Valid</li> <li>• 012 - CRL Expired</li> </ul>	
4xxx	<p>Other TLS failures</p> <p>'xxx' is the TLS alert message code). For example, if the protocol version presented by the server is not supported by the phone, then 'xxx' is 70, and the EAP error code is 4070.</p>	See section 7.2 of <a href="#">RFC 2246</a> for further TLS alert codes and error codes.
5xxx	<p>Credential failures</p> <p>5xxx - wrong user name or password</p>	
6xxx	<p>PAC failures:</p> <ul style="list-style-type: none"> <li>• 080 - No PAC file found</li> <li>• 081 - PAC file password not provisioned</li> <li>• 082 - PAC file wrong password</li> <li>• 083 - PAC file invalid attributes</li> </ul>	
7xxx	<p>Generic failures:</p> <ul style="list-style-type: none"> <li>• 001 - dot1x can not support (user) configured EAP method</li> <li>• 002 - dot1x can't support (user) configured security type</li> <li>• 003 - root certificate couldn't be loaded</li> <li>• 174 - EAP authentication timeout</li> <li>• 176 - EAP Failure</li> <li>• 185 - Disconnected</li> </ul>	

## Power and Start-up Issues

The following table describes possible solutions to power and start-up issues.

Power or Start-up Issue	Possible Solutions:
The phone has power issues or the phone has no power.	<p>Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Verify that no lights appear on the unit when it is powered up.</li> <li>• Check to see if the phone is properly plugged into a functional AC outlet.</li> <li>• Make sure that the phone isn't plugged into an outlet controlled by a light switch that is turned off.</li> <li>• If the phone is plugged into a power strip, try plugging directly into a wall outlet instead.</li> </ul>
The phone doesn't boot.	<p>If the phone doesn't boot, there may be a corrupt or invalid firmware image or configuration on the phone:</p> <ul style="list-style-type: none"> <li>• Ensure that the provisioning server is accessible on the network and a valid software load and valid configuration files are available.</li> <li>• Ensure that the phone is configured with the correct address for the provisioning server on the network.</li> </ul>

## Screen and System Access Issues

The following table describes possible solutions to screen and system access issues.

Issue	Cause and Possible Solution
There is no response from feature key presses.	<p>If your phone keys do not respond to presses:</p> <ul style="list-style-type: none"> <li>• Press the keys more slowly.</li> <li>• Check to see whether or not the key has been mapped to a different function or disabled.</li> <li>• Make a call to the phone 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.</li> <li>• On the phone, go to <b>Menu &gt; Status &gt; Lines</b> to confirm the line is actively registered to the call server.</li> </ul> <p>Reboot the phone to attempt re-registration to the call server. Go to <b>Menu &gt; Settings &gt; Advanced &gt; Reboot Phone</b>).</p>

Issue	Cause and Possible Solution
The display shows the message "Network Link is Down".	<p>This message displays when the LAN cable is not properly connected. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Check the termination at the switch or hub end of the network LAN cable.</li> <li>• Check that the switch or hub is operational (flashing link/status lights).</li> <li>• On the phone, go to <b>Menu &gt; Status &gt; Network</b>. Scroll down to verify that the LAN is active.</li> <li>• Ping the phone from a computer.</li> </ul> <p>Reboot the phone to attempt re-registration to the call server. Go to <b>Menu &gt; Settings &gt; Advanced &gt; Reboot Phone</b>).</p>

## Calling Issues

The following table provides possible solutions to common calling issues.

Issue	Cause and Possible Solution
There is no dial tone.	<p>If there is no dial tone, power may not be correctly supplied to the phone. Try one of the following:</p> <ul style="list-style-type: none"> <li>• Check that the display is illuminated.</li> <li>• Make sure the LAN cable is inserted properly at the rear of the phone; try unplugging and re-inserting the cable.</li> </ul> <p>If you are using in-line powering, check that the switch is supplying power to the phone.</p>
The dial tone is not present on one of the audio paths.	<p>If dial tone is not present on one of the audio paths, do one of the following:</p> <ul style="list-style-type: none"> <li>• Switch between handset, headset (if present), or hands-free speakerphone to see whether or not dial tone is present on another path.</li> <li>• If the dial tone exists on another path, connect a different handset or headset to isolate the problem.</li> </ul> <p>Check configuration for gain levels.</p>
The phone does not ring.	<p>If there is no ringtone but the phone displays a visual indication when it receives an incoming call, do the following:</p> <ul style="list-style-type: none"> <li>• Adjust the ring level from the front panel using the volume up/down keys.</li> </ul> <p>Check the status of handset, headset (if connected), and hands-free speakerphone.</p>

Issue	Cause and Possible Solution
The line icon shows an unregistered line icon.	If the phone displays an icon indicating that a line is unregistered, re-register the line and place a call.

## Display Issues

The following table provides tips for resolving display screen issues.

Issue	Cause and Possible Solution
There's no display or the display is incorrect.	<p>If there's no display, power may not be correctly supplied to the phone. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Check that the display is illuminated.</li> <li>• Make sure that the power cable is inserted properly at the rear of the phone.</li> <li>• If you're using PoE powering, check that the PoE switch is supplying power to the phone.</li> </ul> <p>Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to <a href="#">Capture Your Device's Current Screen</a>.</p>
The display is too dark or too light.	<p>The phone contrast may be set incorrectly. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Adjust the contrast.</li> <li>• Reboot the phone to obtain the default level of contrast.</li> </ul>
The display is flickering.	<p>Certain types of older fluorescent lighting may cause the display to flicker. If your phone is in an environment with fluorescent lighting, angle or move the Polycom phone away from the lights.</p>
The time and date are flashing.	<p>If the time and date are flashing, the phone is disconnected from the LAN or there's no SNTP time server configured. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Reconnect the phone to the LAN.</li> <li>• Configure an SNTP server.</li> </ul> <p>Disable the time and date if you don't want to connect your phone to a LAN or SNTP server.</p>

## Audio Issues

The following table describes possible solutions to audio issues.

Issue	Cause and Possible Solution
There is no audio on the headset	<p>If there is no audio on your headset, the connections may not be correct. Do one of the following:</p> <ul style="list-style-type: none"> <li>• Ensure the headset is plugged into the jack marked Headset at the rear of the phone.</li> <li>• Ensure the headset amplifier (if present) is turned on and adjust the volume.</li> </ul>

## Software Upgrade Issues

The following table describes possible solutions to issues that may occur during or after a software upgrade.

Issue	Cause and Possible Solutions
Some settings or features are not working as expected on the phone.	<p>The phone's configuration may be incorrect or incompatible.</p> <p>Check for errors on the phone by navigating to <b>Menu &gt; Status &gt; Platform &gt; Configuration</b>. If there are messages stating Errors Found, Unknown Params, or Invalid values, correct your configuration files and restart the phone.</p>
The phone displays a Config file error message for five seconds after it boots up.	<p>You are using configuration files from a UC Software version earlier than the UC Software image running on the phones. Configuration parameters and values can change each release and specific parameters may or may not be included. See the UC Software Administrator's Guide and Release Notes for the UC Software version you have installed on the phones.</p> <p>Correct the configuration files, remove the invalid parameters, and restart the phone.</p>

Issue	Cause and Possible Solutions
When using the system web interface to upgrade phone software, the phone is unable to connect to the Poly Hosted Server.	<p>Occasionally, the phone is unable to connect to the Poly-hosted server because of the following:</p> <ul style="list-style-type: none"> <li>• The Poly-hosted server is temporarily unavailable.</li> <li>• There is no software upgrade information for the phone to receive.</li> <li>• The network configuration is preventing the phone from connecting to the Poly hosted server.</li> </ul> <p>To troubleshoot the issue:</p> <ul style="list-style-type: none"> <li>• Try upgrading your phone later.</li> <li>• Verify that new software is available for your phone using the <a href="#">Poly UC Software Release Matrix</a>.</li> <li>• Verify that your network's configuration allows the phone to connect to <code>http://downloads.polycom.com</code>.</li> </ul> <p>If the issue persists, try manually upgrading your phone's software.</p>

## Provisioning Issues

If settings you make from the central server aren't working, check first for priority settings applied from the phone menu system or system web interface. Afterward, check for duplicate settings in your configuration files.