Poly Trio Solution

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

© 2019 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

Before You Begin......................................................................................................................... 14
   Audience, Purpose, and Required Skills..................................................................................... 14
   Related Poly and Partner Resources............................................................................................. 14

Getting Started.............................................................................................................................. 16
   Product Overview........................................................................................................................... 16
   Supported Phones and Accessories............................................................................................... 16
   Working with Polycom UC Software............................................................................................... 17
   UC Software Provisioning Methods............................................................................................... 17
   Record Version Information.......................................................................................................... 17

Supported Inbound and Outbound Ports...................................................................................... 18
   Inbound Ports for Poly Trio Systems.............................................................................................. 18
   Outbound Ports for Poly Trio System............................................................................................ 19
   Poly Trio Visual+ Network Ports.................................................................................................... 21
   Inbound Ports for Poly Trio VisualPro Systems............................................................................ 22
   Outbound Ports for Poly Trio VisualPro Systems.......................................................................... 22

Configuring Security Options....................................................................................................... 24
   Administrator and User Passwords................................................................................................. 24
      Change the Default Administrator Password on the Phone...................................................... 25
      Change the Default Passwords in the Web Configuration Utility.............................................. 25
      Administrator and User Password Parameters.......................................................................... 25
   Disabling External Ports and Features.......................................................................................... 26
      Disable Unused Ports and Features Parameters......................................................................... 27
   Visual Security Classification....................................................................................................... 28
      Visual Security Classification Parameters.................................................................................. 28
   Encryption...................................................................................................................................... 29
      Encrypting Configuration Files.................................................................................................. 29
      Configuration File Encryption Parameters............................................................................... 30
   Voice over Secure IP..................................................................................................................... 31
      VoSIP Parameter......................................................................................................................... 31
   Securing Phone Calls with SRTP.................................................................................................. 32
      SRTP Parameters....................................................................................................................... 32
   Enabling Users to Lock Phones.................................................................................................... 35
      Phone Lock Parameters.............................................................................................................. 35
   Locking the Basic Settings Menu.................................................................................................. 37
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Settings Menu Lock Parameter ............................................... 37</td>
</tr>
<tr>
<td>Secondary Port Link Status Report .................................................. 37</td>
</tr>
<tr>
<td>Secondary Port Link Status Report Parameters .................................... 38</td>
</tr>
<tr>
<td>802.1X Authentication ........................................................................ 39</td>
</tr>
<tr>
<td>802.1X Authentication Parameters .................................................... 39</td>
</tr>
<tr>
<td>SCEP Security Protocol ........................................................................ 40</td>
</tr>
<tr>
<td>SCEP Parameters ................................................................................. 40</td>
</tr>
<tr>
<td>Session Management on the Web Configuration Utility .......................... 43</td>
</tr>
<tr>
<td>Session Management Parameters .......................................................... 43</td>
</tr>
<tr>
<td>Certificates ....................................................................................... 44</td>
</tr>
<tr>
<td>Using the Factory-Installed Certificate ................................................ 45</td>
</tr>
<tr>
<td>Check for a Device Certificate ............................................................. 45</td>
</tr>
<tr>
<td>Customizing Certificate Use .................................................................. 46</td>
</tr>
<tr>
<td>Determining TLS Platform Profiles or TLS Application Profiles .............. 46</td>
</tr>
<tr>
<td>TLS Protocol Configuration for Supported Applications ....................... 49</td>
</tr>
<tr>
<td>TLS Parameters .................................................................................... 52</td>
</tr>
<tr>
<td>Configurable TLS Cipher Suites ........................................................... 55</td>
</tr>
<tr>
<td>Create a Certificate Signing Request ................................................... 56</td>
</tr>
<tr>
<td>Download Certificates .......................................................................... 56</td>
</tr>
<tr>
<td>Custom URL Location for LDAP Server CA Certificate ............................ 57</td>
</tr>
<tr>
<td>Custom URL Location for LDAP Server Certificates Parameter ................. 57</td>
</tr>
<tr>
<td>Confirm the Installed LDAP Server Certificates on the Phone ................. 57</td>
</tr>
<tr>
<td>Online Certificate Status Protocol ...................................................... 58</td>
</tr>
<tr>
<td>Online Certificate Status Protocol Parameter ....................................... 58</td>
</tr>
<tr>
<td>Updating the Software ........................................................................... 59</td>
</tr>
<tr>
<td>Upgrade UC Software Using a USB Flash Drive ...................................... 59</td>
</tr>
<tr>
<td>Updating UC Software on a Single Phone .............................................. 60</td>
</tr>
<tr>
<td>User-Controlled Software Update ....................................................... 60</td>
</tr>
<tr>
<td>User-Controlled Software Update Parameters ....................................... 60</td>
</tr>
<tr>
<td>Updating Camera Firmware ..................................................................... 61</td>
</tr>
<tr>
<td>Diagnostics and Status ......................................................................... 62</td>
</tr>
<tr>
<td>View the Phone's Status ....................................................................... 62</td>
</tr>
<tr>
<td>Test the Hardware .............................................................................. 63</td>
</tr>
<tr>
<td>Upload a Phone's Configuration ............................................................ 64</td>
</tr>
<tr>
<td>Perform Network Diagnostics ............................................................... 64</td>
</tr>
<tr>
<td>Restart a Paired Device ........................................................................ 64</td>
</tr>
<tr>
<td>Reboot Network Devices ....................................................................... 64</td>
</tr>
</tbody>
</table>
Rebooting the Poly Trio System at a Scheduled Time ...................................................... 65
Scheduled Reboot Parameters .................................................................................... 65
Reset the Poly Trio System to Factory Default Settings at Power-up ......................... 65
Reset the Poly Trio System to Factory Default Settings from the Home Menu............. 66
Reset the Poly Trio Visual+ to Factory Default Settings ............................................. 66
Reset the Phone and Configuration ........................................................................... 66
Reset to Factory Parameter ....................................................................................... 67
Access Video Transmission Diagnostics ...................................................................... 67
Status Indicators on the Poly Trio Solution ................................................................. 67
Monitoring the Phone's Memory Usage ...................................................................... 69
Check Memory Usage from the Phone ....................................................................... 69
View Memory Usage Errors in the Application Log .................................................. 69
Phone Memory Resources ......................................................................................... 69

Analytics Support for Polycom Cloud Services ......................................................... 71
Hardware Analytics .................................................................................................... 71
Device Details Sent to the Cloud ............................................................................... 73
Device Asset Details ................................................................................................... 73
Service Details ........................................................................................................... 73
Device Network Details .............................................................................................. 74
Call Experience Details ............................................................................................... 75
Call Data Record (CDR) ............................................................................................. 76
Device Diagnostics Details .......................................................................................... 76
Diagnostic Details for System Logs ............................................................................ 76
Diagnostic Details for Packet Capture ....................................................................... 77
Device Analytics Parameters ....................................................................................... 78
Poly Cloud Connector Parameters ............................................................................. 79
Turn Off the System Usage Data Collection .................................................................. 80

System Logs ................................................................................................................. 81
Configuring Log Files ................................................................................................. 81
Severity of Logging Event Parameter ......................................................................... 82
Log File Collection and Storage Parameters ............................................................. 82
Logging Levels ............................................................................................................ 84
Logging Level, Change, and Render Parameters for Poly Trio ..................................... 84
Logging Parameters .................................................................................................... 88
Upload Logs to the Provisioning Server ....................................................................... 89
Upload Poly Trio System Logs .................................................................................... 89
Uploading Logs to a USB Flash Drive .......................................................................... 90
USB Logging Parameter ............................................................................................. 90
Troubleshooting......................................................................................................................... 91
  Updater Error Messages and Possible Solutions................................................................. 91
  Polycom UC Software Error Messages............................................................................... 92
  Network Authentication Failure Error Codes.......................................................................... 93
  Power and Start-up Issues................................................................................................. 95
  Screen and System Access Issues...................................................................................... 96
  Calling Issues....................................................................................................................... 97
  Display Issues...................................................................................................................... 97
  Software Upgrade Issues..................................................................................................... 98
  Provisioning Issues............................................................................................................. 99
    Place the Poly Trio System into Recovery Mode.......................................................... 99
    Place Poly Trio Visual+ into Recovery Mode............................................................... 99

Content.................................................................................................................................. 101
  Content Sharing................................................................................................................... 101
    Content Sharing Parameters.......................................................................................... 101
    Polycom Content Application......................................................................................... 103
    Polycom People+Content IP.......................................................................................... 104
    Polycom People+Content IP over USB.......................................................................... 105
    HDMI and VGA Content Sharing Parameters.............................................................. 106
    Display Content Automatically While Idle...................................................................... 106
  Screen Mirroring.................................................................................................................. 107
    Screen Mirroring with AirPlay-Certified Devices......................................................... 107
    Screen Mirroring with Miracast-Certified Devices....................................................... 110

Hardware and Power for Poly Trio Systems........................................................................ 114
  Powering Poly Trio Systems............................................................................................... 114
    Powering the Poly Trio 8800.......................................................................................... 114
    Powering the Poly Trio 8500 System............................................................................. 114
    Power the Poly Trio 8800 System with the Optional Power Injector.............................. 115
    Powering the Poly Trio Visual+ Solution........................................................................ 115
  Poly Trio System Power Management................................................................................ 116
    Poly Trio 8500 System Power Management................................................................... 116
    USB Port Power Management......................................................................................... 116
    Using Power over Ethernet (POE) Class 0...................................................................... 116
    Using Power Sourcing Equipment Power (PoE PSE Power)............................................ 116
  Power-Saving on Poly Trio Systems.................................................................................. 117
    Power-Saving Parameters............................................................................................... 117
Pairing with Poly Trio Systems

Pairing Polycom EagleEye Director II Camera System with Poly Trio
Configure Poly Trio System DHCP for EagleEye Director II Pairing Process
Configure Poly Trio IP Address for EagleEye Director II Pairing Process
Pair Polycom EagleEye Director II Camera System

Pair the Poly Trio Visual+ or Trio VisualPro with Poly Trio Systems
Manually Pair with Poly Trio Systems
Poly Trio Visual+ Pairing Parameters
Poly Trio VisualPro Pairing Parameters
Identify Paired Devices
Place the Poly Trio Visual+ in Pairing Diagnostic Mode

Daisy-Chaining Poly Trio Systems
Daisy-Chaining Requirements
Poly Trio System Daisy-Chain Scenarios
Daisy-Chain Poly Trio Systems
Daisy-Chaining Parameters

Video Features for Poly Trio

Display a Monitor Index Number
Video Call Overlays
Video Call Overlay Parameters
Video Quality Parameters
Video and Camera Options
Video and Camera Parameters
Per-Camera Video Parameters
Camera Specific Presets
Camera Specific Preset Parameters
Supported Video Codecs with Poly Trio
Video Codec Parameters for Poly Trio
Toggling Between Audio-only or Audio-Video Calls
Audio-only or Audio-Video Call Parameters
H.323 Protocol
SIP and H.323 Protocol
Supported H.323 Video Standards
H.323 Protocol Parameters
I-Frames
Video Parameters
Video Codec Preference Parameters
Video Profile Parameters for Poly Trio
Phone Display Features

Administrator Menu on Poly Trio Systems

Administrator Menu Parameters

Poly Trio Visual+ and Trio VisualPro Monitor Display Options

Poly Trio Visual+ and Trio VisualPro Display Parameters

Poly Trio System Theme

Poly Trio System Theme Parameter

Poly Trio System Display Name

System Display Name Parameters

Poly Trio System Status Messages

Poly Trio System Status Message Parameters

Olson Time Zone Configuration

Olson Time Zone Parameters

Set an Olson Time Zone with the Web Configuration Utility

Set an Olson Time Zone from the Device Menu

Olson Time Zone IDs

Time Zone Location Description

Time Zone Location Parameters

Time and Date

Time and Date Display Parameters

Phone Languages

Change the Phone Language and Keyboard Layouts

Phone Language Parameters

Multilingual Parameters

Access the Country of Operation Menu in Set Language

Add a Language for the Phone Display and Menu

Hide the MAC Address

Hide MAC Address Parameters

Unique Line Labels for Registration Lines

Unique Line Labels for Registration Lines Parameters

Poly Trio System Number Formatting

Poly Trio System Number Formatting Parameters

Number or Custom Label

Configure the Number or Label from the System

Number and Label Parameters

Custom Icons for Contacts and Line Registrations

Custom Icon Parameters

Example: Configure an Icon for a Line Registration

Example: Set Icons for Speed Dial Contacts

Capture Your Device’s Current Screen
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Current Phone Screen Parameters</td>
<td>226</td>
</tr>
<tr>
<td>Default In-Call Screen</td>
<td>226</td>
</tr>
<tr>
<td>Default In-Call Screen Parameters</td>
<td>226</td>
</tr>
<tr>
<td>Custom Call Control Options</td>
<td>226</td>
</tr>
<tr>
<td>Custom Call Control Options Parameters</td>
<td>227</td>
</tr>
<tr>
<td>Poly Trio Home Screen Parameters</td>
<td>228</td>
</tr>
<tr>
<td><strong>Directories and Contacts</strong></td>
<td>230</td>
</tr>
<tr>
<td>Local Contact Directory</td>
<td>230</td>
</tr>
<tr>
<td>Local Contact Directory Parameters</td>
<td>230</td>
</tr>
<tr>
<td>Maximum Capacity of the Local Contact Directory on Poly Trio</td>
<td>232</td>
</tr>
<tr>
<td>Creating Per-Phone Directory Files</td>
<td>232</td>
</tr>
<tr>
<td>Local Contact Directory File Size Parameters</td>
<td>233</td>
</tr>
<tr>
<td>Speed Dials on Poly Trio Systems</td>
<td>236</td>
</tr>
<tr>
<td>Speed Dial Contacts Parameters</td>
<td>236</td>
</tr>
<tr>
<td>Corporate Directory</td>
<td>237</td>
</tr>
<tr>
<td>Corporate Directory Parameters</td>
<td>237</td>
</tr>
<tr>
<td>Call Lists</td>
<td>244</td>
</tr>
<tr>
<td>Call List Parameters</td>
<td>244</td>
</tr>
<tr>
<td>Call Log Elements and Attributes</td>
<td>245</td>
</tr>
<tr>
<td>Resetting Contacts and Recent Calls Lists on Poly Trio System</td>
<td>247</td>
</tr>
<tr>
<td><strong>Call Controls</strong></td>
<td>248</td>
</tr>
<tr>
<td>Microphone Mute</td>
<td>249</td>
</tr>
<tr>
<td>Microphone Mute Parameters</td>
<td>249</td>
</tr>
<tr>
<td>Persistent Microphone Mute</td>
<td>249</td>
</tr>
<tr>
<td>Persistent Microphone Mute Parameter</td>
<td>250</td>
</tr>
<tr>
<td>Answer Incoming Calls with Mute Button</td>
<td>250</td>
</tr>
<tr>
<td>Answer Incoming Calls with Mute Button Parameter</td>
<td>250</td>
</tr>
<tr>
<td>Call Timer</td>
<td>250</td>
</tr>
<tr>
<td>Called Party Identification</td>
<td>250</td>
</tr>
<tr>
<td>Calling Party Identification Parameters</td>
<td>251</td>
</tr>
<tr>
<td>Connected Party Identification</td>
<td>251</td>
</tr>
<tr>
<td>Calling Party Identification</td>
<td>251</td>
</tr>
<tr>
<td>Calling Party Identification Parameters</td>
<td>251</td>
</tr>
<tr>
<td>Remote Party Caller ID from SIP Messages</td>
<td>252</td>
</tr>
<tr>
<td>Remote Party Caller ID from SIP Messages Parameters</td>
<td>252</td>
</tr>
<tr>
<td>Calling Line Identification</td>
<td>253</td>
</tr>
<tr>
<td>Calling Line Identification Parameters</td>
<td>253</td>
</tr>
<tr>
<td>SIP Header Warnings</td>
<td>254</td>
</tr>
<tr>
<td>SIP Header Warning Parameters</td>
<td>254</td>
</tr>
</tbody>
</table>
Distinctive Call Waiting................................................................. 254
  Distinctive Call Waiting Parameters........................................ 254
Do Not Disturb............................................................................. 255
  Server-Based Do Not Disturb.................................................. 255
  Do Not Disturb Parameters..................................................... 255
Remote Party Disconnect Alert Tone............................................. 256
  Remote Party Disconnect Alert Tone Parameter.................... 257
Call Waiting Alerts....................................................................... 257
  Call Waiting Alert Parameters.............................................. 257
Missed Call Notifications.............................................................. 257
  Missed Call Notification Parameters..................................... 258
Call Hold....................................................................................... 258
  Call Hold Parameters............................................................ 258
  Hold Implementation.......................................................... 259
Call Transfer................................................................................. 260
  Call Transfer Parameters...................................................... 260
Call Forwarding........................................................................... 261
  Call Forward on Shared Lines.............................................. 261
  Call Forwarding Parameters................................................. 261
Automatic Off-Hook Call Placement.......................................... 266
  Automatic Off-Hook Call Placement Parameters................. 266
Multiple Line Keys Per Registration.......................................... 266
  Multiple Line Keys Per Registration Parameter................ 267
Multiple Call Appearances......................................................... 267
  Multiple Call Appearance Parameters............................... 267
Bridged Line Appearance............................................................ 268
  Bridged Line Appearance Signaling.................................... 268
  Bridged Line Appearance Parameters............................... 268
Voicemail.................................................................................... 269
  Voicemail Parameters........................................................ 269
Local Call Recording................................................................. 271
  Local Call Recording Parameter........................................ 271
Local and Centralized Conference Calls on Poly Trio............... 271
  Local and Centralized Conference Call Parameters............ 271
  Conference Management Parameter................................. 272
Conference Meeting Dial-In Options....................................... 273
  Conference Meeting Dial-In Options Parameters............... 273
Hybrid Line Registration.......................................................... 274
  Hybrid Line Registration Limitations................................. 275
  Hybrid Line Registration Parameters............................... 276
  Configure Hybrid Line Registration using the Web Configuration Utility....... 276
Local Digit Map.......................................................................... 277
## Local Digit Maps Parameters ................................................................. 277

## Open SIP Digit Map .............................................................................. 282

## Generating Secondary Dial Tone with Digit Maps ................................. 283

## Enhanced 911 (E.911) ........................................................................... 283

## Enhanced 911 (E.911) Parameters .......................................................... 283

## Multilevel Precedence and Preemption (MLPP) for Assured Services - Session
Initiation Protocol (AS-SIP) ........................................................................ 288

## Preemption Behavior on Low Priority Calls .......................................... 289

## MLPP with AS-SIP Parameters ............................................................... 290

## International Dialing Prefix .................................................................. 291

## International Dialing Prefix Parameters ................................................. 291

## Shared Lines .......................................................................................... 293

## Shared Call Appearances ....................................................................... 293

## Shared Call Appearances Parameters ...................................................... 293

## Private Hold on Shared Lines ................................................................. 308

## Private Hold on Shared Lines Parameters .............................................. 308

## Intercom Calls ....................................................................................... 308

## Creating a Custom Intercom Soft Key ..................................................... 308

## Intercom Calls Parameters ..................................................................... 309

## Group Paging .......................................................................................... 309

## Group Paging Parameters ...................................................................... 310

## User Profiles ........................................................................................ 313

## User Profile Parameters ......................................................................... 313

## Remotely Logging Out Users .................................................................. 315

## Authentication of User Profiles .............................................................. 315

## Server Authentication of User Profiles .................................................. 315

## Phone Authentication of User Profiles .................................................. 317

## Network ................................................................................................. 319

## Two-Way Active Measurement Protocol .............................................. 319

## TWAMP Limitations ............................................................................... 319

## Two-Way Active Measurement Protocol Configuration Parameters .... 320

## System and Model Names ...................................................................... 320

## Incoming Network Signaling Validation ............................................... 321

## Network Signaling Validation Parameters ............................................. 321

## SIP Subscription Timers ....................................................................... 322

## SIP Subscription Timers Parameters .................................................... 322

## Enhanced IPv4 ICMP Management ....................................................... 323

## IPv4 Parameters .................................................................................... 323
Microsoft Exchange Integration ....................................................................................... 366
Integrating with Microsoft Exchange ........................................................................ 367
Poly Trio Solution with Skype for Business ............................................................ 368
Private Meetings in Microsoft Exchange ............................................................... 369
Configuring the Microsoft Exchange Server ......................................................... 370
Join a Meeting with a SIP URI ............................................................................... 376
Microsoft Exchange Advanced Login ..................................................................... 377

Device Parameters ..................................................................................................... 380
Changing Device Parameters .................................................................................. 380
Types of Device Parameters .................................................................................. 381
Parameter List Conventions .................................................................................. 381
Device Parameters .................................................................................................. 383

Configuration Parameters ....................................................................................... 399
Quick Setup Soft Key Parameter .......................................................................... 399
Per-Registration Call Parameters ......................................................................... 400
Remote Packet Capture Parameters ..................................................................... 404
Per-Registration Dial Plan Parameters .................................................................. 404
Local Contact Directory File Size Parameters .................................................... 408
Parameter Elements for the Local Contact Directory ......................................... 409
Feature Activation/Deactivation Parameters .......................................................... 411
HTTPD Web Server Parameters ........................................................................... 412
Feature License Parameter .................................................................................... 414
Chord Parameters .................................................................................................. 414
Message Waiting Parameters ............................................................................... 415
Ethernet Interface MTU Parameters ...................................................................... 416
Presence Parameters ............................................................................................... 416
Provisioning Parameters ......................................................................................... 417
Configuration Request Parameter ......................................................................... 418
General Security Parameters .................................................................................. 418
DHCP Parameter .................................................................................................... 419
Domain Name System (DNS) Parameters ............................................................... 419
TCP Keep-Alive Parameters ................................................................................. 420
File Transfer Parameter ........................................................................................ 420
User Preferences Parameters ................................................................................ 421
Upgrade Parameters ................................................................................................ 426
Voice Parameters .................................................................................................... 427
Acoustic Echo Suppression (AES) Parameter ......................................................... 428
Comfort Noise Parameters ..................................................................................... 428
Voice Jitter Buffer Parameters ............................................................................... 429
Before You Begin

Topics:

• Audience, Purpose, and Required Skills
• Related Poly and Partner Resources

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

• Poly Trio 8300 system
• Poly Trio 8500 system
• Poly Trio 8800 system
• Poly Trio Visual+ system
• Poly Trio VisualPro system

The Poly Trio 8300 system is not supported in Skype for Business or Microsoft Teams environments.

Note: The Poly Trio 8500 system, Poly Trio 8800 system, and Poly Trio Visual+ accessory are also known as the Polycom Trio 8500 system, and Polycom Trio 8800 system, and Polycom Trio Visual+ accessory or Polycom RealPresence Trio 8500 system, Polycom RealPresence Trio 8500 system, and Polycom RealPresence Trio Visual+ accessory. The Poly Trio VisualPro system is also known as the Polycom Trio VisualPro system.

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

Related Poly and Partner Resources

See the following sites for information related to this product.

• The Polycom Support Site is the entry point to online product, service, and solution support information including Licensing & Product Registration, Self-Service, Account Management, Product-Related Legal Notices, and Documents & Software downloads.
• The Polycom 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 Polycom 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 Polycom Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.

• The Polycom Collaboration Services help your business succeed and get the most out of your investment through the benefits of collaboration.
Getting Started

Topics:

• Product Overview
• Working with Polycom UC Software

You can deploy Polycom UC software by configuring individual phones, but Poly recommends setting up a provisioning server on your LAN or the internet for large-scale deployments.

Product Overview

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

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

Each release of software is a new image file.

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.
• SIP and H.323 signaling for video telephony. Support for H.323 varies by phone model.
• Industry-standard security techniques for ensuring that all provisioning, signaling, and media transactions are robustly authenticated and encrypted.
• Advanced audio signal processing for handset, headset, and speakerphone communications using a wide range of audio codecs.
• Flexible provisioning methods to support single phone, small business, and large multi-site enterprise deployments.

Supported Phones and Accessories

The following table lists the product names, model names, and part numbers for Poly phones and devices that support Polycom UC Software.

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Model Name</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio 8300</td>
<td>Polycom Trio8300</td>
<td>3111-66800-001</td>
</tr>
<tr>
<td>Poly Trio 8500</td>
<td>Polycom Trio8500</td>
<td>3111-66700-001</td>
</tr>
<tr>
<td>Poly Trio 8800</td>
<td>Polycom Trio8500</td>
<td>3111-65290-001</td>
</tr>
<tr>
<td>Poly Trio Visual+</td>
<td>Polycom TrioVisualPlus</td>
<td>3111-66420-001</td>
</tr>
</tbody>
</table>
Working with Polycom UC Software

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.

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. Importantly, there is a priority among the methods that impacts your phone deployment when you use multiple methods simultaneously. In the event of a difference between multiple provisioning methods or configuration settings, the Poly phone uses the setting set with the higher-priority method based on the hierarchy below:

1. Quick Setup
2. Phone menu
3. Web Configuration Utility
4. Skype for Business in-band provisioning
5. USB
6. Polycom® Resource Manager
7. Centralized provisioning
8. Default phone values

For example, when you provision the phones using a provisioning server and subsequently apply settings using the Web Configuration Utility, the Web Configuration Utility setting overrides any duplicate settings you set from the provisioning server. Likewise, any settings set from the phone menu override any duplicate settings you set using the Web Configuration Utility.

Record Version Information

In case you need to contact technical support, you should record the following information for future reference:

- Phone models
- Updater version
- UC Software version
- Partner Platform
Supported Inbound and Outbound Ports

Topics:

- Inbound Ports for Poly Trio Systems
- Outbound Ports for Poly Trio System
- Poly Trio Visual+ Network Ports
- Inbound Ports for Poly Trio VisualPro Systems
- Outbound Ports for Poly Trio VisualPro Systems

You can configure the inbound and outbound ports on Poly Trio systems and the Poly Trio Visual+ and Trio VisualPro system.

Inbound Ports for Poly Trio Systems

The following table lists the inbound IP ports currently used by Polycom UC Software running on all Poly Trio systems except where noted.

### Inbound IP Port Connections to Poly Trio Systems

<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Static</td>
<td>TCP</td>
<td>Telnet Diagnostics</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>8300 only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>HTTP Pull Web interface, HTTP Push</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TCP</td>
<td>HTTP Pull Web interface, HTTP Push</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>10010</td>
<td>Static</td>
<td>TLS 1.2</td>
<td>Synchronize Daisy-Chained Poly Trio systems</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>1024 - 65535</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTP media packets</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>1024 - 65535</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTCP media packets statistics</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>2222</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTP media packets</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>(2222 - 2269)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: tcpIpApp.port.rtp.mediaPortRangeStart
### Supported Inbound and Outbound Ports

<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2223</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTCP media packets statistics</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>tcpIpApp.port.rtp.mediaPortRangeStart</td>
</tr>
<tr>
<td>5001</td>
<td>Static</td>
<td>TCP</td>
<td>People+Content IP</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>5060</td>
<td>Static</td>
<td>TCP/UDP</td>
<td>SIP signaling</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>5061</td>
<td>Static</td>
<td>TLS</td>
<td>SIP over TLS signaling</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>8001</td>
<td>Static</td>
<td>TCP</td>
<td>HTTPS for modular room provisioning</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mr.deviceMgmt.port</td>
</tr>
<tr>
<td>8150 - 8153</td>
<td>Static</td>
<td>TCP</td>
<td>Airplay audio control</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>8150 - 8153</td>
<td>Static</td>
<td>UDP</td>
<td>Airplay audio data</td>
<td>On</td>
<td>No</td>
</tr>
</tbody>
</table>

### Outbound Ports for Poly Trio System

The following table lists the outbound IP ports currently used by Polycom UC Software running on Poly Trio 8500 and 8800 systems.

<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Static</td>
<td>TCP</td>
<td>FTP Provisioning, Logs</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>Static</td>
<td>TCP</td>
<td>SSH</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>53</td>
<td>Static</td>
<td>UDP</td>
<td>DNS</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>67</td>
<td>Static</td>
<td>UDP</td>
<td>DHCP Server</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>68</td>
<td>Static</td>
<td>UDP</td>
<td>DHCP Client</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>69</td>
<td>Static</td>
<td>UDP</td>
<td>TFTP Provisioning, Logs</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>Default</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>HTTP Provisioning, Logs, Web Interface</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>Static</td>
<td>UDP</td>
<td>NTP time server</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>Static</td>
<td>TCP/UDP</td>
<td>LDAP directory query</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>static</td>
<td>TCP</td>
<td>HTTPS Provisioning, Logs, Web Interface</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>Static</td>
<td>UDP</td>
<td>SYSLOG</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>636</td>
<td>Static</td>
<td>TCP/UDP</td>
<td>LDAP directory query</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>10010</td>
<td>Static</td>
<td>TLS 1.2</td>
<td>Synchronize Daisy-Chained Poly Trio systems</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>1024 - 65535</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTP media packets</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>1024 - 65535</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTCP media packets statistics</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>2222</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTP media packets</td>
<td>On</td>
<td>Yes, tcpIpApp.port.rtp.media PortRangeStart</td>
</tr>
<tr>
<td>2223</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td>RTCP media packets statistics</td>
<td>On</td>
<td>Yes, tcpIpApp.port.rtp.media PortRangeStart</td>
</tr>
<tr>
<td>5060</td>
<td>TCP/UDP</td>
<td></td>
<td>SIP signaling</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>5061</td>
<td>TCP</td>
<td></td>
<td>SIP over TLS signaling</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>5222</td>
<td>Static</td>
<td>TCP</td>
<td>Resource Manager: XMPP</td>
<td>Off</td>
<td>No</td>
</tr>
</tbody>
</table>
### Poly Trio Visual+ Network Ports

The following table provides port usage information when configuring network equipment to support the Poly Trio Visual+ accessory.

**Network Port Connections to Poly Trio Visual+**

<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>static</td>
<td>TCP</td>
<td>HTTP Provisioning, Logs, Web Interface</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>319</td>
<td>static</td>
<td>PRPv2</td>
<td>Synchronize Poly Trio Visual+ and Trio systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>static</td>
<td>TCP</td>
<td>HTTPS Provisioning, Logs, Web Interface</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>static</td>
<td>UDP</td>
<td>Multicast pairing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6000 - 6005</td>
<td>static</td>
<td>UDP</td>
<td>RTP streams for modular rooms</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>8000</td>
<td>static</td>
<td>TCP</td>
<td>HTTP/HTTPS for modular room communications</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>8001</td>
<td>static</td>
<td>TCP</td>
<td>HTTP (default) or HTTPS for modular room provisioning</td>
<td>On</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Supported Inbound and Outbound Ports**

<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>8001</td>
<td>Static</td>
<td>TCP</td>
<td>HTTPS for modular room provisioning</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>8150 - 8153</td>
<td>Static</td>
<td>TCP</td>
<td>Airplay audio control</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>8000</td>
<td>static</td>
<td>TCP</td>
<td>HTTP/HTTPS for modular room communications</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>8001</td>
<td>static</td>
<td>TCP</td>
<td>HTTP (default) or HTTPS for modular room provisioning</td>
<td>On</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Inbound Ports for Poly Trio VisualPro Systems

The following table provides inbound port usage information when configuring network equipment to support the Trio VisualPro system.

**Note:** The Poly Trio 8300 system does not support the Poly Trio VisualPro system.

### Inbound IP Port Connections to Poly Trio VisualPro Systems

<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>System web interface over HTTP</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>System web interface over HTTPS</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>1719</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 RAS</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>1720</td>
<td>Static</td>
<td>TCP</td>
<td>H.225.0 Call Signaling</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>5060</td>
<td>Static</td>
<td>TCP</td>
<td>SIP (protocol depends on transport protocol setting)</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5061</td>
<td>Static</td>
<td>TLS</td>
<td>SIP</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>49152-65535</td>
<td>Dynamic</td>
<td>TCP</td>
<td>H.245</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>16384-32764(Defau</td>
<td></td>
<td>Dynamic</td>
<td>UDP</td>
<td>RTP/RTCP video and audio</td>
<td>On</td>
</tr>
</tbody>
</table>

Outbound Ports for Poly Trio VisualPro Systems

The following table provides outbound port usage information when configuring network equipment to support the Trio VisualPro system.

### Outbound IP Port Connections to Trio VisualPro Systems

<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Default</th>
<th>Configurable Port Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>Poly Product Registration for system software installation</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>Default</td>
<td>Configurable Port Number?</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>----------</td>
<td>----------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>123</td>
<td>Static</td>
<td>UDP</td>
<td>NTP</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>389</td>
<td>Static</td>
<td>TLS</td>
<td>LDAP</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>389</td>
<td>Static</td>
<td>TLS</td>
<td>LDAP to ADS (External Authentication)</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>RealPresence Resource Manager (provisioning, monitoring, and software update)</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>Microsoft Exchange Server (calendaring)</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>Microsoft Skype Address Book</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>514</td>
<td>Static</td>
<td>UDP</td>
<td>SYSLOG</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>601</td>
<td>Static</td>
<td>TCP</td>
<td>SYSLOG</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>1718</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 Gatekeeper Discovery</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>1719</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 RAS</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>1720</td>
<td>Static</td>
<td>TCP</td>
<td>H.225.0 Call Signaling</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>3601</td>
<td>Static</td>
<td>TCP</td>
<td>GDS</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>5060</td>
<td>Static</td>
<td>UDP TCP</td>
<td>SIP</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>5061</td>
<td>Static</td>
<td>TLS</td>
<td>SIP</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>5222</td>
<td>Static</td>
<td>TCP</td>
<td>RealPresence Resource Manager: XMPP</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>6514</td>
<td>Static</td>
<td>TLS</td>
<td>SYSLOG</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>49152 - 65535</td>
<td>Dynamic</td>
<td>TCP</td>
<td>H.245</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>16384 - 32764 (Default)</td>
<td>Dynamic</td>
<td>UDP</td>
<td>RTP/RTCP video and audio</td>
<td>On</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Polycom UC Software enables you to optimize security settings, such as changing the passwords for the phone, enabling users to lock their phones, and blocking administrator functions from phone users.

Administrator and User Passwords
You can change the default administrator and user passwords.

When you set the Base Profile to Skype, the phones display a message prompting you to change the default administrator password (456). Poly strongly recommends that you change the default password. This password is separate from the Skype for Business user Sign In password. The default administrator password enables administrators to access advanced settings menu on the phone menu and to log in to a phone’s Web Configuration Utility as an administrator.

You can change the default password using any of the following methods:

- The pop-up prompt when the phone first registers
- Phone menu
- Web Configuration Utility
- Use the parameter `reg.1.auth.password`

You must have a user or administrator password before you can access certain menu options on the phone and in the Web Configuration Utility. You can use the following default passwords to access menu options on the phone and to access the Web Configuration Utility:

- Administrative password: 456
- User password: 123

You can use an administrator password where a user password is required, and you will see all of the user options. While you can use the user password where the administrator password is required, you are
presented with limited menu options. Note that the Web Configuration Utility displays different features and options depending on which password is used.

Each time you connect a Poly Trio system with a Poly Trio Visual+ accessory, the Visual+ user password is reset to match the Poly Trio system user password. You can change the Poly Trio Visual+ password on the Poly Trio menu or Web Configuration Utility.

When the Poly Trio solution Base Profile is set to SkypeUSB, you can set the keyboard entry mode for the password in the Advanced menu on the phone.

**Change the Default Administrator Password on the Phone**

If you do not change the default administrative password, the phone displays a warning and a reminder message each time the phone reboots.

If you are registering phones with Microsoft Skype for Business Server, a message displays on the phone screen prompting you to change the default password.

**Procedure**

1. On the phone, navigate to Settings > Advanced, and enter the default password.
2. Select Administration Settings > Change Admin Password.
3. Enter the default password, enter a new password, and confirm the new password.

**Change the Default Passwords in the Web Configuration Utility**

You can change the administrator and user passwords on a per-phone basis using the Web Configuration Utility.

If the default administrative password is in use, a warning displays in the Web Configuration Utility.

**Procedure**

1. In the Web Configuration Utility, select Settings > Change Password.
2. Update the passwords for the Admin and User.

**Administrator and User Password Parameters**

Use the following parameters to set the administrator and user password and configure password settings.

**sec.pwd.length.admin**

The minimum character length for administrator passwords changed using the phone. Use 0 to allow null passwords.

1 (default)
0 -32

Change causes system to restart or reboot.

**sec.pwd.length.user**

The minimum character length for user passwords changed using the phone. Use 0 to allow null passwords.
Change causes system to restart or reboot.

**up.echoPasswordDigits**

1 (default) The phone briefly displays password characters before being masked by an asterisk.
0 - The phone displays only asterisks for the password characters.

**device.auth.localAdminPassword**

Specify a local administrator password.
0 - 32 characters
You must use this parameter with `device.auth.localAdminPassword.set="1"`

**device.auth.localAdminPassword.set**

0 (default) - Disables overwriting the local admin password when provisioning using a configuration file.
1 - Enables overwriting the local admin password when provisioning using a configuration file.

Disabling External Ports and Features

You can disable unused external phone ports and features to increase the security of devices in your deployment.

You can disable the following ports and features:

- Web Configuration Utility
- PC port
- Aux port
- USB port
- Speakerphone
- Call forwarding
- Do Not Disturb
- Push-to-Talk (PTT)
- Auto Answer
- Applications icon
- Headset
- Handset
- Host and device ports
- Bluetooth
- NFC
• Wi-Fi

**Note:** At least one audio port must be enabled to send and receive calls.

## Disable Unused Ports and Features Parameters
Use the parameters in the following list to disable external ports or specific features.

**device.net.etherModePC**
- 0 (default) - Disable the PC port mode that sets the network speed over Ethernet.
- 1 - Enable the PC port mode that sets the network speed over Ethernet.

**device.auxPort.enable**
- 0 (default) - Disable the phone auxiliary port.
- 1 - Enable the phone auxiliary port.

**httpd.enabled**
- **Base Profile = Generic**
  - 1 (default) - The web server is enabled.
  - 0 - The web server is disabled.
- **Base Profile = Skype**
  - 0 (default) - The web server is disabled.
  - 1 - The web server is enabled.
  - Change causes system to restart or reboot.

**ptt.pttMode.enable**
- 0 (default) - Disable push-to-talk mode.
- 1 - Enable push-to-talk mode.

**feature.callRecording.enabled**
- 0 (default) - Disable the phone USB port for local call recording.
- 1 - Enable the phone USB port for local call recording.
  - Change causes system to restart or reboot.

**up.handsfreeMode**
- 1 (default) - Enable handsfree mode.
- 0 - disable handsfree mode.
**feature.forward.enable**

1 (default) - Enable call forwarding.
0 - Disable call forwarding.

**feature.doNotDisturb.enable**

1 (default) - Enable Do Not Disturb (DND).
0 - Disable Do Not Disturb (DND).
Change causes system to restart or reboot.

**homeScreen.doNotDisturb.enable**

1 (default) - Enables the display of the DND icon on the phone's Home screen.
0 - Disables the display of the DND icon on the phone's Home screen.

**call.autoAnswerMenu.enable**

1 (default) - Enables the phone's Autoanswer menu.
0 - Disables the phone's Autoanswer menu.

---

**Visual Security Classification**

The security classification of a call is determined by the lowest security classification among all participants connected to a call.

For example, a Top Secret classification displays when all participants in a call have at least a Top Secret classification level.

**Note:**

Call classification is determined by the lowest classification level among all participants in the call. You can safely exchange information classified no higher than the call's security classification. For example, if User A is classified as Top Secret and User B has a lower classification level of Restricted, both User A and B are connected to the call as Restricted.

Phone users can modify their assigned security classification level to a value lower than their assigned level during a call. When the call is over, the server resets the user's classification level to its original state.

**Visual Security Classification Parameters**

To enable the visual security classification feature, you must configure settings on the BroadSoft BroadWorks server v20 or higher and on the phones.

If a phone has multiple registered lines, administrators can assign a different security classification to each line.

An administrator can 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. The following list includes the parameters you can use to configure visual security classification.

voIpProt.SIP.serverFeatureControl.securityClassification
0 (default) - The visual security classification feature for all lines on a phone is disabled.
1 - The visual security classification feature for all lines on a phone is enabled.
Change causes system to restart or reboot.

reg.x.serverFeatureControl.securityClassification
0 (default) - The visual security classification feature for a specific phone line is disabled.
1 - The visual security classification feature for a specific phone line is enabled.

Encryption
Poly supports the use of encryption to protect configuration files and phone calls.

Encrypting Configuration Files
Poly phones can download encrypted files from the provisioning server and encrypt files before uploading them to the provisioning server.

You can encrypt configuration files from the Web Configuration Utility and local device interface. You can also determine whether encrypted files are the same as unencrypted files and use the SDK to facilitate key generation.

Note: Most configuration files can be encrypted, but you cannot encrypt the master configuration file, contact directory files, and configuration override files.

To encrypt files, you must provide the phone an encryption key. You can generate your own 32 hex-digit, 128 bit key or use the Polycom Software Development Kit (SDK) to generate a key and to encrypt and decrypt configuration files on a UNIX or Linux server.

Note: To request the SDK and quickly install the generated key, see When Encrypting Polycom UC Software Configuration Files: Quick Tip 67442 at Polycom Engineering Advisories and Technical Notifications.

You can use the following parameters to set the key on the phone:

• device.set
• device.sec.configEncryption.key
• device.sec.configEncryption.key.set

If the phone doesn't have a key, you must download the key to the phone in plain text, which is a potential security concern if you are not using HTTPS. If the phone already has a key, you can download a new key. Poly recommends naming each key uniquely to identify which key was used to encrypt a file.
After encrypting a configuration file, it is useful to rename the file to avoid confusing it with the original version, for example, rename `site.cfg` to `site.enc`.

Note: If a phone downloads an encrypted file that it cannot decrypt, the action is logged, and an error message displays. The phone continues to do this until the provisioning server provides an encrypted file that can be read, an unencrypted file, or until the file is removed from the list in the master configuration file.

Change the Encryption Key on the Phone and Server
To maintain secure files, you can change the encryption key on the phones and the server.

Procedure
1. Place all encrypted configuration files that you want to use the new key on the provisioning server.
   The phone may reboot multiple times.
   The files on the server must be updated to the new key or they must be made available in unencrypted format. Updating to the new key requires decrypting the file with the old key, then encrypting it with the new key.
2. Put the new key into a configuration file that is in the list of files downloaded by the phone, specified in `000000000000.cfg` or `<MACaddress>.cfg`.
3. Use the `device.sec.configEncryption.key` parameter to specify the new key.
4. Provision the phone again so that it downloads the new key.
   The phone automatically reboots a second time to use the new key.
   Note that configuration files, contact directory files and configuration override files may all need to be updated if they were already encrypted. In the case of configuration override files, they can be deleted from the provisioning server so that the phone replaces them when it successfully boots.

Configuration File Encryption Parameters
The following list provides the parameters you can use to encrypt your configuration files.

`device.sec.configEncryption.key`
Set the configuration encryption key used to encrypt configuration files.
string
Change causes system to restart or reboot.

`sec.encryption.upload.callLists`
0 (default) - The call list is uploaded without encryption.
1 - The call list is uploaded in encrypted form.
Change causes system to restart or reboot.

`sec.encryption.upload.config`
0 (default) - The file is uploaded without encryption and replaces the phone specific configuration file on the provisioning server.
1 - The file is uploaded in encrypted form and replaces the existing phone specific configuration file on the provisioning server.

**sec.encryption.upload.dir**

0 (default) - The contact directory is uploaded without encryption and replaces the phone specific contact directory on the provisioning server.
1 - The contact directory is uploaded in encrypted form and replaces the existing phone specific contact directory on the provisioning server.
Change causes system to restart or reboot.

**sec.encryption.upload.overrides**

0 (default) - The MAC address configuration file is uploaded without encryption and replaces the phone specific MAC address configuration file on the provisioning server.
1 - The MAC address configuration file is uploaded in encrypted form and replaces the existing phone specific MAC address configuration file on the provisioning server.

---

**Voice over Secure IP**

You can configure phones to dynamically use either Secure Real Time Protocol (SRTP) or Real Time Protocol (RTP) depending on the media security mechanisms negotiated between phone and outbound proxy using Voice over Secure IP (VoSIP). When you enable this feature, the voice signals are transferred securely between endpoints without the need to introduce multiple lines in the Session Description Protocol (SDP).

The following are advantages for Voice over Secure IP (VoSIP):

- The voice signals are encrypted allowing a safe and secure transmission of signals between phones.
- Signaling and media to the cloud-hosted product are encrypted.

**VoSIP Parameter**

The following parameter enables or disables VoSIP.

**reg.X.rfc3329MediaSec.enable**

0 – Disables the media security mechanisms negotiated between Phone and Outbound proxy without the need of multiple m-lines in the Session Description Protocol.
1 – Enables the media security mechanisms negotiated between Phone and Outbound proxy without the need of multiple m-lines in the Session Description Protocol.
Securing Phone Calls with SRTP

Secure Real-Time Transport Protocol (SRTP) encrypts audio stream(s) to prevent interception and eavesdropping on phone calls.

You need to enable this feature to use it. When in use, phones negotiate the type of encryption and authentication to use for the session with the other endpoint.

SRTP authentication proves to the phone receiving the RTP/RTCP stream that the packets are from the expected source and have not been tampered with. Encryption modifies the data in the RTP/RTCP streams so that if the data is captured or intercepted it sounds like noise and cannot be understood. Only the intended receiver knows the key to restore the data.

If the call is completely secure (RTP authentication and encryption and RTCP authentication and RTCP encryption are enabled), a padlock symbol displays. Phone will send only one SRTP m-line for audio and video instead of multiple m-lines when VoSIP is enabled.

Related Links
TLS Parameters on page 52

SRTP Parameters

Use the session parameters in the following list to enable or disable authentication and encryption for RTP and RTCP streams.

You can also turn off the session parameters to reduce the phone’s processor usage.

**mr.srtp.audio.require**

Enable or disable a requirement for SRTP encrypted audio media between MR hubs and devices.

1 (default)

0

Change causes system to restart or reboot.

**mr.srtp.video.require**

Enable or disable a requirement for SRTP encrypted video media between hubs and devices.

1 (default)

0

Change causes system to restart or reboot.

**sec.srtp.answerWithNewKey**

1 (default) - Provides a new key when answering a call.

0 - Does not provide a new key when answering the call.

**sec.srtp.enable**
1 (default) - The phone accepts the SRTP offers.
0 - The phone declines the SRTP offers.
The defaults for SIP 3.2.0 is 0 when Null or not defined.
Change causes system to restart or reboot.

```
sec.srtp.key.lifetime
```

Specifies the lifetime of the key used for the cryptographic parameter in SDP.
Null (default) -
0 - The master key lifetime is not set.
Positive integer minimum 1024 or power of 2 notation - The master key lifetime is set.
Setting this parameter to a non-zero value may affect the performance of the phone.
Change causes system to restart or reboot.

```
sec.srtp.mki.enabled
```

0 (default) - The phone sends two encrypted attributes in the SDP, one with MKI and one without MKI when the base profile is set as Generic.
1 - The phone sends only one encrypted value without MKI when the base profile is set as Skype.
Change causes system to restart or reboot.

```
sec.srtp.mki.startSessionAtOne
```

0 (default) - The phone uses MKI value of 1.
1 - The MKI value increments for each new crypto key.

```
sec.srtp.offer
```

0 (default) - The secure media stream is not included in SDP of an SIP invite.
1 - The phone includes secure media stream along with the non-secure media description in SDP of an SIP invite.
Change causes system to restart or reboot.

```
sec.srtp.offer.HMAC_SHA1_32
```

0 (default) - The AES_CM_128_HMAC_SHA1_32 crypto suite in SDP is not included.
1 - The AES_CM_128_HMAC_SHA1_32 crypto suite in SDP is included.
Change causes system to restart or reboot.

```
sec.srtp.offer.HMAC_SHA1_80
```

1 (default) - The AES_CM_128_HMAC_SHA1_80 crypto suite in SDP is included.
0 - The AES_CM_128_HMAC_SHA1_80 crypto suite in SDP is not included.
Change causes system to restart or reboot.

**sec.srtp.padRtpToFourByteAlignment**

0 (default) - The RTP packet padding is not required when sending or receiving video.
1 - The RTP packet padding is required when sending or receiving video.
Change causes system to restart or reboot.

**sec.srtp.require**

0 (default) - The secure media streams are not required.
1 - The phone is only allowed to use secure media streams.
Change causes system to restart or reboot.

**sec.srtp.requireMatchingTag**

1 (default) - The tag values must match in the crypto parameter.
0 - The tag values are ignored in the crypto parameter.
Change causes system to restart or reboot.

**sec.srtp.sessionParams.noAuth.offer**

0 (default) - The authentication for RTP offer is enabled.
1 - The authentication for RTP offer is disabled.
Change causes system to restart or reboot.

**sec.srtp.sessionParams.noAuth.require**

0 (default) - The RTP authentication is required.
1 - The RTP authentication is not required.
Change causes system to restart or reboot.

**sec.srtp.sessionParams.noEncrypRTCP.offer**

0 (default) - The encryption for RTCP offer is enabled.
1 - The encryption for RTCP offer is disabled.
Change causes system to restart or reboot.

**sec.srtp.sessionParams.noEncrypRTCP.require**

0 (default) - The RTCP encryption is required.
1 - The RTCP encryption is not required.
Change causes system to restart or reboot.

**sec.srtp.sessionParams.noEncrypRTP.offer**

0 (default) - The encryption for RTP offer is enabled.
1 - The encryption for RTP offer is disabled.

Change causes system to restart or reboot.

**sec.srtp.sessionParams.noEncrypRTP.require**

0 (default) - The RTP encryption is required.
1 - The RTP encryption is not required.

Change causes system to restart or reboot.

**sec.srtp.simplifiedBestEffort**

1 (default) - The SRTP is supported with Microsoft Description Protocol Version 2.0 Extensions.
0 - The SRTP is not supported with Microsoft Description Protocol Version 2.0 Extensions.

### Enabling Users to Lock Phones

You can enable users to lock their phones to prevent access to menus or directories.

After the phone is locked, users can only place calls to emergency and authorized numbers. You can specify which authorized numbers users can call.

If a user forgets their password, you can unlock the phone either by entering the administrator password or by disabling and re-enabling the phone lock feature. The latter method facilitates remote unlocking and avoids disclosing the administrator password to the user.

---

**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.

---

### Phone Lock Parameters

Use the parameters in the following list to enable the phone lock feature, set authorized numbers for users to call when a phone is locked, and set scenarios when the phone should be locked.

Phone Lock is different from Device Lock for Skype for Business deployments. If you enable Phone Lock and Device Lock for Skype for Business at the same time on a phone with the Base Profile set to Skype, the Device Lock feature takes precedence over Phone Lock.

**phoneLock.Allow.AnswerOnLock**

1 (default) - Users can answer any incoming call without needing to unlock the phone.
0 - Users must unlock the phone before answering an incoming call.
phoneLock.authorized.x.description
The name or description of an authorized number.
Null (default)
String
Up to five (x=1 to 5) authorized contacts that a user can call while their phone is locked. Each contact needs a description to display on the screen, and a phone number or address value for the phone to dial.

phoneLock.authorized.x.value
The number or address for an authorized contact.
Null (default)
String
Up to five (x=1 to 5) authorized contacts that a user can call while their phone is locked. Each contact needs a description to display on the screen, and a phone number or address value for the phone to dial.

phoneLock.browserEnabled
0 (default) - The microbrowser or browser is not displayed while the phone is locked.
1 - The microbrowser or browser is displayed while the phone is locked.

phoneLock.dndWhenLocked
0 (default) - The phone can receive calls while it is locked
1 - The phone enters Do-Not-Disturb mode while it is locked

phoneLock.enabled1
0 (default) - The phone lock feature is disabled
1 - The phone lock feature is enabled.

phoneLock.idleTimeout
The amount of time (in seconds) the phone can be idle before it automatically locks. If 0, automatic locking is disabled.
0 (default)
0 to 65535

phoneLock.lockState
0 (default) - The phone is unlocked.
1 - The phone is locked.
The phone stores and uploads the value each time it changes via the MAC-phone.cfg. You can set this parameter remotely using the Web Configuration Utility.

phoneLock.powerUpUnlocked

Overrides the phoneLock.lockState parameter.

0 (default) - The phone retains the value in phoneLock.lockState parameter.

1 - You can restart, reboot, or power cycle the phone to override the value for phoneLock.lockState in the MAC-phone.cfg and start the phone in an unlocked state.

You can then lock or unlock the phone locally. Polycom recommends that you do not leave this parameter enabled.

### Locking the Basic Settings Menu

By default, all users can access the Basic settings menu available on a Poly phone.

From this menu, users can customize non-administrative features on their phone. You can choose to lock the Basic settings menu to allow certain users access to the basic settings menu.

If enabled, you can use the default user password (123) or administrator password (456) to access the Basic settings menu, unless the default passwords are not in use.

#### Basic Settings Menu Lock Parameter

Use the parameter below to lock the Basic settings menu.

up.basicSettingsPasswordEnabled

Specifies that a password is required or not required to access the Basic Settings menu.

0 (Default) - No password is required to access the Basic Settings menu.

1 - Password is required for access to the Basic Settings menu.

### Secondary Port Link Status Report

Poly devices can detect an externally connected host connection/disconnection, informing the authenticator switch to initiate the authentication process or drop an existing authentication.

This feature extends Cisco Discovery Protocol (CDP) to include a Second Port Status Type, Length, Value (TLV) that informs an authenticator switch of the status of devices connected to a device's secondary PC port.

This feature ensures the following:

- The port authenticated by the externally attached device switches to unauthenticated upon device disconnection so that other unauthorized devices cannot use it.
- The externally attached device can move to another port in the network and start a new authentication process.
• To reduce the frequency of CDP packets, the phone does not send link-up status CDP packets before a certain time period. The phone immediately sends all link-down indication to ensure that the port security is not compromised.

• If the externally attached device (the host) supports 802.1X authentication, then the device can send an EAPOL-Logoff on behalf of the device after it is disconnected from the secondary PC port. This informs the authenticator switch to drop the authentication on the port corresponding with the previously attached device.

Secondary Port Link Status Report Parameters

You can use the parameters in the following list to configure options for the Secondary Port Link Status Report feature, including the required elapse or sleep time between two CDP UPs dispatching.

**sec.dot1x.eapollogoff.enabled**

0 (default) - The phone does not send an EAPOL Logoff message.
1 - The phone sends an EAPOL Logoff message.

Change causes system to restart or reboot.

**sec.dot1x.eapollogoff.lanlinkreset**

0 (default) - The phone does not reset the LAN port link.
1 - The phone resets the LAN port link.

Change causes system to restart or reboot.

**sec.hostmovedetect.cdp.enabled**

0 (default) - The phone does not send a CDP packet.
1 - The phone sends a CDP packet.

Change causes system to restart or reboot.

**sec.hostmovedetect.cdp.sleepTime**

Controls the frequency between two consecutive link-up state change reports.

1000 (default)
0 to 60000

If sec.hostmovedetect.cdp.enabled is set to 1, there is an x microsecond time interval between two consecutive link-up state change reports, which reduces the frequency of dispatching CDP packets.

Change causes system to restart or reboot.
802.1X Authentication

Poly phones support IEEE 802 standards.

1X authentication and the following EAP authentication methods:

- EAP-TLS (requires Device and CA certificates)
- EAP-PEAPv0/MSCHAPv2 (requires CA certificates)
- EAP-PEAPv0/GTC (requires CA certificates)
- EAP-TTLS/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/GTC (requires CA certificates)
- EAP-FAST (optional Protected Access Credential (PAC) file, if not using in-band provisioning)
- EAP-MD5

802.1X Authentication Parameters

To set up an EAP method that requires a device or CA certificate, you need to configure TLS Platform Profile 1 or TLS Platform Profile 2 to use with 802.1X.

You can use the parameters in the following list to configure 802.1X Authentication.

For more information on EAP authentication protocol, see RFC 3748: Extensible Authentication Protocol.

**device.net.dot1x.enabled**

Enable or disable 802.1X authentication.

0

1

Change causes system to restart or reboot.

**device.net.dot1x.identity1**

Set the identity (user name) for 802.1X authentication.

String

Change causes system to restart or reboot.

**device.net.dot1x.method**

Specify the 802.1X EAP method.

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.password
Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.
String
Change causes system to restart or reboot.

device.net.dot1x.eapFastInBandProv
Enable EAP In-Band Provisioning for EAP-FAST.
0 (default) - Disabled
1 - Unauthenticated, active only when the EAP method is EAP-FAST.

device.pacfile.data
Specify a PAC file for EAP-FAST (optional).
Null (default)
0-2048 - String length.

device.pacfile.password
The optional password for the EAP-FAST PAC file.
Null (default).
0-255 - String length.

SCEP Security Protocol
The Simple Certificate Enrollment Protocol (SCEP) enables you to automatically and securely provision multiple phones with a digital device certificate.

SCEP Parameters
Use the following parameters to configure SCEP.

SCEP.CAFingerprint
Configure the CA certificate fingerprint to confirm the authenticity of the CA response during enrollment.
null (default)
0 - 255 characters
**SCEP.certPoll.retryCount**

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**.

12 (default)
1 - 24

**SCEP.certPoll.retryInterval**

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**.

300 (default)
300 - 3600

**SCEP.certRenewalRetryInterval**

Specify the time interval to retry certificate renewal.

86400 minutes (default)
28800 - 259200 minutes

**SCEP.certRenewalThreshold**

Specify the percentage of the certificate validity interval to initiate a renewal.

80 (default)
50 - 100

**SCEP.challengePassword**

Specify the challenge password to send with the Certificate Signing Request (CSR) when requesting a certificate.

null (default)
0 - 255 characters

**SCEP.csr.commonName**

Specify the common name to use for CSR generation.

null (default)
0 - 64

**SCEP.csr.country**

Specify the country name to use for CSR generation.

null (default)
0 - 2
**SCEP.csr.email**

Specify the email address to use for CSR generation.
null (default)
0 - 64

**SCEP.csr.organization**

Specify the organization name to use for CSR generation.
null (default)
0 - 64

**SCEP.csr.state**

Specify the state name to use for CSR generation.
null (default)
0 - 128 characters

**SCEP.enable**

0 (default) - Disable the SCEP feature.
1 - Enable the SCEP feature.

**SCEP.enrollment.retryCount**

Specify the number of times to retry the enrolment process in case of enrolment failure.
12 (default)
1 - 24

**SCEP.enrollment.retryInterval**

Specify the time interval to retry the enrolment process.
300 seconds (default)
300 - 3600 seconds

**SCEP.http.password**

Specify the password that authenticates with the SCEP server.
null (default)
string, max 255 characters

**SCEP.http.username**

Specify the user name that authenticates with the SCEP server.
null (default)
string, max 255 characters

**SCEP.url**
Specify the URL address of the SCEP server accepting requests to obtain a certificate.
null (default)
0 - 255 characters

### Session Management on the Web Configuration Utility

You can use the Session Management on the Web Configuration Utility to enhance phone security by setting the maximum number of sessions and determining session validity.

If you change the Web Configuration Utility 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 Web Configuration Utility.

**Note:** If you aren’t able to log in to the Web Configuration Utility, clear web browser cookies and re-login.

### Session Management Parameters
Use the following parameters to configure session management.

**httpd.cfg.session.maxSessionAge**
Specify the maximum duration of a session in idle state.
900 seconds (default)
60 – 86,400 seconds
Change causes system to restart or reboot.

**httpd.cfg.session.maxSessions**
Specify the maximum number of concurrent sessions.
10 (default)
1 – 20 sessions
Change causes system to restart or reboot.
Certicates

Topics:

• Using the Factory-Installed Certificate
• Customizing Certificate Use
• Create a Certificate Signing Request
• Custom URL Location for LDAP Server CA Certificate
• Online Certificate Status Protocol

Security certificates are an important element in deploying a solution that ensures the integrity and privacy of communications involving Polycom UC Software devices.

Poly phones come with an authenticated, "built-in" device certificate that you can use. You can also choose to customize your security by requesting additional certificates from a certificate authority of your choice.

You can customize security configuration options to determine type of device certificate used for each of the secure communication options. By default, all operations will use the factory-installed device certificate unless you specify otherwise.

**Note:** You can install custom device certificates on your phones in the same way custom CA certificates are installed. See *Technical Bulletin 17877: Using Custom Certificates With Polycom Phones on Polycom Support* for more information.

Certificates are used in the following situations:

• Mutual TLS Authentication, which allows a server to verify that a device is truly a Poly device (and not a malicious endpoint or software masquerading as a Poly device). This could be used for tasks like provisioning, or SIP signaling using TLS signaling. For example, certain partner provisioning systems use Mutual TLS as does Polycom® Zero Touch Provisioning (ZTP).

• Secure HTTP (HTTPS) access to the web server on the phone at https://<IP ADDRESS OF PHONE>. The web server is used for certain configuration and troubleshooting activities.

• Secure communications using the Polycom Applications API.

There are different options for using device certificates on the phone:

• **Two Platform Device Certificates** — You can configure these certificates for any of the following purposes: 802.1X Authentication, provisioning, syslog, SIP signaling, browser communications, presence, and LDAP. Certificates for syslog, 802.1X, and provisioning must applied using TLS platform profiles.

• **Six Application Device Certificates** — You can configure these certificates for all the same operations as the platform certificates listed above. However, you can’t use TLS application profiles to applied certificates for 802.1X, syslog, and provisioning.
Using the Factory-Installed Certificate

A factory-installed device certificate is installed at the time of manufacture and is unique to a device (based on the MAC address) and signed by the Polycom Certificate Authority (CA).

Since it is installed at the time of manufacture, it is the easiest option for out-of-box activities. This is especially helpful for phone provisioning.

You can use the factory-installed certificate for all your security needs. To configure your web servers and/or clients to trust the Polycom factory-installed certificates, you must download the Polycom Root CA certificate, which is available at http://pki.polycom.com/pki. You may also need to download the Intermediate CA certificates if determined by the authenticating server.

The location of the Certificate Revocation List (CRL)—a list of all expired certificates signed by the Polycom Root CA—is part of the Polycom Root CA digital certificate. If you enable Mutual TLS, you must have a root CA download (the Polycom Root CA certificate or your organization's CA) on the HTTPS server.

The certificate is set to expire on March 9, 2044.

Note: 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 Polycom Engineering Advisories and Technical Notifications.

Check for a Device Certificate

The certificate and associated private key are stored on the phone in its non-volatile memory as part of the manufacturing process.

You can check if a phone has a certificate pre-installed.

Procedure

2. Select a credential and press Info to view the certificate.
   
   One of the following messages displays:
   
   - **Installed** or **Factory Installed** is displayed if the certificate is available in flash memory, all the certificate fields are valid (listed above), and the certificate has not expired.
   - **Not Installed** is displayed if the certificate is not available in flash memory (or the flash memory location where the device certificate is to be stored is blank).
   - **Invalid** is displayed if the certificate is not valid.

   Note: If your phone reports the device certificate as self-signed rather than **Factory Installed**, return the equipment to receive a replacement.
Customizing Certificate Use

You can add custom certificates to the phone and set up the phone to use the certificates for different features.

For example, the phone's factory-installed certificate can be used for authentication when phone provisioning is performed by an HTTPS server. You can use a different certificate when accessing content through a browser.

Determining TLS Platform Profiles or TLS Application Profiles

You use TLS Platform or TLS Application profiles to customize where your installed certificates are used for authentication.

After you install certificates on the phone, you can determine which TLS platform profiles or TLS application profiles use these certificates. By default, TLS Platform Profile 1 uses every CA certificate and the default device certificate. Also, each TLS application uses TLS Platform Profile 1 as the default profile. You can quickly apply a CA certificate to all TLS applications by installing it on the phone and keeping the default TLS profile and default TLS application values.

Alternatively, you can choose which TLS platform profile or application profile to use for each TLS application. You can use platform profiles for any of the following purposes: phone provisioning, for applications running on the microbrowser and browser, and for 802.1X, LDAP, and SIP authentication. You can use application profiles for all applications except 802.1X, syslog, and provisioning.

Note: For more information on using custom certificates, see Technical Bulletin 17877: Using Custom Certificates With Polycom Phones on Polycom Support.

TLS Platform Profile and Application Profile Parameters

By default, all pre-installed profiles are associated with the default cipher suite and use trusted and widely recognized CA certificates for authentication.

The following list shows parameters for TLS Platform Profile 1. To configure TLS Platform Profile 2, use a 2 at the end of the parameter instead of a 1. For example, set device.sec.TLS.profile.caCertList2 instead of device.sec.TLS.profile.caCertList1.

You can use the parameters in the following list to configure the following TLS Profile feature options:

- Change the cipher suite, CA certificates, and device certificates for the two platform profiles and the six application profiles.
- Map profiles directly to the features that use certificates.

device.sec.TLS.customCaCert1

Specify a custom certificate.

Null (default)

String (maximum of 12288 characters)

device.sec.TLS.profile.caCertList1
Specify which CA certificates to use.
Null (default)
String (maximum of 1024 characters)

**device.sec.TLS.profile.cipherSuite1**
Specify the cipher suite.
Null (default)
String (maximum of 1024 characters)

**device.sec.TLS.profile.cipherSuiteDefault1**
Null (default)
0 - Use the custom cipher suite.
1 - Use the default cipher suite.

**device.sec.TLS.profile.deviceCert1**
Specify which device certificates to use.
Builtin (default)
Builtin, Platform1, Platform2

**sec.TLS.customCaCert.x**
The custom certificate for TLS Application Profile x (x= 1 to 6).
Null (default)
String

**sec.TLS.customDeviceKey.x**
The custom device certificate private key for TLS Application Profile x (x= 1 to 6).
Null (default)
String

**sec.TLS.profile.x.caCert.application1**
1 (default) - Enable a CA Certificate for TLS Application Profile 1.
0 - Disable a CA Certificate for TLS Application Profile 1.

**sec.TLS.profile.x.caCert.application2**
1 (default) - Enable a CA Certificate for TLS Application Profile 2.
0 - Disable a CA Certificate for TLS Application Profile 2.
sec.TLS.profile.x.caCert.application3
1 (default) - Enable a CA Certificate for TLS Application Profile 3.
0 - Disable a CA Certificate for TLS Application Profile 3.

sec.TLS.profile.x.caCert.application4
1 (default) - Enable a CA Certificate for TLS Application Profile 4.
0 - Disable a CA Certificate for TLS Application Profile 4.

sec.TLS.profile.x.caCert.application5
1 (default) - Enable a CA Certificate for TLS Application Profile 5.
0 - Disable a CA Certificate for TLS Application Profile 5.

sec.TLS.profile.x.caCert.application6
1 (default) - Enable a CA Certificate for TLS Application Profile 6.
0 - Disable a CA Certificate for TLS Application Profile 6.

sec.TLS.profile.x.caCert.application7
1 (default) - Enable a CA Certificate for TLS Application Profile 7.
0 - Disable a CA Certificate for TLS Application Profile 7.

sec.TLS.profile.x.caCert.defaultList
Specifies the list of default CA Certificate for TLS Application Profile x (x=1 to 7).
Null (default)
String

sec.TLS.profile.x.caCert.platform1
1 (default) - Enable a CA Certificate for TLS Platform Profile 1.
0 - Disable a CA Certificate for TLS Platform Profile 1.

sec.TLS.profile.x.caCert.platform2
1 (default) - Enable a CA Certificate for TLS Platform Profile 2.
0 - Disable a CA Certificate for TLS Platform Profile 2.

sec.TLS.profile.x.cipherSuite
Specifies the cipher suite for TLS Application Profile x (x=1 to 8).
Null (default)
String
sec.TLS.profile.x.cipherSuiteDefault

1 (default) - Use the default cipher suite for TLS Application Profile x (x= 1 to 8).
0 - Use the custom cipher suite for TLS Application Profile x (x= 1 to 8).

sec.TLS.profile.x.deviceCert

Specifies the device certificate to use for TLS Application Profile x (x = 1 to 7).
Polycom (default)
Platform1, Platform2, Application1, Application2, Application3, Application4, Application5, Application6, Application7

TLS Protocol Configuration for Supported Applications

You can configure the TLS Protocol for the following supported applications:

• LDAP
• SIP
• SOPI
• Web server
• XMPP
• Exchange services
• Syslog
• Provisioning
• 802.1x

TLS Protocol Parameters

The following list includes the parameters for the TLS protocol supported applications.

device.sec.TLS.protocol.dot1x

Configures the lowest TLS/SSL version to use for handshake negotiation between phone and 802.1x authentication. The phone handshake starts with the highest TLS version irrespective of the value you configure.

TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

device.sec.TLS.protocol.prov

Configures the lowest TLS/SSL version to use for handshake negotiation between phone and provisioning. The phone handshake starts with the highest TLS version irrespective of the value you configure.
device.sec.TLS.protocol.syslog

Configures the lowest TLS/SSL version to use for handshake negotiation between phone and Syslog. The phone handshake starts with the highest TLS version irrespective of the value you configure.

TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.browser

Configure the lowest TLS/SSL version to use for handshake negotiation between the phone and phone browser. The phone handshake starts with the highest TLS version irrespective of the value you configure.

TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

The microbrowser restarts when there is a change in the browser TLS protocol or TLS cipher settings, and the last web page displayed is not restored.

sec.TLS.protocol.exchangeServices

Configures the lowest TLS/SSL version to use for handshake negotiation between phone and Exchange services. The phone handshake starts with the highest TLS version irrespective of the value you configure.

TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.ldap

Configure the lowest TLS/SSL version to use for handshake negotiation between phone and Lightweight Directory Access Protocol (LDAP). The phone handshake starts with the highest TLS version irrespective of the value you configure.

TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.sip
Configures the lowest TLS/SSL version to use for handshake negotiation between the phone and SIP signaling. The phone handshake starts with the highest TLS version irrespective of the value you configure.
TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.sopi
Configures the lowest TLS/SSL version to use for handshake negotiation between phone and SOPI. The phone handshake starts with the highest TLS version irrespective of the value you configure.
TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.webServer
Configures the lowest TLS/SSL version to use for handshake negotiation between phone and web server. The phone handshake starts with the highest TLS version irrespective of the value you configure.
TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLSv1_2

sec.TLS.protocol.xmpp
Configures the lowest TLS/SSL version to use for handshake negotiation between phone and XMPP. The phone handshake starts with the highest TLS version irrespective of the value you configure.
TLSv1_0 (default)
SSLv2v3
TLSv1_1
TLS Parameters
The next list includes configurable TLS parameters.
For the list of configurable ciphers, refer to the Secure Real-Time Transport Protocol table.

sec.TLS.browser.cipherList
The cipher list is for browser. The format for the cipher list uses OpenSSL syntax found at: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.
NoCipher (default)
String

sec.TLS.customDeviceCert.x
The custom device certificate for TLS Application Profile x (x= 1 to 6).
Null (default)
String

sec.TLS.LDAP.cipherList
The cipher list for the corporate directory. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.
NoCipher (default)
String

sec.TLS.profileSelection.SOPI
Select the platform profile required for the phone.
PlatformProfile1 (default)
1 - 7

sec.TLS.profile.webServer.cipherSuiteDefault
1 (default) - The phone uses the default cipher suite for web server profile.
0 - The custom cipher suite is used for web server profile.

sec.TLS.prov.cipherList
The cipher list for provisioning. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.
NoCipher (default)
String
sec.TLS.SIP.cipherList
The cipher list for SIP. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

NoCipher (default)
String

sec.TLS.SIP.strictCertCommonNameValidation
1 (default) - The common name validation is enabled for SIP.
0 - The common name validation is not enabled for SIP.

sec.TLS.SOPI.cipherList
Selects a cipher key from the list of available ciphers.

NoCipher (default)
1 - 1024 character string

sec.TLS.SOPI.strictCertCommonNameValidation
Controls the strict common name validation for the URL provided by the server.

1 (default) - The SOPI verifies the server certificate to match commonName/SubjectAltName against the server hostname.
0 - The SOPI will not verify the server certificate for commonName/SubjectAltName against the server hostname.

sec.TLS.syslog.cipherList
The cipher list for syslog. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html

NoCipher (default)
String

Related Links
Securing Phone Calls with SRTP on page 32

TLS Profile Selection Parameters
You can configure the parameters listed below to choose the platform profile or application profile to use for each TLS application.

sec.TLS.profileSelection.browser
Specifies to select a TLS platform profile or TLS application profile for the browser or a microbrowser.

PlatformProfile1 (default)
• PlatformProfile1
• PlatformProfile2
• ApplicationProfile1
• ApplicationProfile2
• ApplicationProfile3
• ApplicationProfile4
• ApplicationProfile5
• ApplicationProfile6
• ApplicationProfile7

**sec.TLS.profileSelection.LDAP**

Specifies to select a TLS platform profile or TLS application profile for the corporate directory.

PlatformProfile1 (default)

• PlatformProfile1
• PlatformProfile2
• ApplicationProfile1
• ApplicationProfile2
• ApplicationProfile3
• ApplicationProfile4
• ApplicationProfile5
• ApplicationProfile6
• ApplicationProfile7

**sec.TLS.profileSelection.SIP**

Specifies to select a TLS platform profile or TLS application profile for SIP operations.

PlatformProfile1 (default)

• PlatformProfile1
• PlatformProfile2
• ApplicationProfile1
• ApplicationProfile2
• ApplicationProfile3
• ApplicationProfile4
• ApplicationProfile5
• ApplicationProfile6
• ApplicationProfile7

**sec.TLS.profileSelection.syslog**

Specifies to select a TLS platform profile for the syslog operations.
Configurable TLS Cipher Suites

You can configure which cipher suites to offer and accept during TLS session negotiation. The following table lists supported cipher suites. NULL cipher is a special case that does not encrypt the signaling traffic.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Cipher Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADH</td>
<td>ADH-RC4-MD5, ADH-DES-CBC-SHA, ADH-DES-CBC3-SHA, ADH-AES128-SHA, ADH-AES256-SHA</td>
</tr>
<tr>
<td>AES128</td>
<td>AES128-SHA</td>
</tr>
<tr>
<td>AES256</td>
<td>AES256-SHA</td>
</tr>
<tr>
<td>DES</td>
<td>DES-CBC-SHA, DES-CBC3-SHA</td>
</tr>
<tr>
<td>DHE</td>
<td>DHE-DSS-AES128-SHA, DHE-DSS-AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>EDH</td>
<td>EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC3-SHA, EDH-DSS-CBC-SHA</td>
</tr>
<tr>
<td>NULL</td>
<td>NULL-MD5, NULL-SHA</td>
</tr>
<tr>
<td>RC4</td>
<td>RC4-MD5, RC4-SHA</td>
</tr>
</tbody>
</table>

TLS Cipher Suite Parameters

You can use the parameters listed below to configure TLS Cipher Suites.

sec.TLS.cipherList

String (1 - 1024 characters)
RC4:@STRENGTH (default)
ALL:!aNULL:!eNULL:!DSS:!SEED
%!ECDSA:!IDEA:!MEDIUM:!LOW:
EXP:!ADH:!ECDH:!PSK:!MD5:
RC4:@STRENGTH
The global cipher list parameter. The format for the cipher list uses OpenSSL syntax found at: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

```
sec.TLS.<application>.cipherList

Specify the cipher list for a specific TLS Platform Profile or TLS Application Profile.
```

## Create a Certificate Signing Request

You can generate a certificate signing request directly from your device.

By default, the phone requests a 2048-bit certificate with "sha256WithRSAEncryption" as the signature algorithm. You can use OpenSSL or another certificate signing request utility if you require a stronger certificate.

Poly phones support the use of Subject Alternative Names (SAN) with TLS security certificates but does not support the use of the asterisk (*) or wildcard characters in the Common Name field of a Certificate Authority's public certificate. If you want to enter multiple hostnames or IP addresses on the same certificate, use the SAN field.

You must have a provisioning server in place before generating the certificate signing request.

### Procedure

1. Navigate to **Settings > Advanced > Admin Settings > Generate CSR**.
2. When prompted, enter the administrative password and press Enter.
   - The default administrative password is **456**.
3. From the **Generate CSR Screen**, fill in the Common Name field - the Organization, Email Address, Country, and State fields are optional.
4. Press **Generate**.
   - A message, "CSR generation completed", displays on the phone's screen. The MAC.csr (certificate request) and MAC-private.pem (private key) are uploaded to the phone's provisioning server.
5. Forward the CSR to a Certificate Authority (CA) to create a certificate.
   - If your organization doesn't have its own CA, you need to forward the CSR to a company like Symantec.

## Download Certificates

You can download and install up to eight CA certificates and eight device certificates onto a Poly phone.

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

You can download certificate(s) to a phone in the following ways:

- Using a configuration file
- Through the phone's user interface
- Through the Web Configuration Utility
Procedure

1. Navigate to Settings > Advanced > Administrative Settings > TLS Security and select Custom CA Certificates or Custom Device Certificates.
2. Select Install.
3. Enter the URL where the certificate is stored.
   For example, http://bootserver1.polycom.com/ca.crt
   The certificate is downloaded, and the certificate's MD5 fingerprint displays to verify that the correct certificate is to be installed.
4. Select Accept.
   The certificate is installed successfully.

Custom URL Location for LDAP Server CA Certificate

You can set a custom location on the phones to download a CA certificate or a chain of CA certificates required to authenticate the LDAP server.

By default, all Polycom-installed profiles are associated with the default cipher suite and use trusted and widely recognized CA certificates for authentication. You can download and install up to seven custom CA certificates onto a phone. The certificates 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 certificate slots already have CA certificates installed on your phones, downloading LDAP server CA certificates overwrites any existing certificates on the phone.

Custom URL Location for LDAP Server Certificates Parameter

Use the parameter below to configure a custom URL location for LDAP server certificates.

In addition to the parameter below, you must also configure the following Corporate Directory parameters:

- sec.TLS.profileSelection.LDAP = ApplicationProfile1

sec.TLS.LDAP.customCaCertUrl

Enter the URL location from where the phone can download LDAP server certificates.

String (default)

0 - Minimum

255 - Maximum

You must configure parameters dir.corp.address and feature.corporateDirectory.enabled as well to enable this parameter.

Confirm the Installed LDAP Server Certificates on the Phone

After you set the URL for the location where the phone can download the chain of CA certificates (using the parameter sec.TLS.LDAP.customCaCertUrl) and enabled the dir.corp.address and
feature.corporateDirectory.enabled parameters, the certificates are automatically updated. You can confirm that the correct certificates were downloaded and installed on the phone.

**Procedure**

1. On the phone, navigate to **Settings > Advanced**, and enter the administrator password.
2. Select **Administrative Settings > TLS Security > Custom CA Certificates > Application CA placeholders**.
3. Check that correct certificates were installed on the phone.

**Online Certificate Status Protocol**

The Online Certificate Status Protocol (OCSP) is used to authenticate the revocation status of an X.509 digital certificate. When a user sends a request to a server, the OCSP will retrieve the information whether the certificate is valid or revoked.

**Online Certificate Status Protocol Parameter**

OCSP is a more advanced protocol than the existing CRL. OCSP further offers a grace period for an expired certificate to access servers for a limited time before certificate renewal. OCSP is disabled by default.

**device.sec.TLS.OCSP.enabled**

0 (default) OCSP is disabled.
1 – OCSP is enabled

Change causes system to restart or reboot.

Ensure that `device.set="1", and device.sec.TLS.OCSP.enabled.set="1"` to enable OCSP.
Updating the Software

Topics:

• Upgrade UC Software Using a USB Flash Drive
• Updating UC Software on a Single Phone
• User-Controlled Software Update
• Updating Camera Firmware

You can update the software on your phones to newer versions. The new versions of the software may offer only small enhancements to improve the user experience or large software upgrades that offer new features.

The upgrade process varies depending on the version of Polycom UC Software that is currently running on the phones and the version that you want to upgrade to.

• You can upgrade software with the user-controlled software upgrade feature.
• If you're upgrading from a UC Software version prior to 4.0.x, it must be updated to UC Software 4.0.x first before upgrading further.

Upgrade UC Software Using a USB Flash Drive

You can use a USB flash drive to upgrade the software on your Poly Trio 8500 or 8800 system. USB upgrades are not supported on Poly Trio 8300.

Changes you make using a USB flash drive override the settings you configure using a centralized provisioning server (if applicable). When you remove the USB flash drive, the Poly Trio system reverts to the provisioning server settings.

Note: Poly Trio systems support only File Allocation Table (FAT) file systems. Poly recommends using FAT32.

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 Polycom Support.
3. Copy the configuration files you want to use to the root of the USB device.
   The minimum required configuration files must be copied to the drive:
   • Master configuration file: 000000000000.cfg.
   • Poly Trio 8500: 3111-66700-001.sip.ld
   • Poly Trio 8800: 3111-65290-001.sip.ld.
   • Poly Trio Visual+: 3111-66420.001.sip.ld.
4. Insert the USB flash drive into the Poly Trio system or Poly Trio Visual+ USB port.
5. Enter the Administrator password.

The system detects the flash drive and starts the update within 30 seconds. The mute keys' indicator lights begin to flash, indicating that the update has started.

The system reboots several times during the update. The update is complete when the indicator lights stop flashing and the Home screen displays.

### Updating UC Software on a Single Phone

You can use the Software Upgrade tool in the Web Configuration Utility to update the software version running on a single phone.

For instructions, see *Use the Software Upgrade Tool in the Web Configuration Utility: Feature Profile 67993* at Polycom Engineering Advisories and Technical Notifications.

Configuration changes made to individual phones using the Web Configuration Utility override configuration settings made using central provisioning.

### User-Controlled Software Update

This feature enables phone users to choose when to accept software updates you send to the phones. The software you send to your users' phones can be earlier or later versions.

User-controlled updates apply to configuration changes and software updates you make on the server and Web Configuration Utility. If a user postpones a software update, configuration changes and software version updates from both the server and Web Configuration Utility are postponed. When the user chooses to update, configuration and software version changes from both the server and Web Configuration Utility are sent to the phone.

This feature doesn't work if you enabled ZTP or Skype for Business Device Update. It isn't available with Skype for Business.

### User-Controlled Software Update Parameters

You can 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.

The polling policy is disabled after the phone displays the software update notification.

After the software postponement ends, the phone displays the software update notification again.

**prov.usercontrol.enabled**

- 0 (default) - The phone does not display the software update notification and options and the phone reboots automatically to update the software.
1 - The phone displays the software update notification and options and the user can control the software download.

**prov.usercontrol.postponeTime**

Sets the time interval for software update notification using the HH:MM format.

- 02:00 (default)
- 00:15
- 01:00
- 02:00
- 04:00
- 06:00

**Updating Camera Firmware**

Poly Trio systems with a paired Poly Trio Visual+ accessory automatically update connected Polycom USB cameras and camera systems.

Poly Trio supports automatic firmware updates for the following Polycom USB cameras and camera systems:

- Polycom EagleEye IV USB camera
- Polycom EagleEye Mini USB camera

**Note:** Before updating the EagleEye IV USB camera with firmware stored on a USB drive, disconnect the camera from Poly Trio Visual+ before connecting the USB drive and keep the camera disconnected until the update is complete. Keep in mind that when you reconnect the camera to Poly Trio Visual+, the camera will automatically upgrade or downgrade to the firmware version stored on Poly Trio.
Diagnostics and Status

Topics:

• View the Phone's Status
• Test the Hardware
• Upload a Phone's Configuration
• Perform Network Diagnostics
• Restart a Paired Device
• Reboot Network Devices
• Rebooting the Poly Trio System at a Scheduled Time
• Reset the Poly Trio System to Factory Default Settings at Power-up
• Reset the Poly Trio System to Factory Default Settings from the Home Menu
• Reset the Poly Trio Visual+ to Factory Default Settings
• Reset the Phone and Configuration
• Access Video Transmission Diagnostics
• Status Indicators on the Poly Trio Solution
• Monitoring the Phone's Memory Usage

Poly phones running Polycom UC Software provide a variety of screens and logs that allow you to review information about the phone such as its performance, help you diagnose and troubleshoot problems, view error messages, and test the phone's hardware.

Review the latest UC Software Release Notes for your voice product on Voice Support on Polycom UC Software Support Center for known problems and possible workarounds. If you don't find your problem in this section or in the latest Release Notes, contact your certified reseller for support.

View the Phone's Status

You can troubleshoot phone issues by viewing the phone’s Status menu.

Procedure

1. Select Settings > Status > Select.
2. Scroll to a Status menu item and press Select.

The following table lists available options:
### Menu Item | Menu Information
--- | ---
**Platform** | • Phone's serial number or MAC address  
• Current IP address  
• Updater version  
• Application version  
• Name of the configuration files in use  
• Address of the provisioning server
**Network** | • TCP/IP Setting  
• Ethernet port speed  
• Connectivity status of the PC port (if it exists)  
• Statistics on packets sent and received since last boot  
• Last time the phone rebooted  
• Call Statistics showing packets sent and received on the last call
**Lines** | • Detailed status of each of the phone's configured lines
**Diagnostics** | • Hardware tests to verify correct operation of the microphone, speaker, handset, and third party headset, if present  
• Hardware tests to verify correct operation of the microphones and speaker  
• Tests to verify proper functioning of the phone keys  
• List of the functions assigned to each of the phone keys  
• Real-time graphs for CPU, network, and memory use

## Test the Hardware
If your phone is having any issues, your system administrator may ask you to access a diagnostics menu on the phone to test its hardware.

You can test the display, microphones, and speaker. Contact your system administrator for instructions on how to perform these tests.

### Procedure
1. Go to **Settings > Status > Diagnostics**.
2. Select **Test Hardware** and select one of the following:
   - **Audio Diagnostics**
   - **Display Diagnostics**
   - **Touch Screen Diagnostics**
   - **Keypad Diagnostics**
Upload a Phone's Configuration
You can upload the phone's current configuration files from the phone menu to help you debug configuration problems.

A number of files can be uploaded to the provisioning server, one for every active source as well as the current non-default configuration set. You can use the Web Configuration Utility to upload the files.

Procedure
1. Navigate to Settings > Advanced > Admin Settings > Upload Configuration.
2. Choose which files to upload: All Sources, Configuration Files, Local, MR, Web, or SIP.
   If you use the Web Configuration Utility, you can also upload Device Settings.
4. The phone uploads the configuration file to the location you specified in the parameter prov.configUploadPath.
   For example, if you select All Sources, a file <MACaddress>-update-all.cfg is uploaded.

Perform Network Diagnostics
You can use ping and trace route to troubleshoot network connectivity problems.

Procedure
1. Go to Settings > Status > Diagnostics > Network.
2. Enter a URL or IP address.
3. Press Enter.

Restart a Paired Device
You can restart the Poly Trio Visual+, Poly Trio VisualPro, or RealPresence Group Series system that's paired to your Poly Trio system.

Procedure
   » On the Poly Trio system Home screen, go to Settings > Basic > Restart Networked Devices.

Reboot Network Devices
You can reboot any available devices that are paired and connected to the Poly Trio system.

Procedure
1. On Poly Trio, navigate to Settings > Advanced, and enter the administrator password.
2. Select Network Devices then select a paired device.
3. Select Reboot.
Rebooting the Poly Trio System at a Scheduled Time

You can configure Poly Trio systems to reboot at a scheduled time, period, or days. With this feature, you can schedule a Poly Trio system to reboot daily.

Scheduled Reboot Parameters

Use the following parameters to configure scheduled reboot times for Poly Trio systems.

prov.scheduledReboot.enabled

0 (default) — Disables scheduled reboot.
1 — Enables scheduled reboot.

prov.scheduledReboot.periodDays

Specify the time in days between scheduled reboots.
1 day (default)
1–365 days

prov.scheduledReboot.time

Specify a time to reboot the Poly Trio system. Use the 24 hour time format (HH:mm).
03:00 (default)

prov.scheduledReboot.timeRandomEnd

If this parameter is set to a specific time, the scheduled reboot occurs at a random time between the time set for prov.scheduledReboot.time and prov.scheduledReboot.timeRandomEnd. The time is in 24-hour format.
0–5 hours
hh:mm

Reset the Poly Trio System to Factory Default Settings at Power-up

You can reset the Poly Trio system to factory default settings at power-up.

Resetting to defaults clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Procedure

1. Power on the Poly Trio system.
2. When the Poly logo shows on the screen, press and hold the four corners of the LCD display screen.
3. Let go when the Mute light begins flashing.

Reset the Poly Trio System to Factory Default Settings from the Home Menu

You can reset Poly Trio systems to the factory default settings from the Home menu.
Resetting to factory clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Procedure
  » On the Poly Trio system Home screen, go to Settings > Advanced > Administration settings > Reset to Defaults > Reset to Factory.

The system reboots twice and displays the default home screen.

Reset the Poly Trio Visual+ to Factory Default Settings

You can reset the Poly Trio Visual+ to factory default settings from the interface at power up.
Resetting to defaults clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Procedure
  2. When the pairing button light turns on, press and hold the pair button.
  3. Let go of the pair button when the light begins flashing.

Reset the Phone and Configuration

You can reset the phone and phone configuration. The reset processes can be partial or complete.

Procedure
  » On the phone, go to Settings > Advanced > Administration Settings > Reset to Defaults.

The following list describes the different phone reset options and their effects.

- **Reset Local Configuration** – Clears the override file generated by changes using the phone user interface.
- **Reset Web Configuration** – Clears the override file generated by changes using the Web Configuration Utility.
- **Reset Device Settings** – Resets the phone’s flash file system settings that aren’t 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 UC Software application, log files, configuration, and override files. Note that if the override file is stored on the provisioning server, the phone re-downloads 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 Parameter

By default, only administrators can initiate a factory reset. However, you can make Reset to Factory setting available to users as well.

**up.basicSettings.factoryResetEnabled**

- 0 (default) - Reset to Factory option is not displayed under Basic settings menu.
- 1 – Reset to Factory option is displayed under Basic settings menu

### Access Video Transmission Diagnostics

You can access the Poly Trio solution jitter statistics from the phone menu to evaluate video transmissions.

**Procedure**

1. On the Poly Trio system Home screen, go to **Settings > Status > Diagnostics > Graphs > Networked Devices Graphs**.

### Status Indicators on the Poly Trio Solution

Poly Trio systems, Poly Trio VisualPro, and Poly Trio Visual+ systems use LED lights to indicate the status of the solution.

**Poly Trio Status Indicators**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Device is in an idle state or powered off.</td>
</tr>
<tr>
<td>Green</td>
<td>In a call with audio unmuted.</td>
</tr>
<tr>
<td>Red</td>
<td>Microphones are muted. Device is in a call or in idle state.</td>
</tr>
<tr>
<td>Amber</td>
<td>Power on LED diagnostic.</td>
</tr>
</tbody>
</table>
### Polycom Trio Visual+ Status Indicators

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Device is not powered on.</td>
</tr>
<tr>
<td>Flashing red</td>
<td>Device is booting up or pairing. The pairing button has been pressed.</td>
</tr>
<tr>
<td>Flashing green</td>
<td>Device update is in progress.</td>
</tr>
<tr>
<td>Steady green</td>
<td>Device is powered on and paired with a Polycom Trio system.</td>
</tr>
<tr>
<td>Amber</td>
<td>Device is in a low-power, standby state.</td>
</tr>
<tr>
<td>Alternating orange/red/green/off flashes</td>
<td>Device is in recovery mode.</td>
</tr>
<tr>
<td>Alternating red and green flashes</td>
<td>Device is in pairing diagnostics mode.</td>
</tr>
</tbody>
</table>

### Trio VisualPro Status Indicators

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady blue</td>
<td>Device is powered on and paired with a Poly Trio system.</td>
</tr>
<tr>
<td></td>
<td>Device is in an idle state or powered off.</td>
</tr>
<tr>
<td>Flashing blue</td>
<td>Device is not paired.</td>
</tr>
<tr>
<td></td>
<td>Device is powering on.</td>
</tr>
<tr>
<td>Amber</td>
<td>Device is in a low-power, standby state.</td>
</tr>
<tr>
<td>Green</td>
<td>In a call with audio muted or unmuted.</td>
</tr>
<tr>
<td>Alternating red and green flashes</td>
<td>Device is indicating it is paired.</td>
</tr>
</tbody>
</table>

### Trio VisualPro Microphone Status Indicators

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Device is in an idle state or powered off.</td>
</tr>
<tr>
<td>Green</td>
<td>Microphones are unmuted.</td>
</tr>
<tr>
<td>Red</td>
<td>Microphones are muted. Device is in a call or in idle state.</td>
</tr>
</tbody>
</table>
Monitoring the Phone's Memory Usage

To ensure that your phones and their configured features operate smoothly, verify that the phones have adequate available memory resources.

If you are 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 phone features to all phone models.

For best performance, the phone should use no more 95% of its available memory. When the phone memory resources are low, you may notice one or more of the following symptoms:

- The phones reboot or freeze up.
- The phones do not download all ringtones, directory entries, backgrounds, or XML dictionary files.
- Applications running in the microbrowser or browser stop running or do not start.

Check Memory Usage from the Phone

You can view a graphical representation of the phone's memory usage on the phone display.

Procedure

1. Load and configure the features and files you want to make available on the phone's interface.
2. Navigate to Settings > Status > Diagnostics > Graphs > Memory Usage.

View 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.

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 and consider strategies for reducing the amount of memory you need the feature to use.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Typical Memory Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Browser</td>
<td>Varies, depending on number and complexity of application elements.</td>
<td>To reduce memory resources used by the idle browser:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Display no more than three or four application elements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simplify pages that include large tables or images.</td>
</tr>
<tr>
<td>Feature</td>
<td>Typical Memory Size</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Idle Display Image</td>
<td>15 KB</td>
<td>The average size of the Polycom display image is 15 KB. Custom idle display image files should also be no more than 15 KB.</td>
</tr>
<tr>
<td>Main Browser</td>
<td>Varies, depending on number and complexity of applications.</td>
<td>To reduce memory resources used by the main browser:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Display no more than three or four application elements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simplify pages.</td>
</tr>
<tr>
<td>Local Contact Directory</td>
<td>42.5 KB</td>
<td>Poly phones are optimized to display a maximum of 250 contacts. Each contact has four attributes and requires 170 bytes. A local contact directory of this size requires 42.5 KB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To reduce memory resources used by the local contact directory:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reduce the number of contacts in the directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduce the number of attributes per contact</td>
</tr>
<tr>
<td>Corporate Directory</td>
<td>Varies by server</td>
<td>Poly phones are optimized to corporate directory entries with 5 - 8 contact attributes each. The size of each entry and the number of entries in the corporate directory vary by server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the phone is unable to display directory search results with more than five attributes, make additional memory resources available by reducing memory requirements of another feature.</td>
</tr>
<tr>
<td>Ringtones</td>
<td>16 KB</td>
<td>The ringtone files range in size from 30KB to 125KB. If you use custom ringtones, Poly recommends limiting the file size to 16KB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To reduce memory resources required for ringtones:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduce the number of available ringtones.</td>
</tr>
<tr>
<td>Background Images</td>
<td>8 - 32 KB</td>
<td>Poly phones are optimized to display background images of 50KB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To reduce memory resources required for background images:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduce the number and size of available background images.</td>
</tr>
<tr>
<td>Phone Interface Language</td>
<td>90 - 115 KB, depending on language</td>
<td>The language dictionary file used for the phone's user interface ranges from 90KB to 115KB for languages that use an expanded character set. To conserve memory resources, Polycom recommends using XML language files for only the languages you need.</td>
</tr>
<tr>
<td>Web Configuration Utility Interface</td>
<td>250 KB - 370 KB</td>
<td></td>
</tr>
</tbody>
</table>
Analytics Support for Polycom Cloud Services

Topics:

- Hardware Analytics
- Device Details Sent to the Cloud
- Device Diagnostics Details
- Device Analytics Parameters
- Poly Cloud Connector Parameters
- Turn Off the System Usage Data Collection

You can configure phones to accept commands from the cloud analytics service to perform specified operations on the device and retrieve device details.

The following device details are sent 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 the `da.supported.services` value is set as `all` or `config`, you can perform the following device configurations:

- Download a configuration file to a phone from the cloud.
- Upload the configuration of a phone to cloud.

Device Analytics isn’t supported when Poly phones are configured with IPv6 or dual stack Ethernet configuration.

Note: For more information on Device Analytics, refer to the Polycom Device Analytics Service Guide on the Polycom Documentation Library.

Hardware Analytics

Poly phones send hardware analytics to the cloud at periodic intervals when the `da.supported.services` value is set as `all` or `hardwareanalytics`.

Polycom 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:
  - When the CPU usage value equals or goes above the UpperCPUValue.
  - When the CPU usage value equals or goes below the LowerCPUValue.
  - When 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 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:
  - When free memory equal to and below LowerMemoryValue (Normal to Low memory).
  - When free memory equal to and above UpperMemoryValue (Low to Normal memory).

  When LowerMemoryValue and UpperMemoryValue are defined as 0, memory information is shared with the cloud periodically.
Device Details Sent to the Cloud

When Device Analytics is enabled, Poly 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
- Offset GMT
- Reboot Type
- Wi-Fi Mac Address
- Software Release
- Upload Time
- Updater Version

Service Details

When you enable Device Analytics and the parameter `da.supported.services` value is set as `all` or `service`, the following SIP service details are sent 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

Device Network Details sends network information to cloud services when the phone's network boots up or when there's a change in network parameters. Network information for the Ethernet is passed to the cloud when the phone is idle. Network information for Wi-Fi is passed to the cloud anytime.

When you enable Device Analytics and the parameter `da.supported.services` value is set as `all` or `ni`, the following device network details for Ethernet are sent to the cloud:

• Connection Type
• IPv4 Address
• IPv4 Subnet
• IPv4 Gateway
• VLAN
• IPv4 Address Source
• IPv6 Global Address
• Interface Name
• IPv6 Address Source
• IPv6 Link Local Address
• IPv6 ULA
• 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 following network details for the wireless network are sent 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
- Provisioning Protocol
- MIC Error Count
- EAP Error Count
- NTP Server

**Call Experience Details**

When you enable Device Analytics on your phone, the parameter `da.supported.services` value is set as `all` or `vqmon` along with the dependent features Voice Quality Monitoring Reports (vqmon) and RTP Control Protocol Extended Reports (RTCP XR), the phone sends the following details of Voice Quality Monitoring Reports to the cloud during and after the end of each call:

- Voice Quality Report Type
- Start/Stop Timestamps
- Jitter Buffer
- Packet Loss
- Session Description
- Burst Gap Loss
- Quality Estimate
- Signal Metrics
- Delay Metrics
- Remote Tag
- Local Tag
- Call-ID
Call Data Record (CDR)

When the phone ends an active call and the parameter `da.supported.services` value is set as `all` or `cdr`, the following call summary details are sent to the cloud:

- User
- Remote Party
- Call Direction
- Disconnect Information
- Start Time
- Call Duration
- Protocol Type
- Call Rate
- Call ID
- Remote Tag
- Local Tag

Device Diagnostics Details

Poly phones can send device diagnostics details to the cloud, and you can perform diagnostic actions such as Restart/ Reboot, Factory Reset, and Check Sync from the cloud.

When enabled, the following details are sent to the cloud:

- Core dump file – Sent to the cloud when the parameter `da.supported.services` value is set as `all` or `core`.
- TSID file – Sent to the cloud when the parameter `da.supported.services` value is set as `all` or `tsid`.

Diagnostic Details for System Logs

When you enable Device Analytics and the parameter `da.supported.services` value is set as `all` or `log`, the system log details are sent to the cloud.

When the phone receives a start command from the cloud, the phone sets the value for the `log.render.level`, `log file size`, and `timeout` parameters to the value in the command and starts capturing logs.

The phone uploads log files to the cloud recursively in any of the following cases:

- The file size reaches the threshold limit (configured through start command)
- The phone receives a stop command from the cloud, which resets the `log.render.level` parameter to the previously configured value on the phone.
- Timeout (configured through start command)

Set the file size as well as different log levels appropriately (as per debugging requirements) to avoid excess log capturing; otherwise, it might result in the generation of too many log files uploading to the cloud. This can also impact the phone’s efficiency.
For example, set the file size threshold limit to approximately 50 KB to debug for either Core or UI issues. If you want to set many module log parameters to the debug log level, set the threshold limit to 64 KB or higher.

**Diagnostic Details for Packet Capture**

Set the parameter `da.supported.services` value to `all` or `pcap` to capture the desired packets. Packet capture starts after receiving a request from the cloud, and the phone sends the captured files to the cloud periodically in any of the following ways:

- Until the timeout occurs
- On receiving a stop request from the cloud
- On expiry of upload interval or max packets limit reached.

**Note:** When you enable or use the remote packet capture feature, the packet capture (started through cloud) stops and the captured packets are uploaded to the cloud.

Set the filter properly to avoid excess packet capturing file creation; otherwise, too many files will be generated and uploaded to the cloud, and this might impact the phone’s efficiency. Enable the PCAP feature and set the parameter `work.diags.pcap.enabled` value to 1 to receive PCAP requests from the cloud.

When you set the packet capture filter, follow the filter convention. The following table lists the supported PCAP filter strings.

### Supported PCAP Filter Strings

<table>
<thead>
<tr>
<th>Filter Strings/Types</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp port &lt;number&gt;</td>
<td>udp port 5060 //udp sip traffic</td>
</tr>
<tr>
<td>port &lt;number&gt;</td>
<td>port 5060 //both udp/tcp traffic on port 5060</td>
</tr>
<tr>
<td>portrange &lt;startportnumber-endportnumber&gt;</td>
<td>port 80 //http traffic</td>
</tr>
<tr>
<td></td>
<td>(port 5060)</td>
</tr>
<tr>
<td></td>
<td>portrange 200-300 //traffic on ports from 200 to 300.</td>
</tr>
<tr>
<td>dst host &lt;host&gt;</td>
<td>dst host 1.1.1.1</td>
</tr>
<tr>
<td>src host &lt;host&gt;</td>
<td>dst host <a href="http://www.xyz.com">www.xyz.com</a></td>
</tr>
<tr>
<td>host &lt;host&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Filter Strings/Types

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip, arp, icmp</td>
</tr>
<tr>
<td>ether host &lt;MAC Address&gt;</td>
</tr>
<tr>
<td>ether proto &lt;ethernet-type&gt;</td>
</tr>
<tr>
<td>ip //all ipv4 packets</td>
</tr>
<tr>
<td>ether host 1.1.1.1.1.1</td>
</tr>
<tr>
<td>arp //all arp packets</td>
</tr>
<tr>
<td>ether proto 0x800 //For ipv4 packet filtering</td>
</tr>
<tr>
<td>ether proto 0x806 //For arp packet filtering</td>
</tr>
<tr>
<td>vlan &lt;id&gt;</td>
</tr>
<tr>
<td>vlan 6</td>
</tr>
<tr>
<td>dst net &lt;net&gt;</td>
</tr>
<tr>
<td>dst net 10.10 //All packets with destination</td>
</tr>
<tr>
<td>src net &lt;net&gt;</td>
</tr>
<tr>
<td>net &lt;net&gt;</td>
</tr>
<tr>
<td>net subnet as - 10.10.0.0/16</td>
</tr>
<tr>
<td>greater &lt;packet-length&gt;</td>
</tr>
<tr>
<td>greater 500 //All packets with size &gt;= 500</td>
</tr>
<tr>
<td>less &lt;packet-length&gt;</td>
</tr>
<tr>
<td>Logical expressions (with and/or/&amp;/&amp;=/</td>
</tr>
<tr>
<td>ether[0] &amp; 1 = 0</td>
</tr>
<tr>
<td>ip[16] &gt;= 224</td>
</tr>
</tbody>
</table>

Device Analytics Parameters

Use the following parameters to configure Device Analytics. Additionally, you can configure the Device Analytics feature to only enable services of your choice.

**feature.da.enabled**

1 (default) – Enable the Device Analytics feature.
0 – Disable the Device Analytics feature.
Change causes system to restart or reboot.

**feature.obitalk.enabled**

0 (default) - Disable the connection to the OBiTalk cloud.
1 - Enable the connection to the OBiTalk cloud.
Change causes system to restart or reboot.

**obitalk.accountCode**

Null (default)
String (maximum of 256 characters).
Change causes system to restart or reboot.

**da.supported.services**

Specify the Device Analytics service to enable.

*all* (default)

Comma separated list of below strings need to be configured (maximum of 2048 characters)

- ni
- service
- tsid
- pcap
- log
- config
- core
- vqmon
- cdr
- uptimeanalytics
- hardwareanalytics
- uianalytics
- restart
- reboot
- resettofactory
- restapi

Change causes system to restart or reboot.

**deviceAnalytics.note**

Sets the self-note value on the phone and sends to cloud with primary device information message.

*Null* (default)

*String* (maximum of 512 characters).

**Poly Cloud Connector Parameters**

In order to send Device Analytics details to Poly Cloud Services, you must enable the Poly Cloud Connector for Poly Trio systems.

**feature.pcc.enabled**
0 - Disables the Poly Cloud Connector for Poly Trio systems.

1 (default) - Enables the Poly Trio system to interface with the Poly Cloud Connector.

Change causes system to restart or reboot.

**pcc.url**

Set the URL for the Poly Cloud Connector interface.

`https://api-global.plcm.cloud/globaldirectory` (default)

0 - 256

Change causes system to restart or reboot.

**pcc.accountCode**

Enter the Poly Cloud Connector account code to connect your device with a Poly Cloud Services account.

Null (default)

0 - 256

Change causes system to restart or reboot.

---

**Turn Off the System Usage Data Collection**

You can stop Poly Trio from sending system usage data to Poly.

**Procedure**

- Set the following parameters to turn off data collection:
  - `feature.pcc.enabled = 0`
  - `feature.da.enabled = 0`
System Logs

Topics:

- Configuring Log Files
- Logging Levels
- Upload Logs to the Provisioning Server
- Upload Poly Trio System Logs
- Uploading Logs to a USB Flash Drive

System log files assist when troubleshooting issues.

System log files contain information about system activities and the system configuration profile. After setting 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. In such a situation, 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` containing parameters that configure log levels.

Configuring Log Files

You can configure log files using logging parameters.

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.

When the Poly Trio Visual+ accessory is paired with a Poly Trio system, logging information from both devices is written to the same log files.

When you pair a Poly Trio system with a Trio Visual Pro or RealPresence Group Series system, you must use the Poly Trio VisualPro or RealPresence Group Series system’s web interface to download log files.

- **Boot Log** – Boot logs are sent 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](#).
Severity of Logging Event Parameter

You can configure the severity of the events that are logged independently for each module of the Polycom UC Software. This enables you to capture lower severity events in one part of the application, and high severity events for other components. Severity levels range from 0 to 6, where 0 is the most detailed logging and 6 captures only critical errors.

Note: User passwords display in level 1 log files.

You must contact Poly Customer Support to obtain the template file `techsupport.cfg` containing parameters that configure log levels.

`log.level.change.module_name`

Set the severity level to log for the module name you specify. Not all modules are available for all phone models.

For a list of available module names, module descriptions, and log level severity, see refer to the Web Configuration Utility at Settings > Logging > Module Log Level Limits.

Log File Collection and Storage Parameters

You can configure log file collection and storage using the parameters in the following list. You must contact Customer Support to obtain the template file `techsupport.cfg` containing parameters that configure log file collection and storage.

The Poly Trio solution uploads a system log file `[MAC address]-plcmsyslog.tar.gz` that contains Android logs and diagnostics. This file can be ignored but does contain minimal data that may be useful to investigate Android issues.

There is no way to prevent the system log file `[MAC address]-plcmsyslog.tar.gz` from uploading to the server and you cannot control it using the parameters `log.render.file.upload.append.sizeLimit` and `log.render.file.upload.append.limitMode`. However, you can control the frequency of uploads using `log.render.file.upload.system.period`.

`log.render.level`

Specify the events to render to the log files. Severity levels are indicated in brackets.

0 - SeverityDebug (7)
1 - SeverityDebug (7) - default
2 - SeverityInformational (6)
3 - SeverityInformational (6)
4 - SeverityError (3)
5 - SeverityCritical (2)
6 - SeverityEmergency (0)
**log.render.file.size**
Set the maximum file size of the log file. When the maximum size is about to be exceeded, the phone uploads all logs that have not yet been uploaded and erases half of the logs on the phone. You can use a web browser to read logs on the phone.

512 kb (default)
1 - 10240 kB

**log.render.file.upload.period**
Specify the frequency in seconds between log file uploads to the provisioning server.
Note: The log file is not uploaded if no new events have been logged since the last upload.
172800 seconds (default) - 48 hours

**log.render.file.upload.append**
1 (default) - Log files uploaded from the phone to the server are appended to existing files. You must set up the server to append using HTTP or TFTP.
0 - Log files uploaded from the phone to the server overwrite existing files.
Note that this parameter is not supported by all servers.

**log.render.file.upload.append.sizeLimit**
Specify the maximum size of log files that can be stored on the provisioning server.
512kb (default)
Note that this parameter is not supported by HTTP/HTTPS or TFTP protocols. Logs generated and uploaded via HTTP/HTTPS or TFTP protocol must be deleted manually if needed.

**log.render.file.upload.append.limitMode**
Specify whether to stop or delete logging when the server log reaches its maximum size.
delete (default) - Delete logs and start logging again after the file reaches the maximum allowable size specified by `log.render.file.upload.append.sizeLimit`.
stop - Stop logging and keep the older logs after the log file reaches the maximum allowable size.
Note that this parameter is not supported by HTTP/HTTPS or TFTP protocols. Logs generated and uploaded via HTTP/HTTPS or TFTP protocol must be deleted manually if needed.

**log.render.file.upload.system.period**
Specify the frequency in seconds the Poly Trio system uploads the Android system log file MAC address]-plcmsyslog.tar.gz to the server.
86400 seconds (default)
0 - 2147483647 seconds
Logging Levels

The event logging system supports the classes of events listed in the table Logging Levels.

Two types of logging are supported:

- Level, change, and render
- Schedule

**Note:** Logging parameter changes can impair system operation. Do not change any logging parameters without prior consultation with Technical Support.

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Debug only</td>
</tr>
<tr>
<td>1</td>
<td>High detail class event</td>
</tr>
<tr>
<td>2</td>
<td>Moderate detail event class</td>
</tr>
<tr>
<td>3</td>
<td>Low detail event class</td>
</tr>
<tr>
<td>4</td>
<td>Minor error</td>
</tr>
<tr>
<td>5</td>
<td>Major error – will eventually incapacitate the system</td>
</tr>
<tr>
<td>6</td>
<td>Fatal error</td>
</tr>
</tbody>
</table>

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

Logging Level, Change, and Render Parameters for Poly Trio

Use the following parameters to configure logging features.

**log.level.change.app**

Initial logging level for the Apps log module.
log.level.change.bfcp
Initial logging level for the BFCP content log module.
4 (default)
0 - 6

log.level.change.dasvc
Initial logging level for Device analytics logs.
4 (default)
0 - 6

log.level.change.fec
Sets the log level for video FEC.
4 (default)
0 - 6

log.level.change.fecde
Sets high volume log level to decode video FEC.
4 (default)
0 - 6

log.level.change.fecen
Sets high volume log level to encode video FEC.
4 (default)
0 - 6

log.level.change.flk
Sets the log level for the FLK logs.
4 (default)
0 - 6

log.level.change.mr
Initial logging level for the Networked Devices log module.
4 (default)
**log.level.change.mraud**
Initial logging level for the Networked Devices Audio log module.
4 (default)
0 - 6

**log.level.change.mrcam**
Initial logging level for the Networked Devices Camera log module.
4 (default)
0 - 6

**log.level.change.mrci**
Initial logging level for the Networked Devices HDMI/VGA Content Input log module.
4 (default)
0 - 6

**log.level.change.mrcon**
Initial logging level for the Networked Devices Connection log module.
4 (default)
0 - 6

**log.level.change.mrdis**
Initial logging level for the Networked Devices Display log module.
4 (default)
0 - 6

**log.level.change.mrmgr**
Initial logging level for the Networked Devices Manager log module.
4 (default)
0 - 6

**log.level.change.opxy**
Define the log level for the OPXY ** log. The default logging level for the OPXY ** log is Minor Error.
4 (default)
0 - 6
**log.level.change.ppcip**
Initial logging level for the People+Content IP log module.
4 (default)
0 - 6

**log.level.change.prox**
Initial logging level for the Proximity log module.
4 (default)
0 - 6

**log.level.change.ptp**
Initial logging level for the Precision Time Protocol log module.
4 (default)
0 - 6

**log.level.change.usba**
Sets the logging detail level for the USB audio log.
4 (default)
0 - 6

**log.level.change.usbh**
Sets the logging detail level for the USB HID log.
4 (default)
0 - 6

**log.level.change.xxx**
Controls the logging detail level for individual components. These are the input filters into the internal memory-based log system.
4 (default)
0 - 6

Possible values for xxx are acom, ares, app1, bluet, bdiag, brow, bsdir, cap, cdp, cert, cfg, cipher, clink, clist, cmp, cmr, copy, curl, daa, dapi, dasvc, dbs, dbuf, dhpc, dis, dock, dot1x, dns, drvbt, ec, efk, ethf, flk, fec, fecde, fecen, fur, h323, hset, httpa, httpd, hw, ht, ib, key, ldap, lic, lldp, loc, log, mb, mcu, mobil, mrcl, net, niche, ocsp, osd, pcap, pcd, peer, pgui, pkt, pmt, poll, pps, pres, pstn, ptt, push, pwsrv, rdisk, res, restapi, rtos, rtls, sec, sig, sip, slog, so, srtp, sshc, ssp, stac, statn, style, sync, sys, ta, task, tis, trace, ttrs, usb, usbio, util, utilim, vsr, wdog, wmgr, and xmpp.
**log.render.file**

Polycom recommends that you do not change this value.

1 (default)

0

**log.render.realtime**

Polycom recommends that you do not change this value.

1 (default)

0

**log.render.stdout**

Polycom recommends that you do not change this value.

0 (default)

1

**log.render.type**

Refer to the Event Timestamp Formats table for timestamp type.

2 (default)

0 - 2

---

**Logging Parameters**

The phone can be configured so certain advanced logging tasks take place scheduled basis.

Poly recommends that you set the parameters listed below with consultation with Polycom Technical Support. Each scheduled log task is controlled by a unique parameter set starting with `log.sched.x` where `x` identifies the task. A maximum of 10 schedule logs is allowed.

**log.sched.x.level**

The event class to assign to the log events generated by this command.

3 (default)

0 - 5

This needs to be the same or higher than `log.level.change.slog` for these events to display in the log.

**log.sched.x.period**

Specifies the time in seconds between each command execution.

15 (default)

positive integer
log.sched.x.startDay

When startMode is abs, specifies the day of the week to start command execution. 1=Sun, 2=Mon, ..., 7=Sat
7 (default)
0 - 7

log.sched.x.startMode

Starts at an absolute or relative time to boot.
Null (default)
0 - 64

log.sched.x.startTime

Displays the start time in seconds since boot when startMode is rel or displays the start time in 24-hour clock format when startMode is abs.
Null (default)
positive integer, hh:mm

Upload Logs to the Provisioning Server

You can manually upload logs to the provisioning server.

When you manually upload log files, the word now is inserted into the name of the file, for example, 0004f200360b-now-boot.log.

Procedure

» Press the multiple key combination 1-5-9 on the phone.

Upload Poly Trio System Logs

You can upload log files to your provisioning server.

Uploading log files copies the log files from the phone to the provisioning server and creates new files named <MACaddress>-now-xxx.log.

Procedure

1. Go to Settings > Advanced and enter the administrator password (default 456).
2. Go to Administration Settings > Upload Configuration.
3. Select one or more sources to upload from:
   • All Sources
   • Configuration Files
   • Local
Uploading Logs to a USB Flash Drive

You can configure your Poly Trio systems to copy application and boot logs to a USB flash drive connected to the phone. USB log collection is not supported on Poly Trio 8300.

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.

**USB Logging Parameter**

The following parameters configure the USB logging feature.

`feature.usbLogging.enabled`

- 0 (default) – Disables collecting logs using a USB flash drive.
- 1 – Enables collecting logs using a USB flash drive.
Troubleshooting

Topics:
- 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
- Software Upgrade Issues
- Provisioning Issues

The following sections address several issues you might encounter, along with suggested actions to resolve them.

Updater Error Messages and Possible Solutions

If a fatal error occurs, the phone does not boot up.

If the error is not 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.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause and Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to get boot parameters via DHCP</td>
<td>The phone does not have an IP address and therefore cannot boot.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Check the DHCP configuration.</td>
</tr>
<tr>
<td>Application &lt;file name&gt; is not compatible with this phone!</td>
<td>An application file was downloaded from the provisioning server, but it cannot be installed on this phone.</td>
</tr>
<tr>
<td></td>
<td>Install a compatible software image on the provisioning server. Be aware that there are various hardware and software dependencies.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Cause and Possible Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Could not contact boot server using existing configuration</td>
<td>The phone cannot contact the provisioning server. Possible causes include:</td>
</tr>
<tr>
<td></td>
<td>• Cabling issues</td>
</tr>
<tr>
<td></td>
<td>• DHCP configuration</td>
</tr>
<tr>
<td></td>
<td>• Provisioning server problems</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Error, application is not present!</td>
<td>The phone does not have an application stored in device settings and cannot boot because an application could not be downloaded.</td>
</tr>
<tr>
<td></td>
<td>• Download compatible Polycom UC Software to the phone using one of the supported provisioning protocols.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Polycom UC Software Error Messages**

If an error occurs in the UC Software, an error message and a warning icon displays on the phone. The following table describes Polycom UC Software error messages.
## Polycom UC Software Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause</th>
</tr>
</thead>
</table>
| Config file error: Files contain invalid params: `<filename1>`, `<filename2>`,... | These messages display if the configuration files contain these deprecated parameters:  
• tone.chord.ringer.x.freq.x  
• se.pat.callProg.x.name  
• ind.anim.IP_500.x.frame.x.duration  
• ind.pattern.x.step.x.state  
• feature.2.name  
• feature.9.name  
This message also displays if any configuration file contains more than 100 of the following errors:  
• Unknown parameters  
• Out-of-range values  
• Invalid values.  
To check that your configuration files use correct parameter values, refer to Using Correct Parameter XML Schema, Value Ranges, and Special Characters. |
| Config file error: `<filename>` contains invalid params |  |
| The following contain pre-3.3.0 params: `<filename>` |  |

<table>
<thead>
<tr>
<th>Line: Unregistered</th>
<th>This message displays if a line fails to register with the call server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login credentials have failed. Please update them if information is incorrect.</td>
<td>This message displays when the user enters incorrect login credentials on the phone: Status &gt; Basic &gt; Login Credentials.</td>
</tr>
<tr>
<td>Missing files, config. reverted</td>
<td>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 <code>&lt;MAC Address&gt;.cfg</code> file are not present on the provisioning server.</td>
</tr>
<tr>
<td>Network link is down</td>
<td>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.</td>
</tr>
</tbody>
</table>

## 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.
<table>
<thead>
<tr>
<th>Event Code</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown events</td>
<td>An unknown event by ‘1’ can include any issues listed in this table.</td>
</tr>
<tr>
<td>2</td>
<td>Mismatch in EAP Method type</td>
<td>Authenticating server's list of EAP methods does not match with clients’.</td>
</tr>
<tr>
<td>30xxx</td>
<td>TLS Certificate failure</td>
<td>The phone displays the following codes:</td>
</tr>
<tr>
<td></td>
<td>000 - Represents a generic certificate error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>042 - bad cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>043 - unsupported cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>044 - cert revoked</td>
<td></td>
</tr>
<tr>
<td></td>
<td>045 - cert expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>046 - unknown cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>047 - illegal parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>048 - unknown CA</td>
<td></td>
</tr>
<tr>
<td>31xxx</td>
<td>Server Certificate failure</td>
<td>‘xxx’ can use the following values:</td>
</tr>
<tr>
<td></td>
<td>•009 - Certificate not yet Valid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>•010 - Certificate Expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>•011 - Certificate Revocation List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(CRL) not yet Valid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>•012 - CRL Expired</td>
<td></td>
</tr>
<tr>
<td>4xxx</td>
<td>Other TLS failures</td>
<td>‘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. See section 7.2 of RFC 2246 for further TLS alert codes and error codes.</td>
</tr>
<tr>
<td>5xxx</td>
<td>Credential failures</td>
<td>5xxx - wrong user name or password</td>
</tr>
<tr>
<td>Event Code</td>
<td>Description</td>
<td>Comments</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>6xxx</td>
<td>PAC failures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>080 - No PAC file found</td>
<td></td>
</tr>
<tr>
<td></td>
<td>081 - PAC file password not provisioned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>082 - PAC file wrong password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>083 - PAC file invalid attributes</td>
<td></td>
</tr>
<tr>
<td>7xxx</td>
<td>Generic failures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>001 - dot1x can not support (user) configured EAP method</td>
<td></td>
</tr>
<tr>
<td></td>
<td>002 - dot1x can not support (user) configured security type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>003 - root certificate could not be loaded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>174 - EAP authentication timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>176 - EAP Failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>185 - Disconnected</td>
<td></td>
</tr>
</tbody>
</table>

**Power and Start-up Issues**

The following table describes possible solutions to power and start-up issues.

<table>
<thead>
<tr>
<th>Power or Start-up Issue</th>
<th>Possible Solutions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The phone has power issues or the phone has no power.</td>
<td>Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Verify that no lights appear on the unit when it is powered up.</td>
</tr>
<tr>
<td></td>
<td>• Check to see if the phone is properly plugged into a functional AC outlet.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that the phone is not plugged into an outlet controlled by a light switch that is turned off.</td>
</tr>
<tr>
<td></td>
<td>• If the phone is plugged into a power strip, try plugging directly into a wall outlet instead.</td>
</tr>
<tr>
<td>The phone does not boot.</td>
<td>If the phone does not boot, there may be a corrupt or invalid firmware image or configuration on the phone:</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the provisioning server is accessible on the network and a valid software load and valid configuration files are available.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the phone is configured with the correct address for the provisioning server on the network.</td>
</tr>
</tbody>
</table>
Screen and System Access Issues

The following table describes possible solutions to screen and system access issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause and Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no response from feature key presses.</td>
<td>If your phone keys do not respond to presses:</td>
</tr>
<tr>
<td></td>
<td>• Press the keys more slowly.</td>
</tr>
<tr>
<td></td>
<td>• Check to see whether or not the key has been mapped to a different function or disabled.</td>
</tr>
<tr>
<td></td>
<td>• Make a call to the phone to check for inbound call display and ringing. If successful,</td>
</tr>
<tr>
<td></td>
<td>try to press feature keys while a call is active to access a directory or buddy status.</td>
</tr>
<tr>
<td></td>
<td>• On the phone, go to <strong>Menu &gt; Status &gt; Lines</strong> to confirm the line is actively registered</td>
</tr>
<tr>
<td></td>
<td>to the call server.</td>
</tr>
<tr>
<td></td>
<td>Reboot the phone to attempt re-registration to the call server.</td>
</tr>
<tr>
<td></td>
<td>Go to <strong>Menu &gt; Settings &gt; Advanced &gt; Reboot Phone</strong>).</td>
</tr>
<tr>
<td>The display shows the message &quot;Network Link is Down&quot;.</td>
<td>This message displays when the LAN cable is not properly connected. Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Check the termination at the switch or hub end of the network LAN cable.</td>
</tr>
<tr>
<td></td>
<td>• Check that the switch or hub is operational (flashing link/status lights).</td>
</tr>
<tr>
<td></td>
<td>• On the phone, go to <strong>Menu &gt; Status &gt; Network</strong>. Scroll down to verify that the LAN is</td>
</tr>
<tr>
<td></td>
<td>active.</td>
</tr>
<tr>
<td></td>
<td>• Ping the phone from a computer.</td>
</tr>
<tr>
<td></td>
<td>Reboot the phone to attempt re-registration to the call server.</td>
</tr>
<tr>
<td></td>
<td>Go to <strong>Menu &gt; Settings &gt; Advanced &gt; Reboot Phone</strong>).</td>
</tr>
</tbody>
</table>

Calling Issues

The following table provides possible solutions to common calling issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause and Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no dial tone.</td>
<td>If there is no dial tone, power may not be correctly supplied to the phone. Try one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Check that the display is illuminated.</td>
</tr>
<tr>
<td></td>
<td>• Make sure the LAN cable is inserted properly at the rear of the phone; try unplugging and re-inserting the cable.</td>
</tr>
<tr>
<td></td>
<td>If you are using in-line powering, check that the switch is supplying power to the phone.</td>
</tr>
<tr>
<td>Issue</td>
<td>Cause and Possible Solution</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| The phone does not ring. | If there is no ringtone but the phone displays a visual indication when it receives an incoming call, do the following:  
  • Adjust the ring level from the front panel using the volume up/down keys.  
  Check the status of handset, headset (if connected), and hands-free speakerphone. |
| 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.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause and Possible Solution</th>
</tr>
</thead>
</table>
| There is no display or the display is incorrect. | If there is no display, power may not be correctly supplied to the phone. Do one of the following:  
  • Check that the display is illuminated.  
  • Make sure the power cable is inserted properly at the rear of the phone.  
  • If your are using PoE powering, check that the PoE switch is supplying power to the phone.  
  Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to Capture Your Device's Current Screen. |
| The display is too dark or too light. | The phone contrast may be set incorrectly. Do one of the following:  
  • Adjust the contrast.  
  • Reboot the phone to obtain the default level of contrast. |
| The display is flickering. | 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. |
### Cause and Possible Solution

_The time and date are flashing._

If the time and date are flashing, the phone is disconnected from the LAN or there is no SNTP time server configured. Do one of the following:

- Reconnect the phone to the LAN.
- Configure an SNTP server.

Disable the time and date if you do not want to connect your phone to a LAN or SNTP server.

---

## Software Upgrade Issues

The following table describes possible solutions to issues that may occur during or after a software upgrade.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause and Possible Solutions</th>
</tr>
</thead>
</table>
| Some settings or features are not working as expected on the phone. | The phone's configuration may be incorrect or incompatible.  
Check for errors on the phone by navigating to Menu > Status > Platform > Configuration. If there are messages stating Errors Found, Unknown Params, or Invalid values, correct your configuration files and restart the phone. |
| The phone displays a Config file error message for five seconds after it boots up. | 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. Correct the configuration files, remove the invalid parameters, and restart the phone. |
### Issue and Possible Solutions

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause and Possible Solutions</th>
</tr>
</thead>
</table>
| When using the Web Configuration Utility to upgrade phone software, the phone is unable to connect to the Polycom Hosted Server. | Occasionally, the phone is unable to connect to the Polycom-hosted server because of the following:  
• The Polycom-hosted server is temporarily unavailable.  
• There is no software upgrade information for the phone to receive.  
• The network configuration is preventing the phone from connecting to the Polycom hosted server. |
| To troubleshoot the issue:                                            | • Try upgrading your phone later.  
• Verify that new software is available for your phone using the Polycom UC Software Release Matrix.  
• Verify that your network’s configuration allows the phone to connect to [http://downloads.polycom.com](http://downloads.polycom.com). |
|                                                                      | If the issue persists, try manually upgrading your phone’s software. |

### Provisioning Issues

If settings you make from the central server are not working, check first for priority settings applied from the phone menu system or Web Configuration Utility. Afterward, check for duplicate settings in your configuration files.

### Place the Poly Trio System into Recovery Mode

You can place Poly Trio systems into recovery mode when you want to provision with a USB and the provisioning process is not working during normal phone functioning.

#### Procedure

1. Ensure that the phone is powered off.
2. Plug in a USB device.
3. Power up the phone.
4. When the Poly logo displays, press and hold with four fingers the four corners of the LCD screen until the LEDs blink.  
   (Blinking rotates between orange/red/green/off).
5. Remove fingers from the LCD screen.  
   Recovery process is complete when the device reboots.

### Place Poly Trio Visual+ into Recovery Mode

You can place the Poly Trio Visual+ into recovery mode when you want to provision with a USB and the provisioning process is not working during normal phone functioning.
Procedure

1. Ensure that the phone is powered off.
2. Plug in a USB device.
3. Power up the phone.
4. When the LED initially turns from on to off, press and hold the pairing button until the pairing LED turns orange and release the button.
   
   The pairing LED blinks. (Blinking rotates between orange/red/green/off).
   
   Recovery process is complete when the device reboots.
Content

Topics:

• Content Sharing
• Screen Mirroring

Poly Trio systems support several content sharing options, including AirPlay and Miracast, Polycom Content application, and Polycom RealPresence Desktop.

Content Sharing

You can share content to the local monitor when your Poly Trio system is paired with a Poly Trio Visual+ or Trio VisualPro system. You cannot share content in a Skype for Business meeting.

To share content:

• The Poly Trio Visual+ or Trio VisualPro system must be paired with a Poly Trio system.
• The computer and Poly Trio system must be able to communicate on the same IP network.

You can use the following methods to share content locally:

• Polycom® People+Content™ (PPCIP) technology
• Polycom Content App
• Polycom® RealPresence® Desktop for Windows® or Mac®
• Polycom® RealPresence® Mobile app
• Device connected to a paired Trio VisualPro system with an HDMI or VGA cable

You can download People+Content IP and RealPresence Desktop from Polycom Support and RealPresence Mobile from your mobile application store.

For information about using PPCIP on the Poly Trio solution registered with Skype for Business, see the Poly Trio - User Guide at Poly Trio on Polycom Support.

Note: The default port used by Group Paging when enabled conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Poly Trio system. Since the port used by People+Content is fixed and cannot be configured, configure one of the following workarounds:

• Configure a different port for Group Paging using parameter ptt.port.
• Disable People+Content IP using parameter content.ppcipServer.enabled="0".

Content Sharing Parameters

Use the following parameters to configure content sharing options.

To enable device pairing with the Poly Trio solution, use the smartpairing* parameters.

Note: The Poly Trio 8300 system and People+Content IP technology do not support ultrasonic SmartPairing.
content.autoAccept.rdp
1 (default) - Content sent via Skype for Business Remote Desktop Protocol (RDP) by far-end users is automatically accepted and displayed on a near-end Poly Trio solution.
0 - Near-end users are prompted to accept Skype for Business RDP content sent to Poly Trio solution from a far-end user.

content.bfcp.enabled
1 (default) - Enable content sharing by offering or accepting the Binary Floor Control Protocol (BFCP) in Session Description Protocol (SDP) negotiation during SIP calls. Does not apply to Skype for Business calls.
0 - Disable content sharing using BFCP.

content.bfcp.port
15000 (default)
0 - 65535

content.bfcp.transport
UDP (default)
TCP

content.local.bitRate
Set the default maximum bit rate for local content, content not shared during an active call.
8000000 (8Mb/s) (default)
2000000 - default for Poly Trio 8300
Range is 1000000 (1Mb/s) to 20000000 (20Mb/s).
This parameter does not apply to content shared using Screen Mirroring with Airplay or the Wireless Display feature.

mr.content.rdp.tls.enabled
Enable or disable TLS encryption of Skype for Business RDP content between hubs and devices.
1 (default)
0

mr.content.rdp.tls.enabled
1 (default) - Enable TLS encryption of Skype for Business RDP content between hubs and devices.
Disable TLS encryption of Skype for Business RDP content.
**mr.contentStreamPortEnd**

The IP port range end port used for content input streams received from the Poly Trio Visual+ system.

4320 (default)

1024 – 65436

**mr.contentStreamPortStart**

The IP port range start port used for content input streams received from the Poly Trio Visual+ system.

4300 (default)

1024 – 65436

**mr.localContent.autoDisplay.enable**

1 (Default) – Content automatically displays when an HDMI cable is plugged in.

0 – Content does not automatically start if HDMI is plugged in. Use the Poly Trio system user interface to begin sharing content.

**reg.x.content.bfcp.enabled**

1 (default) - Enable Binary Floor Control Protocol content to be shared during calls for the line you specify.

0 - Disable Binary Floor Control Protocol content.

**smartPairing.mode**

Enables users with People+Content IP or Desktop on a computer or Mobile on a tablet to pair with the Poly Trio conference phone using SmartPairing.

Disabled (default) - Users cannot use SmartPairing to pair with the conference phone.

Manual - Users must enter the IP address of the conference phone to pair with it.

**smartPairing.volume**

The relative volume to use for the SmartPairing ultrasonic beacon.

6 (default)

0 - 10

**Polycom Content Application**

The Polycom Content App enables users to share content over IP from a Poly Trio 8500 or 8800 system with a paired Poly Trio Visual+ or Poly Trio Visual Pro system.

When a user connects to a Poly Trio system over IP in the Polycom Content app, if enabled, the pass code displays in the Global menu on the system and on the connected monitor when the system is idle;
when in a call, the pass code displays in the Global menu, but it does not display on the connected monitor.

For more information on using the Polycom Content App, refer to the Polycom Content App User Guide on the Polycom Documentation Library.

**Bluetooth Discovery on Poly Trio with the Polycom Content Application**

You can share content through the Polycom Content App, version 1.3 or later, by connecting the Poly Trio system to the application.

To enable users to connect Poly Trio to the Polycom Content application, you need to configure Poly Trio to advertise the system's IP address over Bluetooth using the parameter `bluetooth.beacon.ipAddress.enabled`. When this parameter is set to 1, the Bluetooth radio is automatically turned on for the system, and the IP address for the system is sent to the Polycom Content app over Bluetooth. You can also enable Bluetooth discovery on the phone and in the Web Configuration Utility.

The parameter `bluetooth.beacon.ipAddress.enabled` also replaces the parameter `content.airplayServer.discovery.bluetooth.enabled` for AirPlay discovery over Bluetooth.

**Bluetooth Discovery Parameters**

Use the following parameter to enable Bluetooth Discovery between Poly Trio and the Polycom Content App.

`bluetooth.beacon.ipAddress.enabled`

Set to send the IP address of the system over Bluetooth.

1 (default) - Enables sending the system IP address over Bluetooth. Turns Bluetooth radio on when `feature.bluetooth.enabled = 1`.

0 - Disables sending the system IP address over Bluetooth

Note: Enable the parameter `feature.bluetooth.enabled` to use this feature.

**Polycom People+Content IP**

Sharing content with Polycom People+Content IP from a computer connected over IP supports 1080p resolution at a maximum of 30 frames per second (fps) on one or more connected monitors. The computer and Poly Trio solution must be able to communicate on the same IP network, and you must pair your Polycom software application with the Poly Trio system.

When you register Poly Trio systems with Skype for Business, you can only share content to a local monitor. You can’t share content from a Poly Trio system over a Skype for Business call. For instructions, see the Poly Trio Solution User Guide at Poly Trio in the Polycom Documentation Library.

**Polycom People+Content IP Parameters**

The following table lists parameters that configure content sharing with the Poly Trio solution.

`content.ppcip.resolutionPreferred`
1 (default) – The Poly Trio system attempts to get higher resolution content with lower frames per second after the SDP negotiation.
0 - Content resolution is set based on the SDP negotiation.

content.ppcipServer.authType

The authentication type used for PPCIP content sessions.
none (default) - No security code for Polycom People+Content IP-enabled clients is required.
passcode - Use a security code to authenticate Polycom People+Content IP-enabled clients.

content.ppcipServer.enabled

1 (default) - Enable Polycom People+Content IP content server for sharing.
0 - Disable Polycom People+Content IP content server.

content.ppcipServer.enabled.Trio8500

1 (default) - Enable Polycom People+Content IP content server for content sharing with Poly Trio 8500.
0 - Disable Polycom People+Content IP content server for Poly Trio 8500.

content.ppcipServer.enabled.Trio8800

1 (default) - Enable Polycom People+Content IP content server for content sharing with Poly Trio 8800.
0 - Disable Polycom People+Content IP content server for Poly Trio 8800.

Polycom People+Content IP over USB

You can use Polycom® People+Content® IP (PPCIP) to share video or data to a local monitor connected to the Poly Trio 8500 or 8800 system using a Windows® or Mac® computer connected by USB to the Poly Trio system. This is not supported on Poly Trio 8300.

When you install PPCIP version 1.4.2 and run it unopened in the background, the PPCIP application pops up immediately when you connect the computer to Poly Trio solution via USB.

Keep the following points in mind:

• You can show content with People+Content IP on a Windows or Mac computer connected by USB to Poly Trio to a maximum of 1080p resolution and a maximum of 30 frames per second (fps).
• Audio content is not shared.
• Content sent from People+Content is sent over USB, and no network connection is needed. This is useful for environments where guest IP access is not allowed. You must use UC Software 5.4.3AA or later to share your desktop at up to 1080p resolution using a Mac computer connected by USB to the Poly Trio solution.
Important: The default port used by Group Paging when enabled (ptt.pageMode.enable="1") conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Poly Trio system. Since the port used by People+Content is fixed and cannot be configured, configure one of two workarounds:

- Configure a different port for Group Paging using parameter ptt.port or
- Disable People+Content IP using parameter content.ppcipServer.enabled="0".

Polycom People+Content IP over USB Parameter
The following parameter configures the People+Content over USB feature.

**feature.usb.device.content**

1 (default) - Enable content sharing using the People+Content IP application on a computer connected by USB to Poly Trio solution.

Default is 0 for Poly Trio 8300.

0 - Disable content sharing using the People+Content IP application on a computer connected by USB to Poly Trio solution.

HDMI and VGA Content Sharing Parameters
Use the following parameters to configure HDMI and VGA content sharing with the paired Poly Trio VisualPro or RealPresence Group Series system.

**mr.contentStreamPortStart**
Sets where the IP port range begins for content input streams from a network device.

4300 (default)
1024 - 65436

Change causes system to restart or reboot.

**mr.contentStreamPortEnd**
Sets where the IP port range ends for content input streams from a network device.

4320 (default)
1024 - 65436

Change causes system to restart or reboot.

Display Content Automatically While Idle
You can share content while the Poly Trio system is idle. This feature requires a connection via HDMI to a paired Poly Trio VisualPro or RealPresence Group Series system. You can display content on a monitor
at all times when the Poly Trio system isn’t in a call. For example, you can display instructions to help users understand the features of the conference room.

After the Poly Trio system enters an idle state, the content displays. You can stop the content from displaying. The content displays again after a configurable idle time.

**Display Content While Idle Parameters**

Set up the Poly Trio system to display content when idle using the following parameters.

**mr.localContent.autoDisplay.idle**

- When the phone is not in a call, content shared via HDMI is displayed on a connected monitor.
- 0 (Default) – Content does not display when the phone is idle.
- 1 – Content displays when the phone is idle.

**mr.localContent.autoDisplay.idle.autoResumeTimeout**

- Sets the amount of idle time, in minutes, allowed after content sharing is stopped. Once this time limit is reached, the content sharing resumes.
- 60 (default)
- 0 - Infinite

**Screen Mirroring**

The Poly Trio 8800 system supports screen mirroring locally from Apple®-certified devices and the Wireless Display feature for Miracast®-certified Android™ and Windows® devices.

**Screen Mirroring with AirPlay-Certified Devices**

This section provides information you need to set up and configure a Poly Trio 8800 system to work with AirPlay-certified devices.

The following information applies to using AirPlay-certified devices with the Poly Trio system:

- You can display local content only from your AirPlay-certified device to the Poly Trio 8800 system monitor.
- Sharing content from direct streaming sources, such as YouTube™ or web links, is not supported.
- If you share content during a point-to-point or conference call, the content is not sent to far-end participants.
- Audio-only content is not supported. If you only want to share audio, consider using Bluetooth or USB connectivity.
- Apple Lossless Audio Codec (ALAC) is not supported.

Poly Trio 8800 systems support the following AirPlay-certified devices:

- Apple®
- iPad®
- iPad Pro™
• MacBook Pro®

The Poly Trio 8800 system supports a maximum resolution and frame rate of 720p@60fps or 1080p@30fps. If configured for 1080p resolution, an iPad often sends 60fps video, which can result in latency in mirroring, visual artifacts, or both.

When the Poly Trio 8800 system receives content from a Skype for Business client using the Remote Desktop Protocol (RDP) at the same time as content from an AirPlay-certified device, the AirPlay content takes precedence and displays. When you end AirPlay content, available Skype for Business content displays.

Requirements for Screen Mirroring with AirPlay

You must meet the following requirements to use the screen mirroring feature on an AirPlay-certified device with a Poly Trio 8800 system:

• Poly Trio collaboration kit running UC Software version 5.4.4AA or later
• The Poly Trio system and Apple devices are on the same subnet.
  The devices can be on different subnets if the devices are routable and multicast DNS (Bonjour) is bridged between the subnets for discovery. The devices can also be on different subnets if AirPlay Discovery over Bluetooth is enabled, the subnets are routable to each other, and the device is within Bluetooth range.
• The screen mirroring feature uses the following ports:
  ◦ Discovery: UDP port 5353
  ◦ Sessions: TCP ports 7000, 7100, 8009, and 47000; UDP port 1900

Poly Trio 8800 for AirPlay Parameters

Use the following parameters to configure the Poly Trio 8800 system for AirPlay-certified devices.

**bluetooth.beacon.ipAddress.enabled**

Set to send the IP address of the system over Bluetooth.

1 (default) - Enables sending the system IP address over Bluetooth. Turns Bluetooth radio on when `feature.bluetooth.enabled = 1`.

0 - Disables sending the system IP address over Bluetooth

Note: Enable the parameter `feature.bluetooth.enabled` to use this feature.

**content.airplayServer.authType**

none (default) - No security code for AirPlay certified devices is required.

passcode - Use a security code to authenticate AirPlay-certified devices.

**content.airplayServer.enabled**

0 (default) - Disable the content sink for AirPlay-certified devices.

1 - Enable the content sink for AirPlay-certified devices.
**content.airplayServer.maxResolution**

Set the content resolution.

- 720p (default)
- 1080p
- 1024x1024
- 960x960
- 480x480

**content.airplayServer.name**

Specify a system name for the local content sink for AirPlay certified devices. If left blank the previously configured or default system name is used.

NULL (default)

**content.local.authChangeInterval**

Set the interval in minutes between changes to the local content authentication credentials.

- 1440 (default)
- 0 - 65535
- 0 - Do not change

**content.local.authChangeMode**

Specify when the security code for content sharing with AirPlay-certified devices changes.

- session (default) - Code changes at the end of each content sharing session.
- relativeTime - Code changes at an interval specified by the `content.local.authChangeInterval` parameter.

**Troubleshooting**

This section provides solutions to common issues you may have using the Poly Trio 8800 system with AirPlay-certified devices.

**The Poly Trio 8800 system does not advertise on my device**

The Poly Trio may not be broadcasting for discovery, or the broadcasts are being blocked.

- Ensure your Apple device is on the same subnet as the Poly Trio 8800 system and that Poly Trio has screen mirroring enabled.

**AirPlay Debugging Log Parameters**

If you experience further issues using AirPlay-certified devices with the Poly Trio 8800 system, you can enable the following logging parameters on your Poly Trio to get extended debugging data.

```airp```
Session management and communication specifically for AirPlay certified devices.

**airpl**
Protocol library for AirPlay-certified devices

**airps**
Android service AirPlay-certified devices

**lc**
Local Content (including for AirPlay-certified devices and PPCIP) session management

### Screen Mirroring with Miracast-Certified Devices

The Wireless Display feature lets you display content wirelessly from your Miracast-certified Android or Windows device to a local monitor paired with a Poly Trio 8800 system.

Windows or Android devices can discover and connect directly with the Poly Trio 8800 system and don’t have to be on the same network. The Poly Trio 8800 system supports content sharing from the following Android and Windows devices:

- Miracast-certified devices running Windows 10
- Samsung Galaxy smartphones and tablets running Android version 4.4 or earlier

**Note:** Poly can’t guarantee connectivity with all Miracast-certified devices. Connectivity has been validated to work well with Samsung smartphones and tablets using Android version 4.4 or later and the Microsoft Surface® 3 Pro and Surface® 4 Pro running Windows 10.

### Requirements

You must meet the following requirements to use the Wireless Display feature on a Miracast-certified device with the Poly Trio 8800 system:

- Poly Trio 8800 collaboration kit running UC Software version 5.4.4AA or later

If you do not allow auto-negotiation, some devices might fail to pick the best possible video stream parameters.

### Limitations

The following is a list of limitations when using Wireless Display with Poly Trio and supported Miracast-devices:

- Some devices can't establish direct connection to Trio if they are already connected to 5GHz-only Wi-Fi Access Point. If experiencing this issue, disconnect the device from the Access Point while sharing content or by reconfiguring the Access Point to operate on 2.4GHz-only or 2.4Ghz + 5GHz bands.
- Wireless Display can't be used on a Poly Trio system configured for WLAN mode as the Poly Trio Visual+ does not support WLAN.
- The Poly Trio system can display content up to a maximum resolution and frame rate of 720 at 60fps or 1080 at 30fps. If the system is configured to auto-negotiate the frame rate of transmitted
content some tablets might send 1080p at 60fps video, which can cause multiple second latency in mirroring, visual artifacts, or both.

**Poly Trio 8800 for Miracast-Certified Devices Parameters**

Use the following parameters to configure Wireless Display on the Poly Trio 8800 system.

**content.wirelessDisplay.sink.authorizationType**

Auto (Default) - Content is automatically accepted and displays on the Poly Trio 8800 system.

Button - Users must confirm content acceptance on a popup message.

**content.wirelessDisplay.sink.bitrate**

Set the content maximum bitrate in Mbps

30 (default)

0 - 60

0 allows auto-negotiation.

**content.wirelessDisplay.sink.enabled**

0 (default) - Disable Wireless Display.

1 - Enable Wireless Display.

**content.wirelessDisplay.sink.fps**

Set the content frame rate in frames per second.

30 (default)

0 - 60

0 allows auto-negotiation

**content.wirelessDisplay.sink.height**

Set the maximum content height in pixels.

1080 (default)

0 - 1200

0 allows auto-negotiation

**content.wirelessDisplay.sink.name**

NULL - default

Specify a system name for the local content sink for Android or Windows devices. If left blank the previously configured or default system name is used.

**content.wirelessDisplay.sink.width**
Set the maximum content width in pixels.
1920 (Default and Maximum)
0 allows auto-negotiation

Troubleshooting
This section provides solutions to common issues you may have using Wireless Display on the Poly Trio 8800 system.

My Poly Trio 8800 system does not advertise on my smartphone or tablet
If the Poly Trio 8800 system does not advertise on your smartphone or tablet device, check the following:

- Ensure Wi-Fi is enabled on your device and the band is set to 2.4GHz or Auto. The Auto setting allows the connecting device better access to a free wireless channel.
- Ensure the correct country of operation is set and that both bands are selected on the Poly Trio 8800 system by configuring the following:

device.wifi.country.set="1"device.wifi.country="CA"device.wifi.radio.band2_4GHz.enable.set="1"
device.wifi.radio.band2_4GHz.enable="1"device.wifi.radio.band5GHz.enable.set="1"
device.wifi.radio.band5GHz.enable="1"device.wifi.enabled.set="1"
device.wifi.enabled="0"device.net.enabled.set="1"device.net.enabled="1"

Note: The WLAN operating mode on the Poly Trio 8800 system is mutually exclusive of the Wireless Display feature. You can enable Wireless Display only if wired Ethernet is used for calling and conferencing. Ensure that wired Ethernet is used for calling and conferencing.

Video Quality is Poor
Incorrect image resolution can cause content delays and video artifacts.

Note that the Poly Trio 8800 system does not accept 1080@60fps video resolution.

- To resolve video quality issues, configure the following for the Poly Trio 8800 system:

ccontent.wirelessDisplay.sink.width="0"content.wirelessDisplay.sink.height
="0"content.wirelessDisplay.sink.fps="0"

- In addition, you can set a limit on the live stream parameters by setting:

ccontent.wirelessDisplay.sink.fps="30"

Wireless Display Debugging Log Parameters
If you experience further issues using Wireless Display on the Poly Trio 8800 system, you can enable the following logging parameters on your Poly Trio 8800 system to get extended debugging data.

wdisp
  Wireless Display session management and communication with the Wireless Display source

apps
  Wireless Display support for Android

lc
Local Content (including Wireless Display and PPCIP) session management

Access Diagnostic Information

If you experience issues using Wireless Display on the Poly Trio 8800 system, you can access diagnostic information from the Poly Trio 8800 menu.

On the phone menu, go to one of the following settings:

- Settings > Status > Diagnostics > Local Content Media Statistics
- Settings > Status > Diagnostics > Graphs > Local Video Content Statistics
- Settings > Status > Diagnostics > Graphs > Networked Devices Graphs
- Settings > Status > Diagnostics > Networked Devices > Statistics
Hardware and Power for Poly Trio Systems

Topics:

- Powering Poly Trio Systems
- Poly Trio System Power Management
- Power-Saving on Poly Trio Systems

This section provides information on hardware and powering for the Poly Trio system and Poly Trio Visual + accessory, as well as information on power management.

Powering Poly Trio Systems

Powering requirements and options vary between Poly Trio models.

Read the powering requirements and options carefully to understand powering for your Poly Trio system. For more information, see the Setup Sheet for your Poly Trio system model at Poly Trio on Polycom Support.

Powering the Poly Trio 8800

You can power the Poly Trio 8800 system with Power over Ethernet (PoE) or PoE+ (IEEE 802.3at Type 2). When the Poly Trio 8800 system is booting up, an on-screen message indicates the available power supply type. Note that PoE+ provides Poly Trio systems with full functionality.

The following features are not available on Poly Trio 8800 system when using PoE:

- The Poly Trio 8800 system LAN OUT port out does not provide PoE+ power and cannot be used to power the Poly Trio Visual+.
- No USB charging is provided to devices (mobile phones, tablets) connected to the Poly Trio 8800 system USB port.
- Maximum peak power to the loudspeaker is limited.

Powering the Poly Trio 8500 System

You can power Poly Trio 8500 systems with Power over Ethernet (PoE).

Poly Trio 8500 systems do not support:

- PoE+
- Power Sourcing Equipment (PSE)
- LAN Out / PC Port
- USB charging
Power the Poly Trio 8800 System with the Optional Power Injector

If your building is not equipped with PoE+ you can use the optional power injector to provide PoE+ and full functionality to Poly Trio 8800 system.

**Note:** Place the PoE injector in a clean and dry area out of a walkway, and provide sufficient space around the unit for good ventilation. Do not cover or block airflow to the PoE injector. Keep the PoE injector away from heat and humidity and free from vibration and dust.

When using the power injector to power the Poly Trio 8800 system, you must connect cables in the following sequence:

**Procedure**

1. Plug the AC power cord of the power injector into the wall and use a network cable to connect the power injector to the Poly Trio 8800 system.
2. Connect the power injector to the network with a CAT-5E or CAT-6 Ethernet cable.

The power adapter LED is green when the Poly Trio 8800 system is correctly powered. If the LED is yellow, the power injector is bypassed and the Poly Trio 8800 system is drawing PoE power from the outlet.

**Tip:** If the Poly Trio Visual+ loses power after a Poly Trio 8800 system reboot, unplug both devices and repeat steps 1 and 2.

If the power injector LED is yellow, turn off the PoE network port or connect the Poly Trio system in the following sequence:

1. Power up Poly Trio 8800 and Visual+ using the power injector but do not plug the devices into the network wall port.
2. Wait for the Poly Trio 8800 and Visual+ systems to boot up.
3. Plug the devices into the network wall port.
4. Ensure the LED indicator on the power injector is green.

Powering the Poly Trio Visual+ Solution

How you power the Poly Trio Visual+ can depend on the power options your building is equipped with. Consider the following setup points:

- If you are using PoE+ or the optional power injector, you can power the Poly Trio Visual+ directly from the Poly Trio 8800 system using an Ethernet cable. In this scenario, you do not need to pair the Poly Trio system with the Poly Trio Visual+.
- If you are using PoE, you must power the Poly Trio Visual+ separately using an Ethernet cable or use the optional power injector. In this scenario, you must pair the Poly Trio system with the Poly Trio Visual+.
- If you use PoE+, you have the option to power the Poly Trio 8800 system and Poly Trio Visual+ separately and then pair. When powering separately, you do not need to connect the Poly Trio system directly to Poly Trio Visual+. 

Hardware and Power for Poly Trio Systems
Poly Trio System Power Management

Power available to Poly Trio systems is limited and you must choose how to power the system and which features to enable or disable.

Power management options vary between Poly Trio system models. Read the powering requirements and options carefully to understand powering for your Poly Trio system.

Poly Trio 8500 System Power Management

The Poly Trio 8500 system supports:

- USB devices consuming < 2.5W power
- USB port over current detection

Poly Trio 8500 systems do not support:

- PoE+
- Power Sourcing Equipment (PSE)
- LAN Out / PC Port
- USB charging

USB Port Power Management

Device charging with the USB port on the Poly Trio 8800 system is disabled by default and when disabled the USB host port provides 100mA of power for peripheral devices.

USB charging is disabled when powering the Poly Trio Visual+ from a LAN Out port.

To enable USB charging, you must power your Poly Trio 8800 system with an IEEE 802.3at Power over Ethernet Plus (PoE+) compliant power source. When USB charging is enabled, you can power and charge USB 2.0 compliant devices having a power draw of up to 1.500mA/7.5W.

Using Power over Ethernet (POE) Class 0

Powering the Poly Trio 8800 system from a Power over Ethernet (POE) Class 0 source provides full core functionality and results in the following limitations:

- The LAN Out port does not provide PoE power but otherwise is fully functional.

Using Power Sourcing Equipment Power (PoE PSE Power)

You can use Power Sourcing Equipment Power (PoE PSE Power) to power a Poly Trio Visual+ system from the LAN OUT port of the Poly Trio 8800 system.

To use PoE PSE Power, you must power the Poly Trio 8800 system with an IEEE 802.3at Power over Ethernet Plus (PoE+) compliant power source.

Note: You cannot enable USB Charging of the USB host port and PSE PoE Power of LAN OUT port at the same time. If both are enabled, the Poly Trio 8800 system uses PSE PoE Power and ignores the USB charging setting.
Poly Trio System Power Management Parameters
You can use the parameters listed to manage the Poly Trio system's power usage.

\texttt{poe.pse.class}
- Specify the LAN OUT PoE class.
  - 0 (default)
  - 0 - 3

\texttt{poe.pse.enabled}
- 1 (default) - The Poly Trio LAN OUT interface provides PoE power to a connected device.
  - 0 - PoE power is not provided by the LAN OUT port.

\texttt{usb.charging.enabled}
- 0 (default) - You cannot charge USB-connected devices from the USB charging port.
  - 1 - Enable fast charging of devices connected by USB port up to 7.5W power / 1.5A current.

Power-Saving on Poly Trio Systems
Power-saving automatically puts the phone into a lower-power state to conserve energy when not in use. When the phone is in power-saving, an LED light flashes at intervals. The phone returns to a full power state after detecting user movement, or after a button press, screen touch, or incoming call.

You can configure several power-saving options for Poly Trio systems including:
- Configure power-saving during work days.
- Turn on power-saving during nonworking days.
- Configure an idle inactivity time after which the phone enters power-saving.

\underline{Note:} Poly Trio systems cannot enter power-saving mode while idle in the Bluetooth menu. To ensure the phone can enter power-saving, do not leave the phone idle in the Bluetooth menu.

Power-Saving Parameters
Use the following parameters to configure the power-saving features and feature options.

\texttt{powerSaving.cecEnable}
- 0 (default) - The paired device display behavior is controlled only by the value set for \texttt{powerSaving.tvStandbyMode}.
  - 1 - When the Poly Trio system enters power-saving mode, the paired device display switches to standby mode and powers up when the system exits power-saving mode.
**powerSaving.cecEnable**

1 (default) - Enable the LCD power-saving feature.
0 - Disable The LCD power-saving feature.

Note that when the phone is in power-saving mode, the LED Message Waiting Indicator (MWI) flashes. To disable the MWI LED when the phone is in power saving mode, set the parameter `ind.pattern.powerSaving.step.1.state.x` to 0 where x=your phone's model.

**powerSaving.idleTimeout.offHours**

The number of idle minutes during off hours after which the phone enters power saving.

1 (default)
1 - 10

**powerSaving.idleTimeout.officeHours**

The number of idle minutes during office hours after which the phone enters power saving.

30 (default)
1 - 600

**powerSaving.idleTimeout.userInputExtension**

The number of minutes after the phone is last used after which the phone enters power saving.

10 (default)
1 - 20

**powerSaving.officeHours.duration.x**

Append the day of the week for "x". For example, `powerSaving.officeHours.duration.Monday`.

Set the duration of the office working hours by week day.

Monday - Friday = 12 (default)
Saturday - Sunday = 0
0 - 24

**powerSaving.officeHours.startHour.x**

Specify the starting hour for the day's office working hours.

7 (default)
0 - 23

Set x to Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday (refer to `powerSaving.officeHours.duration` for an example).
**powerSaving.tvStandbyMode**

black (default) - The paired device displays a black screen after entering power-saving mode.

noSignal - Power-saving mode turns off the HDMI signal going to the paired device monitor(s).
Audio Features

Topics:

- Automatic Gain Control
- Background Noise Suppression
- Comfort Noise
- Voice Activity Detection
- Comfort Noise Payload Packets
- Synthesized Call Progress Tones
- Jitter Buffer and Packet Error Concealment
- Dual-Tone Multi-Frequency Tones
- Acoustic Echo Cancellation
- Polycom NoiseBlock
- Audio Output Options
- Audio Input Options
- USB Audio Calls
- Location of Audio Alerts
- Ringtones
- Sound Effects
- Supported Audio Codecs for Poly Trio Solution
- IEEE 802.1p/Q
- Voice Quality Monitoring (VQMon)

After you set up your phones on the network, users can send and receive calls using the default configuration. However, you might consider configuring modifications that optimize the audio quality of your network. This section describes the audio sound quality features and options you can configure for your phones. Use these features and options to optimize the conditions of your organization’s phone network system.

**Automatic Gain Control**

Automatic Gain Control (AGC) is available for conference phone models and is used to boost the gain of the near-end conference participant.

Gain control helps conference participants hear your voice. This feature is enabled by default.
Background Noise Suppression
Background noise suppression is designed primarily for hands-free operation and reduces background noise, such as from fans, projectors, or air conditioners, to enhance communication. This feature is enabled by default.

Comfort Noise
Comfort Noise ensures a consistent background noise level to provide a natural call experience and is enabled by default. Comfort noise fill is unrelated to Comfort Noise packets generated if Voice Activity Detection is enabled.

Voice Activity Detection
Voice activity detection (VAD) conserves network bandwidth by detecting periods of silence in the transmit data path so the phone doesn't have to 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 comfort noise transmission processing specified in RFC 3389. The RFC 3389 algorithm is derived from G.711 Appendix II, which defines a comfort noise (CN) payload format (or bit stream) for G.711 use in packet-based, multimedia communication systems.

Voice Activity Detection Parameters
The following list includes the parameters you can use to configure Voice Activity Detection.

**voice.vad.signalAnnexB**

0 – There is no change to SDP. If `voice.vadEnable` is set to 0, add parameter line `a=fmtp:18 annexb="no"` below the `a=rtpmap ...` parameter line (where "18" could be replaced by another payload).

1 (default) – Annex B is used and a new line is added to SDP depending on the setting of `voice.vadEnable`. If `voice.vadEnable` is set to 1, add parameter line `a=fmtp:18 annexb="yes"` below `a=rtpmap ...` parameter line (where "18" could be replaced by another payload).

**voice.vadEnable**

0 - Disable Voice activity detection (VAD).

1 - Enable VAD.

**voice.vadThresh**

The threshold for determining what is active voice and what is background noise in dB. Sounds louder than this set value are considered active voice, and sounds quieter than this threshold
are considered background noise. This does not apply to G.729AB codec operation which has its own built-in VAD function.

25 (default)
Integer from 0 - 30

Comfort Noise Payload Packets
When enabled, the Comfort Noise payload type is negotiated in Session Description Protocol (SDP) with the default of 13 for 8 KHz codecs, and a configurable value between 96 and 127 for 16 KHz codecs.

Comfort Noise Payload Packets Parameters
The following list includes the parameters you can use to configure Comfort Noise payload packets.

voice.CNControl
Publishes support for Comfort Noise in the SDP body of the INVITE message and includes the supported comfort noise payloads in the media line for audio.

1 (default) – Either the payload type 13 for 8 KHz sample rate audio codec is sent for Comfort Noise, or the dynamic payload type for 16 KHz audio codecs are sent in the SDP body.

0 – Does not publish support or payloads for Comfort Noise.

voice.CN16KPayload
Alters the dynamic payload type used for Comfort Noise RTP packets for 16 KHz codecs.

96 to 127
122 (default)

Synthesized Call Progress Tones
Polycom phones play call signals and alerts, called call progress tones, that include busy signals, ringback sounds, and call waiting tones.

The built-in call progress tones match standard North American tones. If you want to customize the phone's call progress tones to match the standard tones in your region, contact Polycom Support.

Jitter Buffer and Packet Error Concealment
The phone employs a high-performance jitter buffer and packet error concealment system designed to mitigate packet inter-arrival jitter and out-of-order, or lost or delayed (by the network) packets.

The jitter buffer is adaptive and configurable for different network environments. When packets are lost, a concealment algorithm minimizes the resulting negative audio consequences. This feature is enabled by default.
Dual-Tone Multi-Frequency Tones

The phone generates dual-tone multi-frequency (DTMF) tones, also called touch tones, in response to user dialing on the dialpad.

These tones are transmitted in the real-time transport protocol (RTP) streams of connected calls.

The phone can encode the DTMF tones using the active voice codec or using RFC 2833-compatible encoding. The coding format decision is based on the capabilities of the remote endpoint. The phone generates RFC 2833 (DTMF only) events but does not regenerate—or otherwise use—DTMF events received from the remote end of the call.

DTMF Tone Parameters

The following list includes the parameters you can use to set up DTMF tones.

**reg.1.telephony**

Allow telephony services for inbound and outbound calls.

1 (default) – Allowed
0 – Disallowed

**tone.dtmf.chassis.masking**

0 (default) - DTMF tones play through the speakerphone in handsfree mode.

1 - Set to 1 only if `tone.dtmf.viaRtp` is set to 0. DTMF tones are substituted with non-DTMF pacifier tones when dialing in handsfree mode to prevent tones from broadcasting to surrounding telephony devices or inadvertently transmitted in-band due to local acoustic echo.

Change causes system to restart or reboot.

**tone.dtmf.level**

The level of the high frequency component of the DTMF digit measured in dBm0; the low frequency tone is two dB lower.

-15
-33 to 3

Change causes system to restart or reboot.

**tone.dtmf.offTime**

When a sequence of DTMF tones is played out automatically, specify the length of time in milliseconds (ms) the phone pauses between digits. This is also the minimum inter-digit time when dialing manually.

50 (default)
1 – Indefinite

Change causes system to restart or reboot.
**tone.dtmf.onTime**

Set the time in milliseconds (ms) DTMF tones play on the network when DTMF tones play automatically. The time you set is also the minimum time the tone plays when manually dialing.

50 (default)
1 - 65535

Change causes system to restart or reboot.

**tone.dtmf.rfc2833Control**

Specify if the phone uses RFC 2833 to encode DTMF tones.

1 (default) - The phone indicates a preference for encoding DTMF through RFC2833 format in its Session Description Protocol (SDP) offers by showing support for the phone-event payload type. This doesn't affect SDP answers and always honor the DTMF format present in the offer.

0 - The phone doesn't offer dynamic payload for RFC2833 phone-event.

Change causes system to restart or reboot.

**tone.dtmf.rfc2833Payload**

Specify the phone-event payload encoding in the dynamic range to be used in SDP offers.

Skype (default) - 101
Generic (default) -127
96 to 127

Change causes system to restart or reboot.

**tone.dtmf.rfc2833Payload_OPUS**

Sets the DTMF payload required to use Opus codec.

126 (default)
96 - 127

Change causes system to restart or reboot.

**tone.dtmf.viaRtp**

1 (default) - Encode DTMF in the active RTP stream. Otherwise, DTMF may be encoded within the signaling protocol only when the protocol offers the option.

0 – If you set this parameter to 0, you must set tone.dtmf.chassis.masking to 1.

Change causes system to restart or reboot.

**tone.localDtmf.onTime**

Set the time in milliseconds (ms) DTMF tones play for when the phone plays out a DTML tone sequence automatically.
tone.dtmf.rfc2833.SupportOpusClockRate
1 – (default) Publishes the Telephone-event DTMF frequency as 48000 Hz along with 8000 Hz on Opus codec.
0 - Publishes the Telephone-event DTMF frequency as 8000 Hz on Opus codec.

Acoustic Echo Cancellation
Configure your phones to use advanced acoustic echo cancellation (AEC) for handsfree operation using the speakerphone.
The phones significantly reduce echo while permitting natural communication.
The AEC feature includes the following:
• 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.
• Non-linear Processing: Suppresses any echo remaining after the Linear Adaptive Filter.
The phones also support headset echo cancellation.

Acoustic Echo Cancellation Parameters
The following list includes the parameters you can use to set up Acoustic Echo Cancellation (AEC).

voice.aec.hf.enable
1 (default)—Enables the AEC function for handsfree options.
0—Disables the AEC function for handsfree options.
Polycom does not recommend disabling this parameter.

voice.aec.hs.enable
0—Disables the AEC function for the handset.
1 (default)—Enables the AEC function for the handset.

Polycom NoiseBlock
Polycom NoiseBlock technology automatically mutes the microphone during audio-only and audio/video calls when a user stops speaking.
This feature silences noises that interrupt conversations such as paper shuffling, food wrappers, and keyboard typing. When a user speaks, the microphone is automatically unmuted.
NoiseBlock Parameters
Use the following parameters to configure NoiseBlock.

voice.ns.hf.block
1 (default) - Enables NoiseBlock.
0 - Disables NoiseBlock.

Audio Output Options
By default, audio plays out of the Poly Trio speakers.
When paired with a Poly Trio Visual+ or Trio VisualPro system, you can play audio out of the connected
the monitor(s) and external speakers.
Using the parameter up.audio.networkedDevicePlayout, you can configure the following audio
output options:
• Poly Trio system speakers only
• Poly Trio Visual+ using HDMI or a connected 3.5mm analog output
• Trio VisualPro system using HDMI

Audio Output Options Parameters
The following table includes the parameters you can use to set the audio routing options for the Poly Trio
solution.

up.audio.networkedDevicePlayout
PhoneOnly (default) - Use the Poly Trio system speakers.
TvOnly - Use the monitor speakers and external speakers (if present).
Auto - Audio-only calls use the Poly Trio system speakers. Video calls use the monitor speakers
and external speakers (if present).

feature.usb.device.hostOs
Specify the operating system of the computer you are connecting by USB when using Poly Trio
as an audio output device.
Windows (default) - The computer connected by USB to the Poly Trio uses a Windows operating
system.
Other—The operating system of the computer connected via USB to the Poly Trio system is
other than Windows or Mac.
Mac—The computer connected by USB to the Poly Trio uses a Mac operating system.
Confirm—The user is prompted to confirm the computer's operating system each time a USB
cable is used to connect to the Poly Trio system.
Audio Input Options

Your Poly Trio system can use the following microphones in addition to its own:

- Poly Trio™ Expansion Microphones
  The expansion microphones include a 2.1 m | 7 ft cable that you can attach directly to the Poly Trio to broaden its audio range to a total of 70 ft.
- Polycom® Microphone Array and/or Polycom® Ceiling Microphone Array (when connected to a Trio VisualPro system)

USB Audio Calls

You can enable Poly Trio systems as an audio device for a tablet or laptop when connected to the Poly Trio system with the USB cable supplied in the box.

When a Microsoft® Windows® computer is connected to the Poly Trio solution using a USB cable, users can control the volume of audio and video calls from the computer or the Poly Trio solution, and the volume is synchronized on both devices.

Poly Trio systems supports Mac computers running the following software versions when connected by USB and used as an audio speakerphone:

- OS X 10.9.x (Mavericks)
- OS X 10.10.x (Yosemite)
- OS X 10.11.x (El Capitan)

USB Audio Call Parameters

The following table includes the parameters you can use to configure USB audio calls for connected devices.

**feature.usb.device.audio**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables the ability to use Trio as a USB speakerphone.</td>
</tr>
<tr>
<td>1 (default)</td>
<td>Enables the ability to use Poly Trio as a USB speakerphone.</td>
</tr>
</tbody>
</table>

Requires restart

**device.baseProfile**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL (default)</td>
<td>Generic - Disables the Skype for Business graphic interface.</td>
</tr>
<tr>
<td></td>
<td>Lync - Use this Base Profile for Skype for Business deployments.</td>
</tr>
<tr>
<td></td>
<td>SkypeUSB - Use this Base Profile when you want to connect Poly Trio to a Microsoft Room System or a Microsoft Surface Hub.</td>
</tr>
</tbody>
</table>

**voice.usb.holdResume.enable**

<table>
<thead>
<tr>
<th>Value (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The Hold and Resume buttons do not display during USB calls.</td>
</tr>
</tbody>
</table>
1 - The Hold and Resume buttons display during USB calls.
This parameter applies only when Poly Trio Base Profile is set to SkypeUSB.

**Location of Audio Alerts**

You can choose where all audio alerts, including incoming call alerts, are played on Polycom phones.
You can specify the audio to play from the hands-free speakerphone (default), the handset, the headset, or the active location. If you choose the active location, audio alerts play out through the handset or headset if they are in use. Otherwise, alerts play through the speakerphone.

**Audio Alert Parameters**

Use the parameters in the following list to configure audio alerts and sound effects.

**se.appLocalEnabled**

Enables or disables audio alerts and sound effects.
1 (default) – Enabled
0 – Disabled
Change causes system to restart or reboot.

**se.destination**

chassis (default) – Alerts and sound effects play through the phone’s speakerphone.
headset – If connected, alerts and sounds play through the headset.
handset active – Alerts play from the destination that is currently in use. For example, if a user is in a call on the handset, a new incoming call rings through the handset.

**se.stutterOnVoiceMail**

1 (default) – A stuttered dial tone is used instead of a normal dial tone to indicate that one or more voicemail messages are waiting at the message center.
0 – A normal tone is used to indicate that one or more voicemail messages are waiting at the message center.

**Ringtones**

Ringtones are used to define a simple ring class that is applied based on credentials carried within the network protocol.
The ring class includes parameters such as call-waiting and ringer index, if appropriate.
The ring class can use one of the following types of rings:
- Ring - Plays a specified ring pattern or call waiting indication.
• Visual - Provides a visual indication (no audio) of an incoming call, no ringer needs to be specified.
• Answer - Provides auto-answer on an incoming call.
• Ring-answer - Provides auto-answer on an incoming call after a certain number of rings.

**Note:** Auto-answer for an incoming call works only when there is no other call in progress on the phone, including no other calls in progress on shared or monitored lines. However, if a phone initiates a call on a shared or monitored line, auto-answer works.

---

**Supported Ring Classes**

The phone supports the following ring classes:

- default
- visual
- answerMute
- autoAnswer
- ringAnswerMute
- ringAutoAnswer
- internal
- external
- emergency
- precedence
- splash
- custom<y> where y is 1 to 17.

**Ringtone Parameters**

The following parameters configure ringtones.

**se.rt.enabled**

Enables or disables ringtone feature.

- 0 – Disabled
- 1 (default) – Enabled

**se.rt.modification.enabled**

Controls whether or not users are allowed to modify the predefined ringtone from the phone's user interface.

- 0 – Users not allowed.
- 1 (default) – Users allowed.

**se.rt.<ringClass>.callWait**
The call waiting tone used for the specified ring class. The call waiting pattern should match the pattern defined in Call Progress Tones.

callWaiting (default)
callWaitingLong
precedenceCallWaiting

```
se.rt.<ringClass>.name
```

The answer mode for a ringtone, which is used for to identify the ringtone in the user interface.

UTF-8 encoded string

```
se.rt.<ringClass>.ringer
```

The ringtone used for this ring class. The ringer must match one listed in Ringtones.

default
ringer1 to ringer24
ringer2 (default)

```
se.rt.<ringClass>.timeout
```

The duration of the ring in milliseconds before the call is auto answered, which only applies if the type is set to ring-answer.

1 to 60000
2000 (default)

```
se.rt.<ringClass>.type
```

The answer mode for a ringtone.

ring
visual
answer
ring-answer

---

**Sound Effects**

The phone uses built-in sampled audio files (SAF) in wave file format for some sound effects.

You can customize the audio sound effects that play for incoming calls and other alerts using synthesized tones or sampled audio files with .wav files you download from the provisioning server or Internet.

Ringtone files are stored in volatile memory which allows a maximum size of 600 kilobytes (614400 bytes) for all ringtones.
## Sampled Audio Files

The phone uses built-in sampled audio files (SAF) in wave file format for some sound effects.

You can add files downloaded from the provisioning server or from the Internet. Ringtone files are stored in volatile memory, which allows a maximum size of 600 kilobytes (614400 bytes) for all ringtones.

The phones support the following sampled audio WAVE (.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

### Default Sample Audio Files

The following table defines the phone's default use of the sampled audio files.

<table>
<thead>
<tr>
<th>Sampled Audio File Number</th>
<th>Default Use (Pattern Reference)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ringer 12 (<a href="#">se.pat.misc.welcome</a>)&lt;br&gt;Ringer 15 (<a href="#">se.pat.ringer.ringer15</a>)</td>
</tr>
<tr>
<td>2</td>
<td>Ringer 16 (<a href="#">se.pat.ringer.ringer16</a>)</td>
</tr>
<tr>
<td>3</td>
<td>Ringer 17 (<a href="#">se.pat.ringer.ringer17</a>)</td>
</tr>
<tr>
<td>4</td>
<td>Ringer 18 (<a href="#">se.pat.ringer.ringer18</a>)</td>
</tr>
<tr>
<td>5</td>
<td>Ringer 19 (<a href="#">se.pat.ringer.ringer19</a>)</td>
</tr>
<tr>
<td>6</td>
<td>Ringer 20 (<a href="#">se.pat.ringer.ringer20</a>)</td>
</tr>
<tr>
<td>7</td>
<td>Ringer 21 (<a href="#">se.pat.ringer.ringer21</a>)</td>
</tr>
<tr>
<td>8</td>
<td>Ringer 22 (<a href="#">se.pat.ringer.ringer22</a>)</td>
</tr>
<tr>
<td>9</td>
<td>Ringer 23 (<a href="#">se.pat.ringer.ringer23</a>)</td>
</tr>
<tr>
<td>10</td>
<td>Ringer 24 (<a href="#">se.pat.ringer.ringer24</a>)</td>
</tr>
<tr>
<td>11 to 24</td>
<td>Not Used</td>
</tr>
</tbody>
</table>
**Sampled Audio File Parameter**

Your custom sampled audio files must be available at the path or URL specified in the parameter `saf.x` so the phone can download the files. Make sure to include the name of the file and the `.wav` extension in the path.

*saf.x*

Specify a path or URL for the phone to download a custom audio file (x).

To use a welcome sound, enable the parameter `up.welcomeSoundEnabled` and specify a file in `saf.x`. The default UC Software welcome sound file is `Welcome.wav`.

Null (default) – The phone uses a built-in file.

Path Name – During startup, the phone attempts to download the file at the specified path in the provisioning server.

URL – During startup, the phone attempts to download the file from the specified URL on the Internet. Must be a RFC 1738-compliant URL to an HTTP, FTP, or TFTP wave file resource.

Note: If using TFTP, the URL must be in the following format: `tftp://<host>/[pathname]<filename>` . For example: `tftp://somehost.example.com/sounds/example.wav`.

**Sound Effect Patterns**

You can specify the sound effects that play for different phone functions and specify the sound effect patterns and the category.

Sound effects are defined by patterns: sequences of chord-sets, silence periods, and wave files. You can also configure sound effect patterns and ringtones. The phones use both synthesized and sampled audio sound effects.

Patterns use a simple script language that allows different chord sets or wave files to be strung together with periods of silence. The script language uses the instructions shown in the next table.

**Sound Effects Pattern Types**

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
</table>
| `sampled(n)` | Play sampled audio file n | `se.pat.misc.SAMPLED_1.inst.1.type ="sampled" (sampled audio file instruction type)`  
<p>|              |                       | <code>se.pat.misc.SAMPLED_1.inst.1.value =&quot;2&quot; (specifies sampled audio file 2)</code> |</p>
<table>
<thead>
<tr>
<th>Instruction</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
</table>
| chord (n, d)  | Play chord set n (d is optional and allows the chord set ON duration to | se.pat.callProg.busyTone.inst.
|               | be overridden to d milliseconds)                                        | 2.type = “chord” (chord set instruction type)                         |
|               |                                                                         | se.pat.callProg.busyTone.inst.
|               |                                                                         | 2.value = “busyTone” (specifies sampled audio file busyTone)           |
|               |                                                                         | se.pat.callProg.busyTone.inst.
|               |                                                                         | 2.param = “2000” (override ON duration of chord set to 2000 milliseconds) |
| silence (d)   | Play silence for d milliseconds (Rx audio is not muted)                 | se.pat.callProg.bargeIn.inst.
|               |                                                                         | 3.type = “silence” (silence instruction type)                          |
|               |                                                                         | se.pat.callProg.bargeIn.inst.
|               |                                                                         | 3.value = “300” (specifies silence is to last 300 milliseconds)         |
| branch (n)    | Advance n instructions and execute that instruction (n must be negative | se.pat.callProg.alerting.inst.
|               | and must not branch beyond the first instruction)                      | 4.type = “branch” (branch instruction type)                            |
|               |                                                                         | se.pat.callProg.alerting.inst.
|               |                                                                         | 4.value = “-2” (step back 2 instructions and execute that instruction) |
| csx           | Plays the tone based on the values set for Frequency, Level, OnDuration, | se.pat.misc.callParkBLFAudioNotification.inst.x.value (specify the file to play the audio tone.) |
|               | OffDuration and Repeat time. There is a pre-defined value for each     |                                                                       |
|               | chord-set (cs). x = 1 to 12                                             |                                                                       |

**Sound Effect Pattern Parameters**

There are three categories of sound effect patterns that you can use to replace cat in the parameter names: callProg (Call Progress Patterns), ringer (Ringer Patterns) and misc (Miscellaneous Patterns).

Keep the following in mind when using the parameters:

- X is the pattern name.
- Y is the instruction number.
- Both x and y need to be sequential.
- Cat is the sound effect pattern category.

**se.pat.callProg.secondaryDialTone.name**

1-255
se.pat.callProg.secondaryDialTone.inst.1.type
0-255

se.pat.callProg.secondaryDialTone.inst.1.value
0-50

se.pat.callProg.secondaryDialTone.inst.1.atte
Sound effects name, where cat is `callProg`, `ringer`, or `misc`. UTF-8 encoded string

se.pat.cat.x.inst.y.type
Sound effects name, where cat is `callProg`, `ringer`, or `misc`.
sample
cord
silence
branch

se.pat.cat.x.inst.y.value
sampled – Sampled audio file number
cord – Type of sound effect
silence – Silence duration in milliseconds
branch – Number of instructions to advance
String

se.pat.callProg.stutter.inst.1.type
chord (1-2) (default) - Type of sound effect
NULL (3-8) (default)
sampled - Sampled audio file number
silence - Silence duration in milliseconds
branch - Number of instructions to advance

se.pat.callProg.stutter.inst.1.value
stutterLong (1) (default)
dialTone (2) (default)
NULL (3-8) (default)
se.pat.misc.callParkBLFAudioNotification.inst.x.type
   Specify the sound effect type to play the audio tone.
   Null (default)
   chord

se.pat.misc.callParkBLFAudioNotification.inst.x.value
   Specify the file to play the audio tone.
   Null (default)
   cs7
   cs4

se.pat.misc.callParkBLFAudioNotification.inst.x.param
   Specify the duration for how long the tone should play.
   0 (default)
   5000 ms

se.pat.misc.callParkBLFAudioNotification.inst.x.atten
   Specify the tone attenuation.
   0 (default)
   -1000 Hz
   5000 Hz

se.pat.misc.callParkBLFReminderTone.inst.x.type
   Specify the sound effect type to play the audio tone.
   Null (default)
   chord

se.pat.misc.callParkBLFReminderTone.inst.x.value
   Specify the file to play the audio tone.
   Null (default)
   cs3
   cs4
   cs6

se.pat.misc.callParkBLFReminderTone.inst.x.param
   Specify the duration for how long the tone should play.
0 (default)
5000 ms

Specify the tone attenuation.
0 (default)
-1000 Hz
5000 Hz

Call Progress Tones
The following table lists the call progress pattern names and their descriptions.

<table>
<thead>
<tr>
<th>Call Progress Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alerting</td>
<td>Alerting</td>
</tr>
<tr>
<td>bargeln</td>
<td>Barge-in tone</td>
</tr>
<tr>
<td>busyTone</td>
<td>Busy tone</td>
</tr>
<tr>
<td>callWaiting</td>
<td>Call waiting tone</td>
</tr>
<tr>
<td>callWaitingLong</td>
<td>Call waiting tone long (distinctive)</td>
</tr>
<tr>
<td>confirmation</td>
<td>Confirmation tone</td>
</tr>
<tr>
<td>dialTone</td>
<td>Dial tone</td>
</tr>
<tr>
<td>howler</td>
<td>Howler tone (off-hook warning)</td>
</tr>
<tr>
<td>intercom</td>
<td>Intercom announcement tone</td>
</tr>
<tr>
<td>msgWaiting</td>
<td>Message waiting tone</td>
</tr>
<tr>
<td>precedenceCallWaiting</td>
<td>Precedence call waiting tone</td>
</tr>
<tr>
<td>precedenceRingback</td>
<td>Precedence ringback tone</td>
</tr>
<tr>
<td>preemption</td>
<td>Preemption tone</td>
</tr>
<tr>
<td>precedence</td>
<td>Precedence tone</td>
</tr>
<tr>
<td>recWarning</td>
<td>Record warning</td>
</tr>
<tr>
<td>reorder</td>
<td>Reorder tone</td>
</tr>
</tbody>
</table>
Call Progress Pattern | Description
--- | ---
ringback | Ringback tone
secondaryDialTone | Secondary dial tone
stutter | Stuttered dial tone

**Miscellaneous Patterns**
The following table lists the miscellaneous patterns and their descriptions.

**Miscellaneous Pattern Names**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Miscellaneous Pattern Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instantmessage</td>
<td>instant message</td>
<td>New instant message</td>
</tr>
<tr>
<td>localHoldNotification</td>
<td>local hold notification</td>
<td>Local hold notification</td>
</tr>
<tr>
<td>messageWaiting</td>
<td>message waiting</td>
<td>New message waiting indication</td>
</tr>
<tr>
<td>negativeConfirm</td>
<td>negative confirmation</td>
<td>Negative confirmation</td>
</tr>
<tr>
<td>positiveConfirm</td>
<td>positive confirmation</td>
<td>Positive confirmation</td>
</tr>
<tr>
<td>remoteHoldNotification</td>
<td>remote hold notification</td>
<td>Remote hold notification</td>
</tr>
<tr>
<td>welcome</td>
<td>welcome</td>
<td>Welcome (boot up)</td>
</tr>
<tr>
<td>callParkBLFReminderTone</td>
<td>call Park BLF Reminder Tone</td>
<td>Cadence of call park reminder tone</td>
</tr>
<tr>
<td>callParkBLFAudioNotification</td>
<td>call Park BLF Audio Notification</td>
<td>Cadence of call park audio notification</td>
</tr>
</tbody>
</table>

**Supported Audio Codecs for Poly Trio Solution**
The following table includes the supported audio codecs and priorities for the Poly Trio systems.

Note that the Opus codec is not compatible with G.729 and iLBC. If you set Opus to the highest priority, G.729 and iLBC are not published; if you set G.729 and iLBC to the highest priority, Opus is not published.

**Audio Codec Priority**

<table>
<thead>
<tr>
<th>Device Support</th>
<th>Supported Audio Codecs</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio systems</td>
<td>G.711 µ-law</td>
<td>6</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.711a-law</td>
<td>7</td>
</tr>
</tbody>
</table>
## Poly Trio Supported Audio Codec Specifications

The following table summarizes the specifications for audio codecs supported on Poly Trio systems.

### Audio Attributes

<table>
<thead>
<tr>
<th>Device Support</th>
<th>Algorithm</th>
<th>Reference</th>
<th>Raw Bit Rate</th>
<th>Maximum IP Bit Rate</th>
<th>Sample Rate</th>
<th>Default Payload Size</th>
<th>Effective Audio Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio systems</td>
<td>G.711 µ-law</td>
<td>RFC 1890</td>
<td>64 Kbps</td>
<td>80 Kbps</td>
<td>8 Kbps</td>
<td>20 ms</td>
<td>3.5 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.711 a-law</td>
<td>RFC 1890</td>
<td>64 Kbps</td>
<td>80 Kbps</td>
<td>8 Kbps</td>
<td>20 ms</td>
<td>3.5 KHz</td>
</tr>
<tr>
<td>Poly Trio 8800</td>
<td>G.719</td>
<td>RFC 5404</td>
<td>32 Kbps</td>
<td>48 Kbps</td>
<td>48 Kbps</td>
<td>20 ms</td>
<td>20 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.711</td>
<td>RFC 1890</td>
<td>64 Kbps</td>
<td>80 Kbps</td>
<td>16 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.722¹</td>
<td>RFC 3551</td>
<td>64 Kbps</td>
<td>80 Kbps</td>
<td>16 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
</tr>
</tbody>
</table>

### Note:

The network bandwidth necessary to send encoded voice is typically 5-10% higher than the encoded bit rate due to packetization overhead. For example, a G.722.1C call at 48kbps for both the receive and transmit signals consumes about 100kbps of network bandwidth (two-way audio).
<table>
<thead>
<tr>
<th>Device Support</th>
<th>Algorithm</th>
<th>Reference</th>
<th>Raw Bit Rate</th>
<th>Maximum IP Bit Rate</th>
<th>Sample Rate</th>
<th>Default Payload Size</th>
<th>Effective Audio Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio systems</td>
<td>G.722.1</td>
<td>RFC 3047</td>
<td>24 Kbps</td>
<td>40 Kbps</td>
<td>16 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.722.1C</td>
<td>G7221C</td>
<td>224 Kbps</td>
<td>40 Kbps</td>
<td>32 Kbps</td>
<td>20 ms</td>
<td>14 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>G.729AB</td>
<td>RFC 1890</td>
<td>8 Kbps</td>
<td>24 Kbps</td>
<td>8 Kbps</td>
<td>20 ms</td>
<td>3.5 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Opus</td>
<td>RFC 6716</td>
<td>8 - 24 Kbps</td>
<td>24 - 40 Kbps</td>
<td>8 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Lin16</td>
<td>RFC 1890</td>
<td>128 Kbps</td>
<td>132 Kbps</td>
<td>8 Kbps</td>
<td>10 ms</td>
<td>3.5 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Lin16</td>
<td>RFC 1890</td>
<td>256 Kbps</td>
<td>260 Kbps</td>
<td>16 Kbps</td>
<td>20 ms</td>
<td>3.5 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Lin16</td>
<td>RFC 1890</td>
<td>512 Kbps</td>
<td>516 Kbps</td>
<td>32 Kbps</td>
<td>20 ms</td>
<td>14 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Lin16</td>
<td>RFC 1890</td>
<td>705.6 Kbps</td>
<td>709.6 Kbps</td>
<td>44.1 Kbps</td>
<td>20 ms</td>
<td>14 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Lin16</td>
<td>RFC 1890</td>
<td>768 Kbps</td>
<td>772 Kbps</td>
<td>48 Kbps</td>
<td>20 ms</td>
<td>22 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren 7</td>
<td>SIREN7</td>
<td>16 Kbps</td>
<td>32 Kbps</td>
<td>16 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren 7</td>
<td>SIREN7</td>
<td>24 Kbps</td>
<td>40 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren 7</td>
<td>SIREN7</td>
<td>32 Kbps</td>
<td>48 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren 7</td>
<td>SIREN7</td>
<td>48 Kbps</td>
<td>64 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren14</td>
<td>SIREN14</td>
<td>24 Kbps</td>
<td>40 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren14</td>
<td>SIREN14</td>
<td>32 Kbps</td>
<td>48 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren14</td>
<td>SIREN14</td>
<td>48 Kbps</td>
<td>64 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren22</td>
<td>SIREN22</td>
<td>32 Kbps</td>
<td>48 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren22</td>
<td>SIREN22</td>
<td>48 Kbps</td>
<td>64 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>Siren22</td>
<td>SIREN22</td>
<td>64 Kbps</td>
<td>80 Kbps</td>
<td>20 ms</td>
<td>7 KHz</td>
<td></td>
</tr>
<tr>
<td>Poly Trio systems</td>
<td>iLBC</td>
<td>RFC 3951</td>
<td>13.33 Kbps</td>
<td>31.2 Kbps</td>
<td>8 Kbps</td>
<td>30 ms</td>
<td>3.5 KHz</td>
</tr>
</tbody>
</table>

*Note: *Trio 8500 supports 3.5, 7, and 14 KHz and not 20 or 22 KHz*
**Audio Codec Parameters**

You can configure a set of codec properties to improve consistency and reduce workload on the phones. Use the following parameters to specify audio codec priority on your phones.

- Permitted values to set audio codec priority are 1 - 27
- A value of 1 is the highest priority, 27 the lowest.
- If 0 or Null, the codec is disabled.
- A change to the default value does not cause a phone to restart or reboot

If a phone does not support a codec, the phone treats the value as 0, does not offer or accept calls using that codec, and continues to the codec next in priority.

**Audio Codec Priority Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Priority Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.codecPref.G711_A</td>
<td>7</td>
</tr>
<tr>
<td>voice.codecPref.G711_Mu</td>
<td>6</td>
</tr>
<tr>
<td>voice.codecPref.G719.32kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.G719.48kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.G719.64kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.G722</td>
<td>4</td>
</tr>
<tr>
<td>voice.codecPref.G7221.24kbps</td>
<td>0</td>
</tr>
</tbody>
</table>

1 Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16ksps), 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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Priority Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.codecPref.G7221_C.24kbps</td>
<td>5</td>
</tr>
<tr>
<td>voice.codecPref.G7221.32kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.G7221_C.48kbps</td>
<td>2</td>
</tr>
<tr>
<td>voice.codecPref.G729_AB</td>
<td>8</td>
</tr>
<tr>
<td>voice.codecPref.iLBC.13_33kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.iLBC.15_2kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Lin16.8ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Lin16.16ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Lin16.32ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Lin16.44_1ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Lin16.48ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren7.16kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren7.24kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren7.32kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren14.24kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren14.32kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren14.48kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren22.32kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren22.48kbps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.Siren22.64kbps</td>
<td>1</td>
</tr>
<tr>
<td>voice.codecPref.SILK.8ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.SILK.12ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.SILK.16ksps</td>
<td>0</td>
</tr>
<tr>
<td>voice.codecPref.SILK.24kbps</td>
<td>0</td>
</tr>
</tbody>
</table>
SILK Audio Codec

Poly recommends disabling the SILK codec due to performance constraints when video is enabled.

Use the following parameters to configure the SILK audio codec.

**voice.codecPref.SILK.8ksps**
Set the SILK audio codec preference for the supported codec sample rates.
0 (default)

**voice.codecPref.SILK.12ksps**
Set the SILK audio codec preference for the supported codec sample rates.

**voice.codecPref.SILK.16ksps**
Set the SILK audio codec preference for the supported codec sample rates.
0 (default)

**voice.codecPref.SILK.24ksps**
Set the SILK audio codec preference for the supported codec sample rates.
0 (default)

**voice.audioProfile.SILK.8ksps.encMaxAvgBitrateKbps**
Set the maximum average encoder output bitrate in kilobits per second (kbps/s) for the supported SILK sample rate.
20 kbps (default)
6 – 20 kbps

**voice.audioProfile.SILK.12ksps.encMaxAvgBitrateKbps**
Set the maximum average encoder output bitrate in kilobits per second (kbps/s) for the supported SILK sample rate.
25 kbps (default)
7 – 25 kbps

**voice.audioProfile.SILK.16ksps.encMaxAvgBitrateKbps**
Set the maximum average encoder output bitrate in kilobits per second (kbps/s) for the supported SILK sample rate.
30 kbps (default)
8 – 30 kbps
**voice.audioProfile.SILK.24kfps.encMaxAvgBitrateKbps**

Set the maximum average encoder output bitrate in kilobits per second (kbps/s) for the supported SILK sample rate.

- 40 kbps (default)
- 12 – 40 kbps

**voice.audioProfile.SILK.encComplexity**

Specify the SILK encoder complexity. The higher the number the more complex the encoding allowed.

- 2 (default)
- 0-2

**voice.audioProfile.SILK.encDTXEnable**

- 0 (default) – Disable Enable Discontinuous transmission (DTX).
- 1 – Enable DTX in the SILK encoder. Note that DTX reduces the encoder bitrate to 0bps during silence.

**voice.audioProfile.SILK.encExpectedPktLossPercent**

Set the SILK encoder expected network packet loss percentage.

A non-zero setting allows less inter-frame dependency to be encoded into the bitstream, resulting in increasingly larger bitrates but with an average bitrate less than that configured with voice.audioProfile.SILK.*.

- 0 (default)
- 0-100

**voice.audioProfile.SILK.encInbandFECEnable**

- 0 (default) - Disable inband Forward Error Correction (FEC) in the SILK encoder.

A non-zero value here causes perceptually important speech information to be sent twice: once in the normal bitstream and again at a lower bitrate in later packets, resulting in an increased bitrate.

**voice.audioProfile.SILK.MaxPTime**

Specify the maximum SILK packet duration in milliseconds (ms).

- 20 ms

**voice.audioProfile.SILK.MinPTime**

Specify the minimum SILK packet duration in milliseconds (ms).

- 20 ms
voice.audioProfile.SILK.pTime

The recommended received SILK packet duration in milliseconds (ms).

20 ms

Opus Audio Codec Parameters

Use the following parameters to configure the Opus audio codec.

voice.audioProfile.Opus.appType

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.BitrateMode

Sets the preferred encoder transmit bit rate mode. Also controls what is sent in the SDP offer using the CBR parameter.

CVBR (default) – Constrained Variable Bit Rate

CBR – Constant Bit Rate

VBR - Variable Bit Rate

voice.audioProfile.Opus.decInbandFECEnable

Enables decoding of any received FEC information from the far end.

0 (default) - All FEC information is ignored.

1 - All information is received and decoded.

voice.audioProfile.Opus.encComplexity

Sets the Opus encoder complexity. A higher value allows for greater encoder complexity. Increased complexity increases processing requirements.

7 (default)

0-10

voice.audioProfile.Opus.encDTXEnable

0 (default) – Disables the encoder discontinuous transmit (DTX) mode in the Opus codec.

1 – The encoder skips packet TX during periods of silence and only sends periodic frames with comfort noise information.
**voice.audioProfile.Opus.encExpectedPktLossPercent**

Helps the Opus encoder decide what amount of redundant information to send when in-band FEC is enabled using the parameter **voice.audioProfile.Opus.encInbandFECEnable**.

0 (default)

0 - 100

---

**voice.audioProfile.Opus.encInbandFECEnable**

0 (default) - Disable encoder in-band FEC (Forward Error Correction) for the Opus codec.

1 - The encoder adds redundant information about the previous packet to the current output packet and determines whether to use FEC based on the expected packet loss percentage and the channel's capacity.

Configure the amount of redundant information to send using the parameter **voice.audioProfile.Opus.encExpectedPktLossPercent**.

---

**voice.audioProfile.Opus.encMaxAvgBitrateKbps**

Communicates to the far end the preferred maximum average bit rate (in kbps) for the Opus encoder.

24 (default)

8 - 510

---

**voice.audioProfile.Opus.MaxPTime**

Sets the maximum duration of media represented by a packet (in milliseconds).

10

20 (default)

---

**voice.audioProfile.Opus.pTime**

Sets the preferred duration of media represented by a packet (in milliseconds (ms)).

10

20 (default)

---

**voice.audioProfile.Opus.signalType**

Specifies the type of signal that is being encoded for the Opus codec.

Voice (default)

Auto

Music
IEEE 802.1p/Q

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

- A valid VLAN ID is specified in the phone’s network configuration.
- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or LLDP

IEEE 802.1p/Q Parameters

Use the following list to set values for IEEE 802.1p/Q parameters.

You can configure the user_priority specifically 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:

- A valid VLAN ID specified in the phone’s network configuration.
- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or CDP.

**qos.ethernet.other.user_priority**

Set user priority for packets without a per-protocol setting.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(Default)</td>
</tr>
<tr>
<td>0 - 7</td>
<td></td>
</tr>
</tbody>
</table>

**qos.ethernet.rtp.video.user_priority**

Set user-priority used for Video RTP packets.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>(Default)</td>
</tr>
<tr>
<td>0 - 7</td>
<td></td>
</tr>
</tbody>
</table>

**qos.ethernet.rtp.user_priority**

Choose the priority of voice Real-Time Protocol (RTP) packets.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>(Default)</td>
</tr>
<tr>
<td>0 - 7</td>
<td></td>
</tr>
</tbody>
</table>

**qos.ethernet.callControl.user_priority**

Set the user-priority used for call control packets.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>(Default)</td>
</tr>
<tr>
<td>0 - 7</td>
<td></td>
</tr>
</tbody>
</table>
Voice Quality Monitoring (VQMon)

You can configure the phones to generate various quality metrics that you can use to monitor sound and listening quality.

These metrics can be sent between the phones in RTCP XR packets, which are compliant with RFC 3611 —RTP Control Extended Reports (RTCP XR). The packets are sent to a report collector as specified in draft RFC Session initiation Protocol Package for Voice Quality Reporting Event. The metrics can also be sent as SIP PUBLISH messages to a central voice quality report collector.

You can use Real Time Control Protocol Extended Report (RTCP XR) to report voice quality metrics to remote endpoints. This feature supports RFC6035 compliance as well as draft implementation for voice quality reporting.

This feature is available for open SIP environments, but is not available with Skype for Business Server. For more information on VQMon, contact your Certified Reseller.

VQMon Reports

You can enable three types of voice quality reports:

- Alert – Generated when the call quality degrades below a configurable threshold.
- Periodic – Generated during a call at a configurable period.
- Session – Generated at the end of a call.

You can generate a wide range of performance metrics using the parameters shown in the following list. Some are based on current values, such as jitter buffer nominal delay and round trip delay, while others cover the time period from the beginning of the call until the report is sent, such as network packet loss. Some metrics are generated using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

VQMon Parameters

The parameters listed in the following list configure Voice Quality Monitoring.

voice.qualityMonitoring.collector.alert.moslq.threshold.critical

Specify the threshold value of listening MOS score (MOS-LQ) that causes the phone to send a critical alert quality report. Configure the desired MOS value multiplied by 10.

For example, a value of 28 corresponds to the MOS score 2.8.

0 (default) - Critical alerts are not generated due to MOS-LQ.

0 - 40

Change causes system to restart or reboot.

voice.qualityMonitoring.collector.alert.moslq.threshold.warning

Specify the threshold value of listening MOS score (MOS-LQ) that causes phone to send a warning alert quality report. Configure the desired MOS value multiplied by 10.
For example, a configured value of 35 corresponds to the MOS score 3.5.

0 (default) - Warning alerts are not generated due to MOS-LQ.

0 - 40
Change causes system to restart or reboot.

`voice.qualityMonitoring.collector.alert.delay.threshold.critical`
Specify the threshold value of one way-delay (in milliseconds) that causes the phone to send a critical alert quality report.
One-way delay includes both network delay and end system delay.

0 (default) - Critical alerts are not generated due to one-way delay.
0 - 2000 ms
Change causes system to restart or reboot.

`voice.qualityMonitoring.collector.alert.delay.threshold.warning`
Specify the threshold value of one-way delay (in milliseconds) that causes the phone to send a critical alert quality report.
One-way delay includes both network delay and end system delay.

0 (default) - Warning alerts are not generated due to one-way delay.
0 - 2000 ms
Change causes system to restart or reboot.

`voice.qualityMonitoring.collector.enable.periodic`
0 (default) - Periodic quality reports are not generated.
1 - Periodic quality reports are generated throughout a call.
Change causes system to restart or reboot.

`voice.qualityMonitoring.collector.enable.session`
1 (default) - Reports are generated at the end of each call.
0 - Quality reports are not generated at the end of each call.
Change causes system to restart or reboot.

`voice.qualityMonitoring.collector.enable.triggeredPeriodic`
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: This parameter is ignored when `voice.qualityMonitoring.collector.enable.periodic` is 1, since reports are sent throughout the duration of a call.

Change causes system to restart or reboot.

**voice.qualityMonitoring.collector.period**

The time interval (in milliseconds) between successive periodic quality reports.

20 (default)
5 - 900 ms

Change causes system to restart or reboot.

**voice.qualityMonitoring.collector.server.x.address**

The server address of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages.

Set x to 1 as only one report collector is supported at this time.

NULL (default)
IP address or hostname

Change causes system to restart or reboot.

**voice.qualityMonitoring.collector.server.x.outboundProxy.address**

This parameter directs SIP messages related to voice quality monitoring to a separate proxy. No failover is supported for this proxy, and voice quality monitoring is not available for error scenarios.

NULL (default)
IP address or FQDN

**voice.qualityMonitoring.collector.server.x.outboundProxy.port**

Specify the port to use for the voice quality monitoring outbound proxy server.

0 (default)
0 to 65535

**voice.qualityMonitoring.collector.server.x.outboundProxy.transport**

Specify the transport protocol the phone uses to send the voice quality monitoring SIP messages.

DNSnaptr (default)
TCP preferred
UDP Only
TLS
TCP Only

**voice.qualityMonitoring.collector.server.x.port**
Set the port of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages.
Set x to 1 as only one report collector is supported at this time.
5060 (default)
1 to 65535

**voice.qualityMonitoring.failover.enable**
1 (default) - The phone performs a failover when voice quality SIP PUBLISH messages are unanswered by the collector server.
0 - No failover is performed; note, however, that a failover is still triggered for all other SIP messages.
This parameter is ignored if
*voice.qualityMonitoring.collector.server.x.outboundProxy* is enabled.

**voice.qualityMonitoring.location**
Specify the device location with a valid location string. If you do not configure a location value, you must use the default string 'Unknown'.
Unknown (default)

**voice.qualityMonitoring.rfc6035.enable**
0 (default) - The existing draft implementation is supported.
1 - Complies with RFC6035.

**voice.qualityMonitoring.rtcpxr.enable**
0 (default) - RTCP-XR packets are not generated.
1 - The packets are generated.
Change causes system to restart or reboot.
Pairing with Poly Trio Systems

Topics:

- Pairing Polycom EagleEye Director II Camera System with Poly Trio
- Pairing the Poly Trio Visual+ or Trio VisualPro with Poly Trio Systems
- Daisy-Chaining Poly Trio Systems

You can pair supported cameras or a Poly Trio Visual+, Trio VisualPro, or RealPresence Group Series system with Poly Trio systems to add video and content sharing.

For information on pairing with a RealPresence Group Series, see the Poly Trio with Polycom RealPresence Group Series Integration Guide.

Pairing Polycom EagleEye Director II Camera System with Poly Trio

Enable users to place video calls by pairing Polycom EagleEye Director II camera with Poly Trio 8800 system. You can pair the EagleEye Director II camera to the system using `mr.pair.uid.1` parameter or from the Poly Trio system menu. Make sure to pair correct device with Poly Trio system.

**Note:** You cannot use EagleEye Director II camera system when Poly Trio Visual+ system is paired to the Poly Trio system. Make sure to unpair Poly Trio Visual+ system and pair EagleEye Director II camera system.

You can connect the EagleEye Director II camera system with Poly Trio system using Ethernet cable directly or corporate network. The Poly Trio connects to MSR Dock and Surface Hub using USB.

The following figure illustrates the connectivity between EagleEye Director II camera system, Poly Trio and MSR Dock.
The following figure illustrates the connectivity between EagleEye Director II camera system, Poly Trio and Surface Hub.

![Diagram of connectivity between EagleEye Director II, Poly Trio, and Surface Hub.]

**Configure Poly Trio System DHCP for EagleEye Director II Pairing Process**

You may need to configure the Poly Trio system to use DHCP to obtain an IP address before pairing with an EagleEye Director II camera system.

Ensure that your network uses a DHCP server to assign IP addresses.

The steps below help you configure the Poly Trio system to retrieve an IP address from the DHCP server before pairing with an EagleEye Director II.

**Procedure**

1. On the Poly Trio system, go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Ethernet Menu** and enable **DHCP**.
2. Check the Poly Trio system's IP address. Go to **Settings > Status > System Information** and note the IP address that was assigned to the Poly Trio system.

**Configure Poly Trio IP Address for EagleEye Director II Pairing Process**

You may need to configure an IP address for the Poly Trio system before pairing it with the EagleEye Director II camera system.

Ensure your network doesn't use a DHCP system to assign IP addresses.

The steps below help you disable DHCP and configure an IP address for the Poly Trio system. This must be done before you pair it with a Polycom EagleEye Director II camera system.
Procedure
1. On the Poly Trio system, go to Settings > Advanced > Administrative Settings > Network Configuration > Network Interfaces > Ethernet Menu and disable DHCP.
2. Set the IP Address. 
   169.254.2.2
3. Set the Subnet Mask. 
   255.255.0.0
4. Verify the Poly Trio system's IP address. Go to Settings > Status > System Information and ensure the IP address that was assigned to the Poly Trio system is displayed.

Pair Polycom EagleEye Director II Camera System
If you are using a Polycom EagleEye Director II camera system with Polycom MSR Dock or Microsoft Surface Hub, you can pair the Poly Trio system from the local interface.

Ensure the Poly Trio system is in Skype USB Optimized mode, and that it is configured on your network.

Procedure
1. Set up EagleEye Director II camera system.
2. On the Poly Trio system, go to Settings > Advanced > Network Devices.
3. Tap the filter icon and select the checkbox for Camera.
4. Navigate to the Network Devices screen.
   The EagleEye Director II camera system's last six characters of the serial number displays in the Available Devices screen.
5. Tap the EagleEye Director II camera system's serial number in the Available Devices screen.
6. Tap Pair button in Details screen.
7. Tap Complete.
   The EagleEye Director II Camera system LED blinks purple when pairing with Trio system.

For more information on EagleEye Director II Camera system LED indicators, see Polycom EagleEye Director II Camera Administrator Guide.

Pairing the Poly Trio Visual+ or Trio VisualPro with Poly Trio Systems
Pair the Poly Trio Visual+ or Trio VisualPro system with a Poly Trio 8500 or 8800 system so users can place video calls and share content.

You can pair only one Poly Trio Visual+ or Trio VisualPro system to a Poly Trio system. Poly recommends that you plug your systems into a local gigabit switch. You can pair the system using configuration files or from the Poly Trio system menu.

To pair, make sure you connect the systems to the same subnetwork and unblock the following network components:
  • Multicast address 224.0.0.200
  • Port 2000
Manually Pair with Poly Trio Systems

You can manually pair a Poly Trio 8500 or 8800 system with Poly Trio Visual+ or Trio VisualPro system from the Poly Trio system's menu.

Procedure

1. Set up the system you plan to pair with the Poly Trio system.
   For setup instructions, refer to your system’s setup sheet.
   The Welcome screen displays on your monitor and indicates steps to pair with a Poly Trio system.

2. (Poly Trio Visual+ only) Tap the Pair button on Poly Trio Visual+ to broadcast discovery to the Poly Trio.

3. On the phone menu, go to Settings > Advanced > Networked Devices and make sure Notification of New Devices is On.

4. Choose one of the following:
   • If you have not paired the device before, tap Pair with New Device, tap the device you want to pair from the Discovered Devices list, and in the Details screen, tap Pair. All currently paired devices display under Paired Devices.
   • If the device has been paired before, select the device from the Available Devices list and tap Pair.

5. When you see the message prompting you to complete pairing, do one of the following:
   • Tap Complete.
   • (Poly Trio Visual+ only) Tap the Pair button on the device.

If paired, a success message displays on the monitor(s) along with a self-view window. The LED light on the device paired with your phone is also continuously green (Poly Trio Visual+) or blue (Trio VisualPro), and a paired icon displays on the phone. If pairing is unsuccessful, you see a message that the devices could not pair. After successful pairing, if your devices disconnect for 60 seconds, a message displays that the devices have temporarily lost connection.

Poly Trio Visual+ Pairing Parameters

To pair using configuration files, enter the MAC address of your Poly Trio Visual+ device as the value for the parameter mr.pair.uid.1.

The MAC address can be in either of the following formats:
   • 00e0d::B09128D
   • 00E0DB09128D.

Use the following parameters to configure this feature and additional feature options.

mr.PairButton.notification

1 (default) - The Poly Trio system displays notifications of devices available to pair with after you press the Pair button on the Poly Trio Visual+.
0 - The Poly Trio system does not display pairing notifications.

**mr.audio.srtp.require**
1 (default) - SRTP is used to encrypt and authenticate modular room audio signals sent between Poly Trio and Poly Trio Visual+.
0

**mr.pair.uid.1**
Enter the MAC address of the Poly Trio Visual+ you want to pair with.
Null (default)
String (maximum of 64 characters)

**mr.pair.tls.enabled**
1 (default) - Enable TLS to encrypt communication between the Poly Trio and Poly Trio Visual+ systems.
0 - Disable TLS for communication between Poly Trio systems and Poly Trio Visual+ systems.
Change causes system to restart or reboot.

**mr.video.camera.focus.auto**
NULL (default)
0 - Disable the camera's automatic focus.
1 - Enable the camera's automatic focus.
Change causes system to restart or reboot.

**mr.video.camera.focus.range**
Specify the distance to the camera's optimally-focused target.
NULL (default)
0
0 - 255

**mr.video.iFrame.minPeriod**
Choose the minimum time in seconds between transmitted video i-Frames or transmitted i-Frame requests.
2 (default)
1 - 60

**smartPairing.mode**
Enables users with RealPresence Desktop on a laptop or RealPresence Mobile on a tablet to pair with the Poly Trio system using SmartPairing.

disabled (default)
manual

**smartPairing.volume**

The relative volume to use for the SmartPairing ultrasonic beacon.
6 (default)
0 - 10

**Poly Trio VisualPro Pairing Parameters**

You can pair your peripheral system with a Poly Trio using the `mr.pair.uid.1` parameter. Once paired, you can configure some Trio VisualPro system settings (including software updates) using the following parameters.

**mr.pair.uid.1**

Enter the MAC address of the peripheral you want to pair with.
Null (default)
String (maximum of 64 characters)

**mr.pair.tls.enabled**

1 (default) - Enable TLS to encrypt communication between the Poly Trio and peripheral systems.
0 - Disable TLS for communication between Poly Trio systems and peripheral systems.
Change causes system to restart or reboot.

**mr.deviceMgmt.vc2.param.softwareUpdateUri**

Identifies the URI where the paired peripheral gets its software updates.
String

**mr.deviceMgmt.vc2.param.softwareUpdateProxyServer**

Identifies the proxy server where the paired peripheral gets its software updates.
String

**mr.deviceMgmt.vc2.param.softwareUpdateMaintenceWindowEnabled**

1 (default) - Enables the maintenance window for updating the paired peripheral’s software.
0 - Disables the maintenance window for updating the paired peripheral’s software.
**mr.deviceMgmt.vc2.param.softwareUpdateMaintenceWindowStart**

Specifies when the paired peripheral’s maintenance window begins in 24-hour clock format (e.g., “10:30” or “15:00”).

String

**mr.deviceMgmt.vc2.param.softwareUpdateMaintenceWindowDuration**

Specifies how long the paired peripheral’s maintenance window lasts.

Range is 1-6 hours; default is 3.

**mr.deviceMgmt.vc2.param.displayName**

Sets the paired peripheral’s system name.

String

**mr.deviceMgmt.vc2.param.hostName**

Sets the paired peripheral’s host name.

String

### Identify Paired Devices

If you’re using multiple Poly Trio systems, you can verify which one is paired with a specific Poly Trio Visual+ or Trio VisualPro system.

**Procedure**

1. On the phone menu, go to **Settings > Advanced > Networked Devices**, and ensure that **Notification of New Devices** is **On**.
2. Select a device that displays under Paired Devices or Available Devices.
3. Tap **Identify**.
   
   The LED of the device you selected flashes to indicate it is paired.

### Place the Poly Trio Visual+ in Pairing Diagnostic Mode

If you are using multiple Poly Trio systems and want to distinguish which Poly Trio Visual+ system is paired, you can place the Poly Trio Visual+ system in pairing diagnostic mode.

**Procedure**

1. Power up the Poly Trio Visual+ device.
2. Wait for the initial LED on state to turn off.
3. Press and hold the pairing button until the LED turns orange.
4. Release the pairing button.
   
   The LED blinks.
5. Wait for the device to reboot.
   
   The paired device’s LED glows steady green.
Daisy-Chaining Poly Trio Systems

You can pair (daisy-chain) a Poly Trio 8500 or 8800 system with up to two other Poly Trio systems for enhanced audio performance in large or acoustically challenging rooms. Or you can pair a Poly Trio system with one other Poly Trio system and one Poly Trio Visual+, Poly Trio VisualPro, or Polycom RealPresence Group Series to add video and content sharing capabilities.

When you daisy-chain Poly Trio systems, the speakers and microphones act as a single speaker and microphone array for superior acoustic performance.

Note: You cannot pair or daisy-chain a Poly Trio system with another Poly Trio system or with a Poly Trio Visual+, Poly Trio VisualPro, or RealPresence Group Series system when it is connected to your network using Wi-Fi.

Daisy-Chaining Requirements

Daisy-Chain Requirements for Audio-Only

You can daisy-chain up to two Poly Trio systems to a Poly Trio 8500 or 8800 system for audio-only calls when you meet the following requirements:

▪ The Poly Trio systems must be connected to the same IP network.
▪ The Poly Trio systems must be connected to the same network subnet.
▪ The network must support multicast and multicast must be enabled.
▪ All daisy-chained Poly Trio systems are running UC Software 5.8.0AA or later.
▪ For optimal performance, follow the guidelines for setting the distance between Poly Trio systems:
  ◦ Set Poly Trio 8800 systems about 3.0 m (10 ft) apart.
  ◦ Set Poly Trio 8500 systems about 2.5 m (8 ft) apart.
▪ When signing in to Office 365/Skype for Business Online from a Poly Trio system daisy-chained to another Poly Trio system:
  ◦ Do not enter a domain. Leave the Domain field blank.
  ◦ Complete the Username field with a fully-qualified domain name, for example, user@domain.com.

Daisy-Chain Requirements for Video and Content

You can add video and content-sharing capabilities to your daisy-chained devices when you meet the above and following requirements:

▪ A Poly Trio 8500 or 8800 system is paired with one Poly Trio system and only one Poly Trio Visual+, Poly Trio VisualPro, or Group Series system for video and content
▪ Set the parameter mr.pair.maxDevices to the maximum number of paired devices (up to 2), minus 1 for the Hub system. For example, if you have a Poly Trio system set as the Hub with one daisy-chained Poly Trio system and a paired Poly Trio Visual+, set the mr.pair.maxDevices to 2.
Poly Trio System Daisy-Chain Scenarios

You can daisy-chain Poly Trio 8500 and 8800 systems in any of the following configuration scenarios.

Scenario: Audio-Only

You can daisy-chain up to two Poly Trio systems to a Poly Trio 8500 or 8800 system for enhanced audio-only when the Poly Trio systems are in Skype for Business, USB Optimized, or Generic Base Profile.

- Maximum of three Poly Trio systems.
- You must configure Poly Trio systems to the same Base Profile.
- Video or content-sharing are not supported when more than two Poly Trio systems are paired.

Scenario: Video and Content Sharing

You can daisy-chain a Poly Trio 8500 or 8800 system with two Poly Trio systems and one paired Poly Trio Visual+ system, Poly Trio VisualPro system, or RealPresence Group Series system with a Poly Trio system configured to Skype for Business, Generic, or USB Optimized Base Profile.

- Maximum of three Poly Trio devices.
- You must configure Poly Trio systems to the same Base Profile.
- Maximum of one Poly Trio Visual+ system, Poly Trio VisualPro system, or Poly RealPresence Group Series system.

Daisy-Chain Poly Trio Systems

You can daisy-chain up to three Poly Trio 8500 and 8800 systems for audio-only calls or up to two Poly Trio systems and one Poly Trio Visual+, VisualPro, or RealPresence Group Series system to add video and content sharing capabilities. You must configure one Poly Trio system as the Hub and the other systems as Devices.

Procedure

1. On the Poly Trio system you want to set as the Hub, go to Settings > Advanced > Networked Devices, and confirm Networked Device Role is set to Hub.
2. On the systems you want to set as the Device, go to Settings > Advanced > Networked Devices, and set Networked Device Role to Device.
   The systems you set as Device reboot.
3. After the Device systems reboot, on the Hub system, go to Settings > Advanced > Networked Devices, and under Available Devices, select the Device system.
4. Tap Pair and wait for the devices to connect.
   When two or more Poly Trio systems are daisy-chained, both systems display the same user interface.

Daisy-Chaining Parameters

Use the following parameters to configure daisy-chaining options for Poly Trio systems.

up.daisyChain.device.style

Choose how to visually indicate which Poly Trio system is set to Device in a daisy-chaining scenario.
LineAtTopOfScreen (default) - A line displays at the top of the Poly Trio screen.
GlobalMenuIcon - An icon displays on the Poly Trio system Home screen.
Change causes system to restart or reboot.
Video Features for Poly Trio

Topics:

- **Display a Monitor Index Number**
- **Video Call Overlays**
- **Video Quality Parameters**
- **Video and Camera Options**
- **Camera Specific Presets**
- **Supported Video Codecs with Poly Trio**
- **Toggling Between Audio-only or Audio-Video Calls**
- **H.323 Protocol**
- **I-Frames**
- **Video Parameters**

After you set up phones on your network with the default configuration, you can make custom configurations to optimize video calling for your phones, if supported.

Poly Trio system support for the Poly Trio Visual+ and VisualPro systems varies by model:

- You can pair any Poly Trio system with a Poly Trio Visual+ system.
- You can pair a Poly Trio 8500 or Poly Trio 8800 system with a Poly Trio Visual+ or VisualPro system. The Poly Trio 8300 system does not support the Trio VisualPro system.

The Poly Trio system with a paired Poly Trio Visual+ supports transmission and reception of high-quality video images with the following supported cameras:

- Polycom EagleEye IV USB camera
- Polycom EagleEye Mini USB camera
- Poly EagleEye Cube USB camera
- Polycom EagleEye Director II camera (Poly Trio 8800 only)
- Logitech C930e webcam

The Poly Trio system with a paired Trio VisualPro or RealPresence Group Series system supports transmission and reception of high-quality video images with the following supported cameras:

- Polycom EagleEye IV camera
- Polycom EagleEye Director II camera
- Polycom EagleEye Producer camera
- Polycom EagleEye Acoustic camera
- Poly EagleEye Cube HDCl camera
- Poly Studio USB video bar

Polycom Open SIP video is compatible with the following RFCs:

- RFC 3984 - RTP Payload Format for H.264 video
- RFC 5168 - XML Schema for Media Control
Display a Monitor Index Number
You can display a number on monitors connected to a Poly Trio Visual+ paired to the Poly Trio system.

Procedure
» On the Poly Trio system, go to Settings > Advanced > Networked Devices > Identify Devices. An index number displays on each monitor.

Video Call Overlays
When using the Poly Trio Visual+ system for video calls, you can configure where and for how long the video overlay displays on the monitor.

The video overlay displays call details including participant names and a call timer. By default, the call overlay displays at the bottom of the monitor screen with no timeout.

Video Call Overlay Parameters
Use the following parameters to configure the video call overlay that displays on the Poly Trio Visual+ system monitor during video calls.

`video.conf.galleryView.overlayPosition`
Use this parameter to set the location of the video overlay.
- Bottom (default) - The video overlay displays at the bottom of the monitor screen.
- Top - The video overlay displays at the top of the monitor screen.
- None - The video overlay does not display.

`video.conf.galleryView.overlayTimeout`
Set the timer for the video overlay on the Poly Trio Visual+ monitor. The overlay disappears after the time you set.
- 0 (default) - The video overlay does not time out and displays indefinitely.
- 0 - 60000 ms

Video Quality Parameters
Use the following parameters to configure quality settings for video calls.

`video.quality`
The optimal quality for video that is sent in a call or a conference.
- motion (default) — For outgoing video that has motion or movement.
sharpness — For outgoing video that has little or no movement.

Note: If motion is not selected, moderate to heavy motion can cause some frames to be dropped.

**video.quality.content**
- motion (default) - For outgoing video that has motion or movement.
- sharpness — For outgoing video that has little or no movement.

**video.autoFullScreen**
- 0 (default) — Video calls only use the full screen layout if it is explicitly selected by the user.
- 1 — Video calls use the full screen layout by default, such as when a video call is first created or when an audio call transitions to a video call.

**video.callRate**
- The default call rate (in kbps) to use when initially negotiating bandwidth for a video call.
  - 2048 (default)
  - 128 - 6144

**video.forceRtcpVideoCodecControl**
- 0 (default) — RTCP feedback messages depend on a successful SDP negotiation of a=rtcp-fb and are not used if that negotiation is missing.
- 1 — The phone is forced to send RTCP feedback messages to request fast I-frame updates along with SIP INFO messages for all video calls irrespective of a successful SDP negotiation of a=rtcp-fb.

For an account of all parameter dependencies when setting I-frame requests, refer to the section I-Frames.

**video.maxCallRate**
- Sets the maximum call rate that the users can select. The value set on the phone cannot exceed this value. If video.callRate exceeds this value, this parameter overrides video.callRate and this value is used as the maximum.
  - 4096 (default)
  - 128 - 6144
Video and Camera Options

At the start of a video call, video-enabled phones, including those with a connected USB camera, transmit an RTP encapsulated video stream by default. Use the following configuration parameters to configure the video and camera options for supported cameras.

Use the global video and camera parameters to configure settings for any Poly camera. Use per-camera video parameters to control settings for specific Poly camera models.

Video and Camera Parameters

Use the following parameters to configure video and camera options for all Poly cameras.

**feature.fecc.enabled**

1 (default) – Enable far-end camera control.
0 – Disable far-end camera control.
Change causes system to restart or reboot.

**feature.fecc.payload**

Set the RTP payload used to receive far-end camera control data.

124 (default)
100 - 127

**homeScreen.camera.enable**

0 (default) - A Camera menu item is shown on the main menu.
1 - A Camera menu item displays on the Home Screen allowing users to pan, tilt, or zoom.

**mr.video.camera.focus.auto**

NULL (default)
0 - Disable the camera's automatic focus.
1 - Enable the camera's automatic focus.
Change causes system to restart or reboot.

**mr.video.camera.focus.range**

Specify the distance to the camera's optimally-focused target.

NULL (default)
0
0 - 255
**reg.x.fecc.enabled**

1 (default) – Enable far-end camera control for the line you specify with x.
0 - Disable far-end camera control for the line.

**up.arrow.repeatDelay**

Choose the milliseconds (ms) an arrow button must be held before the arrow starts repeating in the Camera Controls menu for supported Poly USB cameras.

500 ms (default)
100 – 5000 ms

**up.arrow.repeatRate**

Choose the milliseconds (ms) between repeated simulated presses while an arrow button is being held down. This applies to the arrows in the Camera Controls menu for supported Poly USB cameras.

80 ms (default)
50 – 2000 ms

**video.camera.autoWhiteBalance**

0 – Disable auto white balance.
1– Enable auto white balance.

**video.camera.backlightCompensation**

NULL (default)
0 - 1000

**video.camera.brightness**

Sets the brightness level of the video stream. The value range is from 0 (dimmest) to 1000 (brightest).

NULL (default)
0 - 1000

**video.camera.contrast**

Sets the contrast level of the video stream for all supported USB cameras. The value range is from 0 (no contrast increase) to 3 (most contrast increase), and 4 (noise reduction contrast).

NULL (default)
0 - 1000

**video.camera.controlStyle**
Choose whether to control pan and tilt Poly USB cameras with directional arrow buttons or separate pan/tilt sliders.

Default (default)
Alternate

`video.camera.flickerAvoidance`
Sets the flicker avoidance for all supported USB cameras.
Null (default) - Flicker avoidance is automatic.
50hz AC power frequency flicker avoidance (Europe/Asia).
60hz AC power frequency flicker avoidance (North America).
Disabled

`video.camera.focus.auto`
NULL (default)
0 - Disable the camera's automatic focus.
1 - Enable the camera's automatic focus.
Change causes system to restart or reboot.

`video.camera.focus.range`
Specify the distance to the camera's optimally-focused target.
NULL (default)
0 - 255

`video.camera.frameRate`
Sets the target frame rate (frames per second) for all supported USB cameras. Values indicate a fixed frame rate from 5 (least smooth) to 30 (most smooth).
25 (default)
5 - 30
If `video.camera.frameRate` is set to a decimal number, the value 25 is used instead.

`video.camera.menuLocation`
Specify if camera settings display under the Advanced menu for administrators or the Basic menu for users.
Basic (default)
Advanced

`video.camera.preset.home.pan`
Set the pan coordinate for a camera home preset. Default values are set by and depend on the camera you are using.

0 – 1000

**video.camera.preset.home.tilt**

Set the tilt coordinate for a camera home preset. Default values are set by and depend on the camera you are using.

0 - 1000

**video.camera.preset.home.uponIdle.delay**

Set the number of minutes after the idle timeout expires to move the camera to the home preset.

0 (default)
0 - 3600

**video.camera.preset.home.uponIdle.enabled**

0 (default) – Do not move the camera to the home preset when the phone is idle.
1 - Move the camera to the home preset when the phone is idle.

**video.camera.preset.home.zoom**

Set the zoom coordinate for a camera home preset. Default values are set by and depend on the camera you are using.

0 - 1000

**video.camera.presetIndex**

Preset Index
(default)
0-1000

**video.camera.saturation**

Sets the saturation level of video captured by any supported USB camera.

NULL (default)
0 - 1000

**video.camera.sharpness**

Sets the sharpness level of video captured.

NULL (default)
0 - 1000

**video.camera.trackingEnabled**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 (default) - Enables automatic camera tracking. You can then set the tracking type, speed, and size.

0 - Disables camera tracking.

**video.camera.trackingFramingMode**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

0 (default) - Frame Speaker: Frames the active speaker.

1 - Frame Group: Frames the participants in the room (camera movement is seen on the far end).

2 - Frame Group with Transition (EagleEye Producer only): Frames the participants in the room (camera movement is seen on the far end).

**video.camera.trackingFramingSize**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 - Medium (default): Average-sized frame.

0 - Wide: Most expansive frame.

2 - Tight: Close-up frame.

**video.camera.trackingPipEnabled**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 (default) - Enables People in Picture (PIP), which displays a group or room view to far-end participants.

0 - Disables PIP.

**video.camera.trackingSpeed**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 (default) - Normal: Tracks transitions at a medium rate.

0 - Slow: Tracks transitions slowly.

2 - Fast: Tracks transitions quickly.

**video.camera.whiteBalance**

Use to correct the white balance tint of video captured by any supported USB camera.

NULL (default)

0 - 1000
**video.localCameraView.callState**

This parameter applies only when `video.localCameraView.userControl` is set to PerSession or Hidden.

1 (default) - The local camera view displays on the Poly Trio Visual+ monitor.

0 - The local camera view does not display on the Poly Trio Visual+ monitor.

**video.localCameraView.fullScreen.callState**

Set to determine how the local call view (LCV) displays when the phone is in a call.

0 (default) - Displays the LCV in PIP during a call.

1 - Displays the LCV in full screen during a call.

**video.localCameraView.fullScreen.idleState**

Set to determine how the local call view (LCV) displays when the phone is idle.

0 (default) - Does not display the LCV when the phone is idle.

1 - Displays the LCV in picture-in-picture (PIP) when the phone is idle.

**video.localCameraView.fullScreen.userControl**

Set to enable users to control how the local call view (LCV) displays during a call.

Persistent (default) - Enables users to access the Layout menu and control how the LCV displays before a call.

PerSession - Enables users to access the Layout menu and control how the LCV displays before or during a call.

Hidden - Hides the Layout menu so that users cannot control how the LCV displays.

**video.vc4Decode.overrunTolerance**

Set the overrun errors per second for video decoder tolerance. If the decoder generates more overrun errors than the number you set, the Poly Trio system drops SVC video layer 1 to reduce the decoder load.

0 (default) – Disable tolerance for decoder overrun errors.

0 – 100 overrun errors per second

**Per-Camera Video Parameters**

You can use the following per-camera parameters to configure camera and video options for each type of Poly camera used in your environment.

Using the parameter `video.camera.x.type`, you can configure parameters differently for the following cameras supported with Poly Trio 8300, 8500 and 8800 systems paired with Poly Trio Visual+:

- Polycom EagleEye IV USB camera
- Polycom EagleEye Mini USB camera
Accessories:
- Poly EagleEye Cube USB camera
- Polycom EagleEye Director II camera (Poly Trio 8800 only)
- Logitech C930e webcam

You can also use the parameter `video.camera.x.type` to configure the following cameras that are supported with a paired Trio VisualPro system:
- Polycom EagleEye IV camera
- Polycom EagleEye Director II camera
- Polycom EagleEye Producer camera
- Polycom EagleEye Acoustic camera
- Poly EagleEye Cube HDCI camera
- Poly Studio USB video bar

Below is an example of per-camera configurations for the EagleEye IV USB camera and EagleEye Mini USB camera.

**Example Per-Camera Configuration**

<table>
<thead>
<tr>
<th>Camera Type Configuration</th>
<th>Per-Camera Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>video.camera.1.type = EagleEyeIVUSB</code></td>
<td><code>video.camera.1.focus.auto=1</code></td>
</tr>
<tr>
<td></td>
<td><code>video.camera.1.orientation=Inverted</code></td>
</tr>
<tr>
<td><code>video.camera.2.type=EagleEyeMini</code></td>
<td><code>video.camera.2.focus.auto=0</code></td>
</tr>
<tr>
<td></td>
<td><code>video.camera.2.focus.range=150</code></td>
</tr>
</tbody>
</table>

For information about camera parameters with a paired RealPresence Group Series system, see the [Poly Trio with Polycom RealPresence Group Series Integration Guide](#).

**call.singleKeyPressCameraControls**

1 (default) - Tapping **Camera** in the call view directly shows the **Camera Controls** menu for Poly USB cameras.

0 - Tapping **Camera** in the call view shows a menu with camera preferences, presets, and camera controls menu items for Poly USB cameras.

**feature.fecc.allowLocalCameraFarEndControl**

1 (default) – Allow the far-end user to control the local near-end camera controls, such as pan, tilt, and zoom, for the Poly USB cameras.

0 - The far-end user cannot control the local near-end camera.

**video.camera.gamma**

Set the factor to use for gamma correction applied to each frame of video captured by the Poly USB cameras. You can use this setting to correct for video that appears too dark or too light.

NULL (default)
**video.camera.hue**

Use to correct the color of video captured by the Poly USB cameras.

NULL (default)

0 - 1000

**video.camera.invertPanControl**

Invert the direction of the pan control for the Poly USB camera.

0 (default)

**video.camera.orientation**

Specify the camera mounting orientation for Poly USB cameras: Normal or Inverted (upside down)

Normal (default)

Inverted

**video.camera.x.presetIndex**

Set the number of presets available.

NULL (default)

0-1000

**video.camera.preset.x.label**

Enter a label for the Poly USB camera preset.

NULL (default)

String 0 – 12 characters

**video.camera.preset.x.pan**

Set the pan for the Poly USB camera presets, where x equals the preset.

NULL (default)

0 - 1000

**video.camera.preset.x.tilt**

Set the tilt for the Poly USB camera presets, where x equals the preset.

NULL (default)

0 - 1000
**video.camera.preset.x.zoom**
Set the zoom for the EagleEye IV USB camera presets, where x equals the preset.
- NULL (default)
- 0 - 1000

**video.camera.x.autoWhiteBalance**
Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.
- 1 – Enable auto white balance. This overrides the `video.camera.whiteBalance` parameter.
- 0 – Disable auto white balance.

**video.camera.x.backlightCompensation**
Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.
Set the backlight compensation of the video stream.
- NULL (default)
- 0 - 1000
This overrides the `video.camera.backlightCompensation` parameter.

**video.camera.x.brightness**
Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.
Sets the brightness level of the video stream. The value range is from 0 (dimmest) to 1000 (brightest).
- NULL (default)
- 3
- 0 - 1000
This overrides the `video.camera.brightness` parameter.

**video.camera.x.contrast**
Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.
Sets the contrast level of the video stream. The value range is from 0 (no contrast increase) to 3 (most contrast increase), and 4 (noise reduction contrast).
- NULL (default)
- 0 - 1000
This overrides the `video.camera.contrast` parameter.
**video.camera.x.flickerAvoidance**

Set for per-camera configuration when you specify the camera type using the video.camera.x.type parameter.

Null (default) - Flicker avoidance is automatic.

50hz AC power frequency flicker avoidance (Europe/Asia).

60hz AC power frequency flicker avoidance (North America).

Disabled

This parameter overrides video.camera.flickerAvoidance.

**video.camera.x.focus.auto**

Set for per-camera configuration when you specify the camera type using the video.camera.x.type parameter.

NULL (default)

0 - Disable the camera's automatic focus.

1 - Enable the camera's automatic focus. This overrides the video.camera.focus.auto parameter.

Change causes system to restart or reboot.

**video.camera.x.focus.range**

Set for per-camera configuration when you specify the camera type using the video.camera.x.type parameter.

Specify the distance to the camera's optimally-focused target.

NULL (default)

0

255

This overrides the video.camera.focus.range parameter.

**video.camera.x.gamma**

Set for per-camera configuration when you specify the camera type using the video.camera.x.type parameter.

Set the factor to use for gamma correction applied to each frame of video captured. You can use this setting to correct video that appears too dark or too light.

NULL (default)

0

1000

This parameter overrides video.camera.gamma.
**video.camera.x.hue**

Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.

Use to correct the color of video captured.

- NULL (default)
- 500
- 1000

This parameter overrides `video.camera.hue`.

**video.camera.x.orientation**

Specify the camera mounting orientation for Poly USB cameras: Normal or Inverted (upside down)

- Normal (default)
- Inverted

This parameter overrides `video.camera.orientation`.

**video.camera.x.saturation**

Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.

Sets the saturation level of video captured by any supported USB camera.

- NULL (default)
- 0 - 1000

This parameter overrides `video.camera.saturation`.

**video.camera.x.sharpness**

Set for per-camera configuration when you specify the camera type using the `video.camera.x.type` parameter.

Sets the sharpness level of video captured.

- NULL (default)
- 0 - 1000

This parameter overrides `video.camera.sharpness`.

**video.camera.x.trackingEnabled**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

- 1 (default) - Enables automatic camera tracking. You can then set the tracking type, speed, and size.
- 0 - Disables camera tracking.
**video.camera.x.trackingFramingMode**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

0 (default) - Frame Speaker: Frames the active speaker.

1 - Frame Group: Frames the participants in the room (camera movement is seen on the far end).

2 - Frame Group with Transition (EagleEye Producer only): Frames the participants in the room (camera movement is seen on the far end).

**video.camera.x.trackingFramingSize**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 - Medium (default): Average-sized frame.

0 - Wide: Most expansive frame.

2 - Tight: Close-up frame.

**video.camera.x.trackingPipEnabled**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 (default) - Enables People in Picture (PIP), which displays a group or room view to far-end participants.

0 - Disables PIP.

**video.camera.x.trackingSpeed**

For the EagleEye Director II, EagleEye Producer, Poly Studio, or EagleEye Cube USB cameras.

1 (default) - Normal: Tracks transitions at a medium rate.

0 - Slow: Tracks transitions slowly.

2 - Fast: Tracks transitions quickly.

**video.camera.x.type**

Choose a camera type that corresponds to x, where x = 1 to 3. The value set for x in this parameter and related parameters determines the configuration settings for the camera type you specify.

NULL (default)

EagleEyeMini

EagleEyeDirectorII

EagleEyeProducer

EagleEyeAcoustic

EagleEyeCubeUSB

EagleEyeIVUSB
video.camera.x.whiteBalance

Set for per-camera configuration when you specify the camera type using the video.camera.x.type parameter.

Use to correct the white balance tint of video captured.

NULL (default)
0 - 1000

This parameter overrides video.camera.whiteBalance.

Camera Specific Presets

If you have multiple cameras configured to work with a Poly Trio system, you can configure your system to switch automatically between cameras when a user selects a preset.

Using the cameras unique ID, you can configure preset positions specifically for that camera. For example, you can associate Preset 1 with a Poly EagleEye Cube HDCI camera paired with a Poly Trio VisualPro and Poly Trio 8800 system and associate Preset 2 with a Polycom EagleEye IV camera. Below is an example of this camera preset configuration where x is the preset.

```
video.camera.multiCamera.enabled=1
video.camera.selection.1.uniqueId="64167f2e1de9-12345"
video.camera.preset.1.selection="0004f2fd19f4-12345"
video.camera.selection.2.uniqueId="532563e1de9-67890"
video.camera.preset.2.selection="0005f3fd21f3-67890"
```

Camera Specific Preset Parameters

Use the following parameters to set presets to automatically select a camera associated with a preset.

video.camera.multiCamera.enabled

Set to indicate if one or more cameras are paired with the Poly Trio system and you want to automatically switch to a paired camera when a user selects a preset.

0 (default) A single camera is paired with the Poly Trio system.
1 - More than one camera is paired with the Poly Trio system.

video.camera.selection.x.uniqueId

Enter the unique ID of the camera.
**video.camera.preset.x.selection**

Enter the unique ID of the camera associated with the selected preset. Leave blank if preset applies to the active camera.

NULL (default)
String

**video.camera.preset.home.selection**

Enter the unique ID of the camera associated with the selected preset. Leave blank if preset applies to the active camera.

NULL (default)
String

---

**Supported Video Codecs with Poly Trio**

Poly supports the following video standards and codecs:

- H.264 advanced video coding (AVC) baseline profile and high profile
- H.264 scalable video coding (SVC) (X-H264UC) and Remote Desktop Protocol (RDP) for desktop and application sharing. (Microsoft only)

The following table lists video codecs supported by Poly Trio systems.

**Supported Video Codecs**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>MIME Type</th>
<th>Frame Size</th>
<th>Bit Rate (kbps)</th>
<th>Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.264</td>
<td>H264/90000</td>
<td></td>
<td>6144 kbps</td>
<td>30</td>
</tr>
<tr>
<td>XH264UC</td>
<td></td>
<td></td>
<td>6144 kbps</td>
<td></td>
</tr>
</tbody>
</table>

**Video Codec Parameters for Poly Trio**

To support Poly Trio solution video interoperability with Cisco, set the following parameters:

- `video.codecPref.H264HP="0"`
- `video.codecPref.H264HP.packetizationMode0="0"`
- `video.codecPref.H264="0"`

Use the parameters in the following table to prioritize and adjust the video codecs used by the Poly Trio solution.

**video.codecPref.H264HP**
Sets the H.264 High Profile video codec preference priority.

- 0 - 8
- 2 (default)

`video.codecPref.H264HP.packetizationMode0`

- 0 - 8
- 5 (default)

`video.codecPref.H264SVC`

`video.codecPref.Xdata`

Sets the Remote Desktop Protocol (RDP) codec preference priority. A value of 1 indicates the codec is the most preferred and has highest priority.

- 0 - 8
- 7 (default)

`video.codecPref.XH264UC`

Sets the Microsoft H.264 UC video codec preference priority.

- 0 - 8
- 1 (default)

`video.codecPref.XUlpFecUC`

Sets the forward error correction (FEC) codec priority.

- 8 (default)
- 0 - 8

### Toggling Between Audio-only or Audio-Video Calls

You can enable users to toggle between audio-only and audio-video calls.

When this feature is enabled on a phone using video capabilities, you can toggle calls between audio-only or audio-video.

This feature applies only to outbound calls from your phone; incoming video calls to your phone are answered using video even when you set the feature to use audio-only.

When the phone is registered, you can:

- **Use** `video.callMode.default` **to begin calls as audio-video or audio only.** By default, calls begin as audio-video. After a video call has ended, the phone returns to audio-only.
  
  If you set this parameter to audio, users can choose to add Video to the call.
• **Use** `up.homeScreen.audioCall.enabled` **to enable a Home screen icon that allows users to make audio-only calls.** Far-end users can add video during a call if the far-end device is video capable.

### Audio-only or Audio-Video Call Parameters

The following parameters configure whether the phone starts a call with audio and video.

**up.homeScreen.audioCall.enabled**

- 0 (default) - Disable a Home screen icon that allows users to make audio-only calls.
- 1 - Enable a Home screen icon that allows users to make audio-only calls.

Devices that support video calling show an 'Audio Call' button on the Home screen to initiate audio-only calls.

**video.autoStartVideoTx**

- 1 (default) - Automatically begin video to the far side when you start a call.
- 0 - Video to the far side does not begin.

Note that when the phone Base Profile is set to Skype or Lync, the default is 1.

**audioVideoToggle.callMode.persistent**

- 0 - Resets the call mode set by a user to the default.
- 1 (default) - Maintains the call mode set by a user.

**audioVideoToggle.callMode.persistent**

- 0 - Resets the call mode set by a user to the default.
- 1 - Maintains the call mode set by a user.

**video.callMode.default**

Allow the user to begin calls as audio-only or with video.

- video (default)
- audio - Set the initial call to audio only and video may be added during a call.

On Poly Trio solution, you can combine this parameter with `video.autoStartVideoTx`.
**H.323 Protocol**

You can configure Poly Trio systems to use H.323 protocol and enable direct communication with H.323 endpoints, gatekeepers, call servers, media servers, and signaling gateways.

**Note:** H.460 is not supported on Poly Trio systems, so you cannot configure NAT firewall traversal for H.323 calls.

**SIP and H.323 Protocol**

The Poly Trio phones can support both SIP and H.323 signaling simultaneously, and the phones support bridging both types of calls during multi-party conference calls.

By default, when more than one protocol is available, each protocol displays as a soft key and the user can choose which protocol to use.

While SIP supports server redundancy and several transport options, only a single configured H.323 gatekeeper address is supported per phone. The phone does not require H.323 gatekeepers, but you can use them if available. If an H.323 gatekeeper is not configured or is unavailable, you can still enable the phones to make H.323 calls.

You can also disable support of the SIP protocol for telephony signaling so that all calls are routed via the H.323 protocol; keep in mind that the phone then will not be able to answer SIP calls.

**SIP and H.323 Directory Protocols**

When the SIP and H.323 protocols are both enabled on Poly Trio systems, the systems can automatically detect the correct or optimal signaling protocol when dialing a call from the local or corporate directory.

The protocol used when placing a call from the user's local contact directory is unspecified by default. The user can select whether to use SIP or H.323 protocol for specific contacts from the directory.

The protocol used when placing a call from the user's corporate directory depends on the order of the attributes in the corporate directory. If only `SIP_address` is defined, then the SIP protocol is used. If only `H323_address` is defined, then the H.323 protocol is used. If both are defined, then the one that was defined first is used.

For example, if `dir.corp.attribute.4.type` is `SIP_address` and `dir.corp.attribute.5.type` is `H323_address`, then the SIP protocol is used by default.

**H.323 and SIP Protocol Limitations and Restrictions**

Take into consideration the following conditions and limitations for H.323 Protocol:

- If the phone has only the H.323 protocol enabled, the phone cannot be used to answer SIP calls.
- If the phone has only the SIP protocol enabled, the phone cannot be used to answer H.323 calls.
- If both SIP and H.323 protocols are disabled, the phone continues to work as a SIP-only phone; however, the phone is not registered, but users can send and receive SIP URL calls.
- H.460 NAT firewall traversal is not supported.
- Calls made using H.323 cannot be forwarded or transferred, and the following conditions apply:
  - The Transfer and Forward soft keys do not display during an H.323 call.
  - The Forward soft key does not display on the Lines screen if the primary line is an H.323 line.
- If a user presses the **Transfer** soft key during an H.323 call, no action is taken.
- The auto-divert field in the local contact directory entry is ignored when a call is placed to that contact using H.323.
- If a conference host ends a three-way conference call and one of the parties is connected by H.323, that party is not transferred to the other party that was part of the conference call.

**Supported H.323 Video Standards**

The following table lists the standards the H.323 feature supports.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU-T Recommendation Q.931 (1998)</td>
<td>ISDN user-network interface layer 3 specification for basic call control</td>
</tr>
<tr>
<td>ITU-T Recommendation H.225.0 (2003)</td>
<td>Call signaling protocols and media stream packetization for packet-based multimedia communications systems</td>
</tr>
<tr>
<td>ITU-T Recommendation H.239 (2014)</td>
<td>Content sharing protocol</td>
</tr>
<tr>
<td>ITU-T Recommendation H.224 (2005)</td>
<td>A real time control protocol for far-end camera control</td>
</tr>
</tbody>
</table>

**H.323 Protocol Parameters**

Use the following parameters to do the following:

- Configure SIP and H.323 protocols.
- Set up a SIP and H.323 dial plan.
- Set up manual protocol routing using soft keys.
  - If the protocol to place a call cannot be determined, the **Use SIP** and **Use H.323** soft keys display, and users must select one to place the call.
- Configure auto-answering on H.323 calls only.
- Set the preferred protocol to SIP.
- Set to configure one SIP line, one H.323 line, and a dual protocol line—both SIP and H.323 can be used.
- Set the preferred protocol for off-hook calls on the third (dual protocol) line to SIP.

H.323 is supported only on Poly Trio systems.

**up.manualProtocolRouting**
Specifies whether to choose a protocol routing or use a default protocol.

1 (Default) - User is presented with a protocol routing choice in situations where a call can be placed using either protocol (for example, with SIP and H.323 protocols).
0 - Default protocol is used.

**up.manualProtocolRouting.softKeys**


1 (Default) - Soft keys are enabled. Use soft keys to choose between the SIP or H.323 protocol.
0 - Soft keys for protocol routing do not display.

**call.autoAnswer.H323**

Enables and disables auto-answer for H.323 calls.

0 (default) - Disabled
1 - Enabled

**call.enableOnNotRegistered**

Enable or disable calls on the phone when it is not registered. When enabled, the phones can make calls using the H.323 protocol even though an H.323 gatekeeper is not configured.

Lync Base Profile – 0 (default)
Generic Base Profile – 1 (default)
1 - Enabled
0 - Disabled
Change causes system to restart or reboot.

**call.autoAnswer.videoMute**

0 (default) - Video begins transmitting (video Tx) automatically after a call is auto-answered.
1 - User must start video transmission (video Tx) manually when a call is auto-answered.

**call.autoRouting.preferredProtocol**

SIP (default) - Calls are placed via SIP if available or via H.323 if SIP is not available.
H323 - Calls are placed via H.323 if available, or via SIP if H.323 is not available.

**call.autoRouting.preference**

line - Calls are placed via the first available line, regardless of its protocol capabilities. If the first available line has both SIP and H.323 capabilities, the preferred protocol is used (call.autoRouting.preferredProtocol).
protocol - The first available line with the preferred protocol activated is used, if available. If not available, the first available line is used. Note that auto-routing is used when manual routing selection features (\texttt{up\_manualProtocolRouting}) are disabled.

\texttt{reg.x.protocol.H323}

Enable or disable H.323 signalling for registration x.

0 (default) - Disabled
1 - Enabled

\texttt{reg.x.server.H323.y.address}

Address of the H.323 gatekeeper.

Null (default)
IP address or hostname

\texttt{reg.x.server.H323.y.port}

Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used.

0 (default)
0 to 65535

\texttt{reg.x.server.H323.y.expires}

Desired registration period.

3600
positive integer

\texttt{voIpProt.H323.autoGateKeeperDiscovery}

1 (default) - The phone will attempt to discover an H.323 gatekeeper address via the standard multicast technique, provided that a statically configured gatekeeper address is not available.

0 - The phone will not send out any gatekeeper discovery messages.

Change causes system to restart or reboot.

\texttt{voIpProt.H323.blockFacilityOnStartH245}

0 (default) - Facility messages when using H.245 are not removed.
1 - Facility messages when using H.245 are removed.

Change causes system to restart or reboot.

\texttt{voIpProt.H323.dtmfViaSignaling.enabled}

Enable or disable use of H.323 signaling channel for DTMF key press transmission.
1 (default) - Enabled
0 - Disabled
Change causes system to restart or reboot.

**voIpProt.H323.dtmfViaSignaling.H245alphanumericMode**
1 (default) - The phone supports H.245 signaling channel alphanumeric mode DTMF transmission.
0 - The phone does not support H.245 signaling channel alphanumeric mode DTMF transmission

Note: If both alphanumeric and signal modes can be used, the phone gives priority to DTMF.
Change causes system to restart or reboot.

**voIpProt.H323.dtmfViaSignaling.H245signalMode**
1 (default) - The phone will support H.245 signaling channel signal mode DTMF transmission.
0 - The phone will not support H.245 signaling channel signal mode DTMF transmission.
Change causes system to restart or reboot.

**voIpProt.H323.enable**
0 (default) - The H.323 protocol is not used for call routing, dial plan, DTMF, and URL dialing.
1 - The H.323 protocol is used for call routing, dial plan, DTMF, and URL dialing.
Change causes system to restart or reboot.

**voIpProt.H323.local.port**
Local port for sending and receiving H.323 signaling packets.
0 - 1720 is used for the local port but is not advertised in the H.323 signaling.
0 to 65535 - The value is used for the local port and it is advertised in the H.323 signaling.
Change causes system to restart or reboot.

**voIpProt.H323.local.RAS.port**
Specifies the local port value for RAS signaling.
1719 (default)
1 to 65535
Change causes system to restart or reboot.

**voIpProt.server.H323.x.address**
Specify the address of the H.323 gatekeeper. Only one H.323 gatekeeper per phone is supported. If more than one is configured, only the first is used.

Null (default)

IP address or hostname

`voIpProt.server.H323.x.port`

Designate a port to be used for H.323 signaling. The H.323 gatekeeper RAS signaling uses UDP, while the H.225/245 signaling uses TCP.

1719 (default)
0 to 65535

`voIpProt.server.H323.x.expires`

Set a desired registration period.

3600 (default)
positive integer.

`sec.H235.mediaEncryption.enabled`

Enable or disable H.235 media encryption.

1 (default) - Enabled
0 - Disabled

Change causes system to restart or reboot.

`sec.H235.mediaEncryption.offer`

0 (default) - The media encryption offer is not initiated with the far-end.
1 - If `sec.H235.mediaEncryption.enabled` is also set to 1, media encryption negotiations are initiated with the far-end; however, successful negotiations are not a requirement for the call to complete.

Change causes system to restart or reboot.

`sec.H235.mediaEncryption.require`

0 (default) - The media encryption requirement is not required.
1 - If `sec.H235.mediaEncryption.enabled` is also set to 1, media encryption negotiations are initiated or completed with the far end, but if negotiations fail, the call is dropped.

Change causes system to restart or reboot.
I-Frames

When video streams initialize, devices transmit video packets called I-frames (reference frames) that contain information to display a complete picture.

The devices subsequently send smaller and less complete frames, known as P-frames, to consume less bandwidth. Due to packet loss, jitter, or corruption, devices occasionally need to make multiple requests for a complete I-frame in order to reset the full frame, after which devices can 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

<table>
<thead>
<tr>
<th>video.forceRtcpVideoCodecControl</th>
<th>video.dynamicControlMethod</th>
<th>volpProt.SDP.offer.rtcpVideoCodecControl</th>
<th>Behavior when requesting video I-frame updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 (n/a)</td>
<td>0</td>
<td>Only SIP INFO messages are sent. No RTCP-FB is offered in SDP.</td>
</tr>
<tr>
<td>0</td>
<td>1 (n/a)</td>
<td>0</td>
<td>Only SIP INFO messages are sent. No RTCP-FB is offered in SDP.</td>
</tr>
<tr>
<td>0</td>
<td>0 (n/a)</td>
<td>1</td>
<td>RTCP-FB is offered in SDP. If SDP responses do not contain the required RTCP-FB attribute, then only SIP INFO requests are used.</td>
</tr>
<tr>
<td>0</td>
<td>1 (n/a)</td>
<td>1</td>
<td>RTCP-FB is offered in SDP. If SDP responses do not contain the required RTCP-FB attribute, then only SIP INFO requests are used.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>The SDP attribute a=rtcp-fb is not included in SDP offers. Both RTCP-FB and SIP INFO messages are attempted.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>The SDP attribute a=rtcp-fb is not included in SDP offers. Both RTCP-FB and SIP INFO messages are attempted. If no RTCP-FB messages are received, only SIP INFO messages are sent. If no response is received for SIP INFO messages then, again, both RTCP-FB and SIP INFO messages are attempted.</td>
</tr>
</tbody>
</table>
Video Features for Poly Trio

<table>
<thead>
<tr>
<th>video.forceRtcpVideoCodecControl</th>
<th>video.dynamicControlMethod</th>
<th>volpProt.SDP.offer.rtcpVideoCodecControl</th>
<th>Behavior when requesting video I-frame updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>RTCP-FB is offered in SDP. Even if the SDP response does not include an accepted a=rtcp-fb attribute both RTCP-FB and SIP INFO messages are sent.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>RTCP-FB is offered in SDP. Even if the SDP response does not include an accepted a=rtcp-fb attribute both RTCP-FB and SIP INFO messages are sent initially. If no RTCP-FB response is received, only SIP INFO messages are sent afterwards.</td>
</tr>
</tbody>
</table>

Video Parameters

Use the following parameters to configure video features on video-capable phones.

**video.allowWithSource**

Restricts sending video codec negotiation in Session Description Protocol (SDP).

- 0 (default)
- 0 or 1

**video.enable**

1 (default) - Enables video calling capabilities for outgoing and incoming calls.

0 - Disables video calling capabilities.

**video.autoFullScreen**

0 (default) - Video calls use the full screen layout, only if explicitly selected by the user.

1 - Video calls use the full screen layout by default.

**video.conf.profile**

Sets the video resolution to large window in all layouts.

- 540p (default)
- 1080p
- 720p
- 360p
240p
180p

**video.dynamicControlMethod**

0 (default)
1 - The first I-Frame request uses the method defined by
`video.forceRtcpVideoCodecControl` and subsequent requests alternate between RTCP-FB and SIP INFO.

To set other methods for I-frame requests, refer the parameter
`video.forceRtcpVideoCodecControl`.

**video.iFrame.delay**

0 (default)
1 - 10 seconds - Transmits an extra I-frame after the video starts.

The amount of delay from the start of video until the I-frame is sent is configurable up to 10 seconds.

Change causes system to restart or reboot.

**video.iFrame.minPeriod**

Time taken before sending a second I-frame in response to requests from the far end.

2 (default)
1 - 60

**video.iFrame.onPacketLoss**

0 (default)
1 - Transmits an I-frame to the far end when video RTP packet loss occurs.

**video.iFrame.period.onBoard**

Set the I-Frame interval used for the VC4 encoder.

180 (default)
300 maximum

**video.mute.sendCannedVideo**

1 (default) - The Poly Trio system sends a custom image to the far end when you press Stop my video.

0 - The Poly Trio system does not send a video to the far end when you press Stop my video and displays a no video graphic, by default.
**Video Codec Preference Parameters**

Use the following video codec parameters to specify video codec preferences.

To disable codecs, set the value to 0. A value of 1 indicates the codec is the most preferred and has highest priority.

```plaintext
video.codecPref.H261
  Sets the H.261 payload type.
  6 (default)
  0 - 8

video.codecPref.H264
  Sets the H.264 payload type.
  4 (default)
  0 - 8

video.codecPref.H263 1998
  Sets the H.263 payload type.
  5 (default)
  0 - 8

video.codecPref.H263
  5 (default)
  0 - 8

video.codecPref.H264
  4 (default)
  0 - 8

video.codecPref.H264.packetizationMode0
  Sets the H.264 payload type when packetization mode is set to 0.
  5 (default)
  0 - 8

video.codecPref.H264HP
  Sets the H.264 High Profile video codec preference priority.
  2 (default)
  0 - 8
```
**video.codecPref.H264HP.packetizationMode0**
Sets the H.264 high profile payload type when packetization mode is set to 0.
- 3 (default)
- 0 - 8

**video.codecPref.H264SVC**

**video.codecPref.Xdata**
Sets the Remote Desktop Protocol (RDP) codec preference priority.
- 7 (default)
- 0 - 8
- 1 - Codec has highest priority.

**video.codecPref.XH264UC**
Sets the Microsoft H.264 UC video codec preference priority.
- 1 (default)
- 0 - 8

**video.codecPref.XUlpFecUC**
Sets the forward error correction (FEC) codec priority.
- 8 (default)
- 0 - 8

**Video Profile Parameters for Poly Trio**
These settings include a group of low-level video codec parameters.
For most use cases, the default values are appropriate. does not recommend changing the default values unless specifically advised to do so.

**video.profile.H264.payloadType**
Specifies the RTP payload format type for H264/90000 MIME type.
- 109 (default)
- 96 to 127
- Change causes system to restart or reboot.

**video.profile.H264.payloadType.packetizationMode0**
Sets the H.264 payload type when packetization mode is set to 0.
video.profile.H264.payloadType.packetizationModel
Sets the H.264 payload type when packetization mode is set to 1.
109 (default)
0 - 127

video.profile.H264.profileLevel
Specifies the highest profile level within the baseline profile supported in video calls.
4.1 (default)
1, 1b, 1.1, 1.2, 1.3, and 2
Change causes system to restart or reboot.

video.profile.H264HP.jitterBufferMax
The largest jitter buffer depth to be supported (in milliseconds).
2000 (default)
533 - 2500 milliseconds
This parameter should be set to the smallest possible value that supports the expected network jitter. Jitter above this size always causes packet loss.

video.profile.H264HP.jitterBufferMin
The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time.
150 milliseconds (default)
33 - 1000 milliseconds
Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.

video.profile.H264HP.jitterBufferShrink
The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks.
70 milliseconds (default)
33 - 1000 milliseconds
Use smaller values (33 ms) to minimize the delay from trusted networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
**video.profile.H264HP.payloadType**

Specifies the RTP payload format type for H264/90000 MIME type.

100 (default)

0 - 127

**video.profile.H264HP.payloadType.packetizationMode1**

Sets the H.264 high profile payload type when packetization mode is set to 1.

100 (default)

0 - 127

**video.profile.H264HP.profileLevel**

Specifies the highest profile level within the baseline profile supported in video calls.

4.1 (default)

String (1 - 5 characters)

**video.profile.H264M.payloadType.packetizationMode0**

Sets the H.264 high profile payload type when packetization mode is set to 0.

113 (default)

0 - 127

**video.profile.Xdata.payloadType**

Specifies the payload type to use in SDP negotiations of the payload used for Skype for Business desktop content sharing.

127 (default)

0 - 127

**video.profile.XH264UC.jitterBufferMax**

The largest supported jitter buffer depth.

2000 (default)

533 - 2500 milliseconds

Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.

**video.profile.XH264UC.jitterBufferMin**

The smallest jitter buffer depth that must be achieved before play out begins for the first time.

150 (default)

33 - 1000 milliseconds
Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.

**video.profile.XH264UC.jitterBufferShrink**

Specifies the minimum duration in milliseconds of Real-time Transport Protocol (RTP) packet Rx, with no packet loss to trigger jitter buffer size shrinks.

- 70 (default)
- 33 - 1000

Use smaller values (1000 ms) to minimize the delay on known good networks.

**video.profile.XH264UC.mstMode**

Specifies the multi-session transmission packetization mode.

- NI-TC (default)
- String

The value of NI-TC identifies non-interleaved combined timestamp and CS-DON mode. This value should not be modified for interoperation with other Skype for Business devices.

**video.profile.XH264UC.payloadType**

Specifies the RTP payload format type for H.264 MIME type.

- 122 (default)
- 0 - 127

**video.profile.XUlpFecUC.alwaysOn**

- 1 (default) - Enable Forward Error Correction during video calls even when it is not needed.
- 0 - Disable Forward Error Correction.

**video.profile.XUlpFecUC.debug.rxDropBurst**

- 1 (default)
- 1 - 100

**video.profile.XUlpFecUC.debug.rxDropOnlyLayer0**

- 1 (default)
- 0 or 1

**video.profile.XUlpFecUC.debug.rxDropRate**

- 0 (default)
video.profile.XUlPFecUC.debug.txDropBurst
1 (default)
1 - 100

video.profile.XUlPFecUC.debug.txDropRate
0 (default)
0 - 40000

video.profile.XUlPFecUC.noLossTurnOffTimeout
300 (default)
10 - 7200

video.profile.XUlPFecUC.payloadType
123 (default)
0 - 127

video.profile.XUlPFecUC.rxEnabled
1 (default)
0 or 1

video.profile.XUlPFecUC.txEnabled
1 (default)
0 or 1

video.simpleJB.enable
1 (default)
0 or 1

video.simpleJB.lipSyncDelayMs
0 (default)
0 - 250 ms

video.simpleJB.timeoutMs
100 ms (default)
0 - 250 ms
video.rtcpbandwidthdetect.enable

0 (default)

1 - Poly Trio 8800 uses an estimated bandwidth value from the RTCP message to control Tx/Rx video bps.
Phone Display Features

Topics:

- Administrator Menu on Poly Trio Systems
- Poly Trio Visual+ and Trio VisualPro Monitor Display Options
- Poly Trio System Theme
- Poly Trio System Display Name
- Poly Trio System Status Messages
- Olson Time Zone Configuration
- Time Zone Location Description
- Time and Date
- Phone Languages
- Hide the MAC Address
- Unique Line Labels for Registration Lines
- Poly Trio System Number Formatting
- Number or Custom Label
- Custom Icons for Contacts and Line Registrations
- Capture Your Device's Current Screen
- Default In-Call Screen
- Custom Call Control Options
- Poly Trio Home Screen Parameters

This section explains features you can configure for the phone's screen display and lists parameters you can use to configure these features.

Administrator Menu on Poly Trio Systems

On the Poly Trio systems, you can add the Advanced menu containing a subset of administrator settings. The Advanced menu item does not require a password but one can be assigned to it.

After enabling this feature, the Advanced menu provides access to all administrator features except:

- Line Configuration
- Call Server Configuration
- TLS Security
- Test Automation
Administrator Menu Parameters

Use the following parameters to enable the Administrator or Advanced menu.

\texttt{device.auth.localAdvancedPassword.set}

Set a password for the \texttt{Advanced} menu.
- 0 (default) - You cannot set a password for the \texttt{Advanced} menu.
- 1 - You can set a password for the \texttt{Administrator} menu.

\texttt{device.auth.localAdvancedPassword}

Enter a password for the \texttt{Administrator} menu.
- Null (default)
- String (0 to 64 characters)

\texttt{feature.advancedUser.enabled}

- 0 (default) - The password-protected \texttt{Advanced} menu displays.
- 1 - Renames the \texttt{Advanced} menu item to \texttt{Admin} and adds a menu item \texttt{Advanced} that contains a subset of administrator features.

The \texttt{Advanced} menu does not require a password, but you have the option to assign one to it.

Poly Trio Visual+ and Trio VisualPro Monitor Display Options

When using the Poly Trio system with a paired peripheral system, you can configure display options on the connected monitor(s), including system information, user menu options, and background images and logos.

Poly Trio Visual+ and Trio VisualPro Display Parameters

Use the following parameters to hide or display icons and features on monitors connected with Poly Trio Visual+ or Trio VisualPro systems when paired with a Poly Trio system.

\texttt{feature.exchangeVoiceMail.menuLocation}

- Default (default) - Show the Voicemail menu in the global menu only when unread voicemails are available. After the voicemail is accessed, the Voicemail option no longer displays in the global menu and is accessible in the phone menu.
- Everywhere - Always show the Voicemail menu in the global menu and phone menu.
- MenusOnly - Show the Voicemail menu only in the phone Features menu.

\texttt{mr.bg.selection}
Sets a background image for the connected monitor(s).

Poly (default)

Auto - Automatically cycles through HallstatterSeeLake, BavarianAlps, and ForgetMeNotPond. The background image changes each time a video call ends.

BlueGradient

BavarianAlps

ForgetMeNotPond

HallstatterSeeLake

Custom - Use a custom background specified by mr.bg.url.

A custom background image must be a JPEG with 1920x1080 resolution and a maximum size of 2.9 MB for it to display correctly on the paired Trio VisualPro or RealPresence Group Series system monitor(s). (PNG images, which typically are supported on Poly Trio, are not supported in this setup.)

**mr.bg.showPlcmLogo**

1 (default) - The Poly logo shows on the connected monitor(s).

0 - Hides the Poly logo.

**mr.bg.showWelcomeInstructions**

All (default) - Display the content-sharing graphic and welcome message on the connected monitor(s).

TextOnly - Hide the content-sharing graphic.

None - Hide both the content-sharing graphic and welcome message.

**mr.bg.url**

Specify an HTTP URL location of a background image to use on the connected monitor(s).

The Poly Trio system supports PNG and JPEG images up to 2.9 MB.

A custom background image must be a JPEG with 1920x1080 resolution and a maximum size of 2.9 MB for it to display correctly on the paired Trio VisualPro or RealPresence Group Series system monitor(s). (PNG images, which typically are supported on Poly Trio, are not supported in this setup.)

This background image is used only if mr.bg.selection= "Custom"

Null (default)

String (maximum 256 characters)

**up.hideSystemIpAddress**

Specify where the IP address of the Poly Trio system and Poly Trio Visual+ system are hidden from view.
You can access the IP address from the phone Advanced menu if you set this parameter to ‘Menus’ or ‘Everywhere’.

Poly Trio System Theme
You can set the Poly Trio system theme, labels, and colors that display on the user interface. When the Poly Trio system's Base Profile is set to Skype, the Skype for Business theme displays by default.

Poly Trio System Theme Parameter
The following parameter configures the Poly Trio system theme.

\texttt{up.uiTheme}

- Default (default) - The phone displays the default Poly theme.
- SkypeForBusiness - The phone displays the Skype for Business theme.

Poly Trio System Display Name
The system name displays in the Global menu of the Poly Trio systems and on monitor(s) connected to a paired Poly Trio Visual+ or Trio VisualPro system.

The system name also displays on any devices connected with the system wirelessly, such as Bluetooth-enabled or AirPlay-certified devices.

By default, the system name displays as Poly Trio <model number> (xxxxxx) where (xxxxxx) is the last six digits of the phone's MAC address. For example, Poly Trio 8800 (01161C).

You can configure the name that displays on the system, the connected monitor, and any devices wirelessly connected to the system. The name you configure for the system, using any of the following parameters, displays in the subsequent priority order:

- \texttt{system.name}
- \texttt{reg.1.displayname}
- \texttt{reg.1.label}
- \texttt{reg.1.address}
- Default system name

If you set the system name using the \texttt{system.name} parameter, the value you set displays for the system 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 \texttt{system.name}:

- AirPlay: \texttt{content.airplayServer.name}
- Bluetooth: \texttt{bluetooth.device.name}
- Wireless Display: \texttt{content.wirelessDisplay.name}
System Display Name Parameters

Set the system name using one or more of following parameters.

**content.airplayServer.name**

Specify a system name for the local content sink for AirPlay-certified devices. If left blank, the previously configured or default system name is used.

- NULL (default)
- UTF-8 encoded string

**content.wirelessDisplay.sink.name**

Specify a system name for the local content sink for Android or Windows devices. If left blank the previously configured or default system name is used.

- NULL (default)
- UTF-8 encoded string

**bluetooth.device.name**

Enter the name of the system that broadcasts over Bluetooth to other devices.

- NULL (default)
- UTF-8 encoded string

**reg.1.address**

The user part (for example, 1002) or the user and the host part (for example, 1002@polycom.com) of the registration SIP URI or the H.323 ID/extension.

- Null (default)
- string address

**reg.1.displayname**

The display name used in SIP signaling and/or the H.323 alias used as the default caller ID.

- Null (default)
- UTF-8 encoded string

**reg.1.label**

The text label that displays next to the line key for registration x.

The maximum number of characters for this parameter value is 256; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters you use. Parameter values that exceed the phone’s maximum display length are truncated by ellipses (...). The rules for parameter up.cfgLabelElide determine how the label is truncated.
Null (default)
UTF-8 encoded string

**system.name**

The system name that displays at the top left corner of the monitor, and at the top of the Global menu of the Poly Trio system.
Enter a string, maximum 96 characters.

**Poly Trio System Status Messages**

You can choose to display a maximum of five multi-line messages in the Poly Trio Visual+ or Trio VisualPro system Status Bar.

Each message can contain a maximum of 64 characters. If the length of the message exceeds the size of the status bar, the message wraps into multiple lines.

When you configure multiple messages, you can adjust the number of seconds each message displays.

**Poly Trio System Status Message Parameters**

Use the following parameters to configure status messages on the Poly Trio system.

**up.status.message.flash.rate**

Specify the number of seconds to display a message before moving to the next message.

- 2 seconds (default)
- 1 - 8 seconds

**up.status.message.x**

<messaging line one>
<messaging line two>
<messaging line three>
<messaging line four>
<messaging line five>

**Olson Time Zone Configuration**

Poly Trio systems support Olson time zones in the Internet Assigned Numbers Authority (IANA) database.

**Note:** To ensure you set the correct time zone for your devices, Poly recommends that you configure an Olson time zone.
When you set a valid Olson time zone ID from the IANA database, it overrides existing Greenwich Mean Time (GMT) offset and daylight saving time (DST) rules set for your Poly device and any paired Poly Trio Visual+ or Polycom RealPresence Group Series system.

If the parameter value is null, the Poly device attempts to match your existing GMT offset and DST rules with one of the Olson time zones that you can choose in the Web Configuration Utility or device menu. Note that your GMT offset and DST rules may not match one of these time zones because not every Olson time zone in the IANA database is listed in these locations. In these cases:

- The Poly Trio system uses the existing configured GMT offset and DST rules.
- The time zone for third-party applications, for example, the Zoom Rooms Controller application, is set to the GMT offset with DST rules disabled.
- The Poly Trio system application log logs a warning.
- Paired Trio VisualPro and RealPresence Group Series systems use the default time zone.
- Paired Poly Trio Visual+ systems use the time zone configured for the Poly Trio system.

You can set an Olson time zone on Poly Trio systems using one of the following methods:

- Set a valid Olson time zone ID using the parameter `tcpIpApp.sntpolsonTimezoneID`. Poly recommends this method for mass provisioning.
- Use the Web Configuration Utility to select a time zone for a single device.
- Use a device menu to choose a time zone for a single device.

Note that if you are using multiple methods, there are priority rules among methods.

### Olson Time Zone Parameters

Use the following parameters to configure an Olson time zone.

**tcpIpApp.sntpolsonTimezoneID**

Enter an Olson time zone ID. If set to an invalid or unrecognized value, the time zone is be set to GMT with daylight saving disabled.

- **Null (default)**
  - When set, this parameter overrides existing GMT offset and DST rules.

### Set an Olson Time Zone with the Web Configuration Utility

You can set a valid Olson time zone for a single device using the Web Configuration Utility.

**Procedure**

1. Get the IP address for your Poly device.
2. Enter the IP address to a browser on a computer connected to the same network as the phone.
3. Log into the Web Configuration Utility as an admin.
4. Go to **Preference > Date & Time**.
5. From the **Time Zone ID**, select a time zone.
   - Refer to the Olson Time Zone IDs table to see which option you should choose for the Olson time zone you want.
6. Select **Save**.
Set an Olson Time Zone from the Device Menu

You can set a valid Olson time zone for a single device from its menu.

Procedure
1. On the phone menu, go to **Settings > Advanced**.
2. In **Advanced**, login with the admin password.
3. Go to **Administration settings > Network Configurations > Time Zone ID**.
4. Select a time zone.
   Refer to the Olson Time Zone IDs table to see which option you should choose for the Olson time zone you want.

Olson Time Zone IDs

The following table lists the Olson time zone IDs from the IANA database with the corresponding time zone IDs you can select using the Poly Trio system Web Configuration Utility or device menu.

**Note:** Not every Olson time zone ID in the IANA database is included in the table.

<table>
<thead>
<tr>
<th>Olson Time Zone ID</th>
<th>Poly Trio Time Zone ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacific/Midway</td>
<td>(GMT -11:00) Midway Island</td>
</tr>
<tr>
<td>Pacific/Honolulu</td>
<td>(GMT -10:00) Hawaii</td>
</tr>
<tr>
<td>America/Anchorage</td>
<td>(GMT -9:00) Alaska</td>
</tr>
<tr>
<td>Mexico/BajaNorte</td>
<td>(GMT -8:00) Baja California</td>
</tr>
<tr>
<td>America/Phoenix</td>
<td>(GMT -7:00) Arizona</td>
</tr>
<tr>
<td>America/Chihuahua</td>
<td>(GMT -7:00) Chihuahua,La Paz</td>
</tr>
<tr>
<td>America/Denver</td>
<td>(GMT -7:00) Mountain Time (US &amp; Canada)</td>
</tr>
<tr>
<td>America/Costa_Rica</td>
<td>(GMT -6:00) Central America</td>
</tr>
<tr>
<td>America/Chicago</td>
<td>(GMT -6:00) Central Time (US &amp; Canada)</td>
</tr>
<tr>
<td>America/Mexico_City</td>
<td>(GMT -6:00) Mexico City</td>
</tr>
<tr>
<td>America/Regina</td>
<td>(GMT -6:00) Saskatchewan</td>
</tr>
<tr>
<td>America/Bogota</td>
<td>(GMT -5:00) Bogota,Lima</td>
</tr>
<tr>
<td>America/New_York</td>
<td>(GMT -5:00) Eastern Time (US &amp; Canada)</td>
</tr>
<tr>
<td>America/Caracas</td>
<td>(GMT -4:30) Caracas</td>
</tr>
<tr>
<td>America/Barbados</td>
<td>Atlantic Time (Barbados)</td>
</tr>
<tr>
<td>Olson Time Zone ID</td>
<td>Poly Trio Time Zone ID</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>America/Halifax</td>
<td>(GMT -4:00) Atlantic Time (Canada)</td>
</tr>
<tr>
<td>America/Manaus</td>
<td>(GMT -4:00) Manaus,La Paz</td>
</tr>
<tr>
<td>America/Santiago</td>
<td>(GMT -3:00) Santiago</td>
</tr>
<tr>
<td>America/St_Johns</td>
<td>(GMT -3:30) Newfoundland</td>
</tr>
<tr>
<td>America/Sao_Paulo</td>
<td>(GMT -3:00) Brasilia</td>
</tr>
<tr>
<td>America/Argentina/Buenos_Aires</td>
<td>(GMT -3:00) Buenos Aires</td>
</tr>
<tr>
<td>America/Godthab</td>
<td>(GMT -3:00) Greenland</td>
</tr>
<tr>
<td>America/Montevideo</td>
<td>(GMT -3:00) Montevideo</td>
</tr>
<tr>
<td>Atlantic/South_Georgia</td>
<td>(GMT -2:00) Mid-Atlantic</td>
</tr>
<tr>
<td>Atlantic/Azores</td>
<td>(GMT -1:00) Azores</td>
</tr>
<tr>
<td>Atlantic/Cape_Verde</td>
<td>(GMT -1:00) Cape Verde Islands</td>
</tr>
<tr>
<td>Africa/Casablanca</td>
<td>(GMT 0:00) Casablanca</td>
</tr>
<tr>
<td>Europe/London</td>
<td>(GMT 0:00) London,Lisbon</td>
</tr>
<tr>
<td>Europe/Amsterdam</td>
<td>(GMT +1:00) Amsterdam,Berlin</td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td>(GMT +1:00) Bratislava</td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td>(GMT +1:00) Brussels</td>
</tr>
<tr>
<td>Europe/Sarajevo</td>
<td>(GMT +1:00) Sarajevo,Skopje</td>
</tr>
<tr>
<td>Africa/Brazzaville</td>
<td>(GMT +1:00) West Central Africa</td>
</tr>
<tr>
<td>Africa/Windhoek</td>
<td>(GMT +1:00) Windhoek</td>
</tr>
<tr>
<td>Asia/Amman</td>
<td>Amman</td>
</tr>
<tr>
<td>Europe/Athens</td>
<td>(GMT +2:00) Athens</td>
</tr>
<tr>
<td>Asia/Beirut</td>
<td>Beirut</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td>(GMT +2:00) Bucharest,Cairo</td>
</tr>
<tr>
<td>Europe/Helsinki</td>
<td>(GMT +2:00) Helsinki,Kyiv</td>
</tr>
<tr>
<td>Asia/Jerusalem</td>
<td>(GMT +2:00) Jerusalem</td>
</tr>
<tr>
<td>Africa/Harare</td>
<td>(GMT +2:00) Harare,Pretoria</td>
</tr>
<tr>
<td>Europe/Minsk</td>
<td>(GMT +3:00) Minsk</td>
</tr>
<tr>
<td>Olson Time Zone ID</td>
<td>Poly Trio Time Zone ID</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Asia/Istanbul</td>
<td>(GMT +3:00) Istanbul</td>
</tr>
<tr>
<td>Europe/Moscow</td>
<td>(GMT +3:00) Moscow</td>
</tr>
<tr>
<td>Asia/Kuwait</td>
<td>(GMT +3:00) Kuwait,Riyadh</td>
</tr>
<tr>
<td>Africa/Nairobi</td>
<td>(GMT +3:00) Nairobi</td>
</tr>
<tr>
<td>Asia/Tehran</td>
<td>(GMT +3:30) Tehran</td>
</tr>
<tr>
<td>Asia/Baku</td>
<td>(GMT +4:00) Baku,Tbilisi</td>
</tr>
<tr>
<td>Asia/Yerevan</td>
<td>(GMT +4:00) Yerevan</td>
</tr>
<tr>
<td>Asia/Dubai</td>
<td>Dubai</td>
</tr>
<tr>
<td>Asia/Kabul</td>
<td>(GMT +4:30) Kabul</td>
</tr>
<tr>
<td>Asia/Karachi</td>
<td>(GMT +5:00) Karachi</td>
</tr>
<tr>
<td>Asia/Tashkent</td>
<td>(GMT +5:00) Tashkent</td>
</tr>
<tr>
<td>Asia/Yekaterinburg</td>
<td>(GMT +5:00) Yekaterinburg (RTZ 4)</td>
</tr>
<tr>
<td>Asia/Calcutta</td>
<td>(GMT +5:30) Kolkata,New Delhi</td>
</tr>
<tr>
<td>Asia/Colombo</td>
<td>(GMT +5:30) Sri Jayawardenepura</td>
</tr>
<tr>
<td>Asia/Katmandu</td>
<td>(GMT +5:45) Kathmandu</td>
</tr>
<tr>
<td>Asia/Dhaka</td>
<td>(GMT +6:00) Astana,Dhaka</td>
</tr>
<tr>
<td>Asia/Rangoon</td>
<td>(GMT +6:30) Yangon (Rangoon)</td>
</tr>
<tr>
<td>Asia/Krasnoyarsk</td>
<td>(GMT +7:00) Krasnoyarsk (RTZ 6)</td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td>(GMT +7:00) Bangkok,Hanoi</td>
</tr>
<tr>
<td>Asia/Jakarta</td>
<td>(GMT +7:00) Jakarta</td>
</tr>
<tr>
<td>Asia/Shanghai</td>
<td>(GMT +8:00) Beijing,Chongqing</td>
</tr>
<tr>
<td>Asia/Hong_Kong</td>
<td>(GMT +8:00) Hong Kong,Urumqi</td>
</tr>
<tr>
<td>Asia/Irkutsk</td>
<td>(GMT +8:00) Irkutsk (RTZ 7)</td>
</tr>
<tr>
<td>Asia/Kuala_Lumpur</td>
<td>(GMT +8:00) Kuala Lumpur</td>
</tr>
<tr>
<td>Asia/Taipei</td>
<td>(GMT +8:00) Taipei,Perth</td>
</tr>
<tr>
<td>Asia/Tokyo</td>
<td>(GMT +9:00) Tokyo,Seoul,Osaka</td>
</tr>
<tr>
<td>Asia/Yakutsk</td>
<td>(GMT +9:00) Sapporo,Yakutsk (RTZ 8)</td>
</tr>
<tr>
<td>Olson Time Zone ID</td>
<td>Poly Trio Time Zone ID</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Australia/Adelaide</td>
<td>Adelaide</td>
</tr>
<tr>
<td>Australia/Darwin</td>
<td>Darwin</td>
</tr>
<tr>
<td>Australia/Brisbane</td>
<td>Brisbane</td>
</tr>
<tr>
<td>Australia/Hobart</td>
<td>(GMT +10:00) Hobart</td>
</tr>
<tr>
<td>Australia/Sydney</td>
<td>Sydney, Canberra</td>
</tr>
<tr>
<td>Asia/Vladivostok</td>
<td>(GMT +10:00) Vladivostok</td>
</tr>
<tr>
<td>Pacific/Guam</td>
<td>(GMT +10:00) Guam, Port Moresby</td>
</tr>
<tr>
<td>Asia/Magadan</td>
<td>(GMT +10:00) Magadan (RTZ 9)</td>
</tr>
<tr>
<td>Pacific/Auckland</td>
<td>(GMT +12:00) Auckland, Anadyr</td>
</tr>
<tr>
<td>Pacific/Fiji</td>
<td>(GMT +12:00) Fiji Islands</td>
</tr>
<tr>
<td>Pacific/Majuro</td>
<td>(GMT +12:00) Marshall Islands</td>
</tr>
<tr>
<td>Pacific/Tongatapu</td>
<td>(GMT +13:00) Nuku'alofa</td>
</tr>
</tbody>
</table>

**Time Zone Location Description**

The following two parameters configure a time zone location description for their associated GMT offset:

- `device.sntp.gmtOffsetcityID` If you are not provisioning phones manually from the phone menu or Web Configuration Utility and you are setting the `device.sntp.gmtOffset` parameter, then you must configure `device.sntp.gmtOffsetcityID` to ensure that the correct time zone location description displays on the phone menu and Web Configuration Utility. The time zone location description is set automatically if you set the `device.sntp.gmtOffset` parameter manually using the phone menu or Web Configuration Utility.

- `tcpIpApp.sntp.gmtOffsetcityID` If you are not provisioning phones manually from the Web Configuration Utility and you are setting the `tcpIpApp.sntp.gmtOffset` parameter, then you must configure `tcpIpApp.sntp.gmtOffsetcityID` to ensure that the correct time zone location description displays on the Web Configuration Utility. The time zone location description is set automatically if you set the `tcpIpApp.sntp.gmtOffset` parameter manually using the Web Configuration Utility.

**Related Links**

- [Time and Date Display Parameters](#) on page 211
**Time Zone Location Parameters**

The following parameters configure time zone location.

**Time Zone Location Parameter Values**

<table>
<thead>
<tr>
<th>Permitted Value</th>
<th>Time Zone Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(GMT -12:00) Eniwetok,Kwajalein</td>
</tr>
<tr>
<td>1</td>
<td>(GMT -11:00) Midway Island</td>
</tr>
<tr>
<td>2</td>
<td>(GMT -10:00) Hawaii</td>
</tr>
<tr>
<td>3</td>
<td>(GMT -9:00) Alaska</td>
</tr>
<tr>
<td>4</td>
<td>(GMT -8:00) Pacific Time (US &amp; Canada)</td>
</tr>
<tr>
<td>5</td>
<td>(GMT -8:00) Baja California</td>
</tr>
<tr>
<td>6</td>
<td>(GMT -7:00) Mountain Time (US &amp; Canada)</td>
</tr>
<tr>
<td>7</td>
<td>(GMT -7:00) Chihuahua,La Paz</td>
</tr>
<tr>
<td>8</td>
<td>(GMT -7:00) Mazatlan</td>
</tr>
<tr>
<td>9</td>
<td>(GMT -7:00) Arizona</td>
</tr>
<tr>
<td>10</td>
<td>(GMT -6:00) Central Time (US &amp; Canada)</td>
</tr>
<tr>
<td>11</td>
<td>(GMT -6:00) Mexico City</td>
</tr>
<tr>
<td>12</td>
<td>(GMT -6:00) Saskatchewan</td>
</tr>
<tr>
<td>13</td>
<td>(GMT -6:00) Guadalajara</td>
</tr>
<tr>
<td>14</td>
<td>(GMT -6:00) Monterrey</td>
</tr>
<tr>
<td>15</td>
<td>(GMT -6:00) Central America</td>
</tr>
<tr>
<td>16</td>
<td>(GMT -5:00) Eastern Time (US &amp; Canada)</td>
</tr>
<tr>
<td>17</td>
<td>(GMT -5:00) Indiana (East)</td>
</tr>
<tr>
<td>18</td>
<td>(GMT -5:00) Bogota,Lima</td>
</tr>
<tr>
<td>19</td>
<td>(GMT -5:00) Quito</td>
</tr>
<tr>
<td>20</td>
<td>(GMT -4:30) Caracas</td>
</tr>
<tr>
<td>Permitted Value</td>
<td>Time Zone Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>21</td>
<td>(GMT -4:00) Atlantic Time (Canada)</td>
</tr>
<tr>
<td>22</td>
<td>(GMT -4:00) San Juan</td>
</tr>
<tr>
<td>23</td>
<td>(GMT -4:00) Manaus, La Paz</td>
</tr>
<tr>
<td>24</td>
<td>(GMT -4:00) Asuncion, Cuiaba</td>
</tr>
<tr>
<td>25</td>
<td>(GMT -4:00) Georgetown</td>
</tr>
<tr>
<td>26</td>
<td>(GMT -3:30) Newfoundland</td>
</tr>
<tr>
<td>27</td>
<td>(GMT -3:00) Brasilia</td>
</tr>
<tr>
<td>28</td>
<td>(GMT -3:00) Buenos Aires</td>
</tr>
<tr>
<td>29</td>
<td>(GMT -3:00) Greenland</td>
</tr>
<tr>
<td>30</td>
<td>(GMT -3:00) Cayenne, Fortaleza</td>
</tr>
<tr>
<td>31</td>
<td>(GMT -3:00) Montevideo</td>
</tr>
<tr>
<td>32</td>
<td>(GMT -3:00) Salvador</td>
</tr>
<tr>
<td>33</td>
<td>(GMT -3:00) Santiago</td>
</tr>
<tr>
<td>34</td>
<td>(GMT -2:00) Mid-Atlantic</td>
</tr>
<tr>
<td>35</td>
<td>(GMT -1:00) Azores</td>
</tr>
<tr>
<td>36</td>
<td>(GMT -1:00) Cape Verde Islands</td>
</tr>
<tr>
<td>37</td>
<td>(GMT 0:00) Western Europe Time</td>
</tr>
<tr>
<td>38</td>
<td>(GMT 0:00) London, Lisbon</td>
</tr>
<tr>
<td>39</td>
<td>(GMT 0:00) Casablanca</td>
</tr>
<tr>
<td>40</td>
<td>(GMT 0:00) Dublin</td>
</tr>
<tr>
<td>41</td>
<td>(GMT 0:00) Edinburgh</td>
</tr>
<tr>
<td>42</td>
<td>(GMT 0:00) Monrovia</td>
</tr>
<tr>
<td>43</td>
<td>(GMT 0:00) Reykjavik</td>
</tr>
<tr>
<td>44</td>
<td>(GMT +1:00) Belgrade</td>
</tr>
<tr>
<td>45</td>
<td>(GMT +1:00) Bratislava</td>
</tr>
<tr>
<td>46</td>
<td>(GMT +1:00) Budapest</td>
</tr>
<tr>
<td>47</td>
<td>(GMT +1:00) Ljubljana</td>
</tr>
<tr>
<td>48</td>
<td>(GMT +1:00) Prague</td>
</tr>
<tr>
<td>49</td>
<td>(GMT +1:00) Sarajevo, Skopje</td>
</tr>
<tr>
<td>50</td>
<td>(GMT +1:00) Warsaw, Zagreb</td>
</tr>
<tr>
<td>Permitted Value</td>
<td>Time Zone Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>51</td>
<td>(GMT +1:00) Brussels</td>
</tr>
<tr>
<td>52</td>
<td>(GMT +1:00) Copenhagen</td>
</tr>
<tr>
<td>53</td>
<td>(GMT +1:00) Madrid,Paris</td>
</tr>
<tr>
<td>54</td>
<td>(GMT +1:00) Amsterdam,Berlin</td>
</tr>
<tr>
<td>55</td>
<td>(GMT +1:00) Bern,Rome</td>
</tr>
<tr>
<td>56</td>
<td>(GMT +1:00) Stockholm,Vienna</td>
</tr>
<tr>
<td>57</td>
<td>(GMT +1:00) West Central Africa</td>
</tr>
<tr>
<td>58</td>
<td>(GMT +1:00) Windhoek</td>
</tr>
<tr>
<td>59</td>
<td>(GMT +2:00) Bucharest,Cairo</td>
</tr>
<tr>
<td>60</td>
<td>(GMT +2:00) Amman,Beirut</td>
</tr>
<tr>
<td>61</td>
<td>(GMT +2:00) Helsinki,Kyiv</td>
</tr>
<tr>
<td>62</td>
<td>(GMT +2:00) Riga,Sofia</td>
</tr>
<tr>
<td>63</td>
<td>(GMT +2:00) Tallinn,Vilnius</td>
</tr>
<tr>
<td>64</td>
<td>(GMT +2:00) Athens,Istanbul</td>
</tr>
<tr>
<td>65</td>
<td>(GMT +2:00) Damascus</td>
</tr>
<tr>
<td>66</td>
<td>(GMT +2:00) E.Europe</td>
</tr>
<tr>
<td>67</td>
<td>(GMT +2:00) Harare,Pretoria</td>
</tr>
<tr>
<td>68</td>
<td>(GMT +2:00) Jerusalem</td>
</tr>
<tr>
<td>69</td>
<td>(GMT +2:00) Kaliningrad (RTZ 1)</td>
</tr>
<tr>
<td>70</td>
<td>(GMT +2:00) Tripoli</td>
</tr>
<tr>
<td>71</td>
<td>(GMT +3:00) Moscow</td>
</tr>
<tr>
<td>72</td>
<td>(GMT +3:00) St.Petersburg</td>
</tr>
<tr>
<td>73</td>
<td>(GMT +3:00) Volgograd (RTZ 2)</td>
</tr>
<tr>
<td>74</td>
<td>(GMT +3:00) Kuwait,Riyadh</td>
</tr>
<tr>
<td>75</td>
<td>(GMT +3:00) Nairobi</td>
</tr>
<tr>
<td>76</td>
<td>(GMT +3:00) Baghdad</td>
</tr>
<tr>
<td>77</td>
<td>(GMT +3:00) Minsk</td>
</tr>
<tr>
<td>78</td>
<td>(GMT +3:30) Tehran</td>
</tr>
<tr>
<td>79</td>
<td>(GMT +4:00) Abu Dhabi,Muscat</td>
</tr>
<tr>
<td>80</td>
<td>(GMT +4:00) Baku,Tbilisi</td>
</tr>
<tr>
<td>Permitted Value</td>
<td>Time Zone Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>81</td>
<td>(GMT +4:00) Izhevsk,Samara (RTZ 3)</td>
</tr>
<tr>
<td>82</td>
<td>(GMT +4:00) Port Louis</td>
</tr>
<tr>
<td>83</td>
<td>(GMT +4:00) Yerevan</td>
</tr>
<tr>
<td>84</td>
<td>(GMT +4:30) Kabul</td>
</tr>
<tr>
<td>85</td>
<td>(GMT +5:00) Yekaterinburg (RTZ 4)</td>
</tr>
<tr>
<td>86</td>
<td>(GMT +5:00) Islamabad</td>
</tr>
<tr>
<td>87</td>
<td>(GMT +5:00) Karachi</td>
</tr>
<tr>
<td>88</td>
<td>(GMT +5:00) Tashkent</td>
</tr>
<tr>
<td>89</td>
<td>(GMT +5:30) Mumbai,Chennai</td>
</tr>
<tr>
<td>90</td>
<td>(GMT +5:30) Kolkata,New Delhi</td>
</tr>
<tr>
<td>91</td>
<td>(GMT +5:30) Sri Jayawardenepura</td>
</tr>
<tr>
<td>92</td>
<td>(GMT +5:45) Kathmandu</td>
</tr>
<tr>
<td>93</td>
<td>(GMT +6:00) Astana,Dhaka</td>
</tr>
<tr>
<td>94</td>
<td>(GMT +6:00) Almaty</td>
</tr>
<tr>
<td>95</td>
<td>(GMT +6:00) Novosibirsk (RTZ 5)</td>
</tr>
<tr>
<td>96</td>
<td>(GMT +6:30) Yangon (Rangoon)</td>
</tr>
<tr>
<td>97</td>
<td>(GMT +7:00) Bangkok,Hanoi</td>
</tr>
<tr>
<td>98</td>
<td>(GMT +7:00) Jakarta</td>
</tr>
<tr>
<td>99</td>
<td>(GMT +7:00) Krasnoyarsk (RTZ 6)</td>
</tr>
<tr>
<td>100</td>
<td>(GMT +8:00) Beijing,Chongqing</td>
</tr>
<tr>
<td>101</td>
<td>(GMT +8:00) Hong Kong,Urumqi</td>
</tr>
<tr>
<td>102</td>
<td>(GMT +8:00) Kuala Lumpur</td>
</tr>
<tr>
<td>103</td>
<td>(GMT +8:00) Singapore</td>
</tr>
<tr>
<td>104</td>
<td>(GMT +8:00) Taipei,Perth</td>
</tr>
<tr>
<td>105</td>
<td>(GMT +8:00) Irkutsk (RTZ 7)</td>
</tr>
<tr>
<td>106</td>
<td>(GMT +8:00) Ulaanbaatar</td>
</tr>
<tr>
<td>107</td>
<td>(GMT +9:00) Tokyo,Seoul,Osaka</td>
</tr>
<tr>
<td>108</td>
<td>(GMT +9:00) Sapporo,Yakutsk (RTZ 8)</td>
</tr>
<tr>
<td>109</td>
<td>(GMT +9:30) Adelaide,Darwin</td>
</tr>
<tr>
<td>110</td>
<td>(GMT +10:00) Canberra</td>
</tr>
</tbody>
</table>
### Permitted Value

<table>
<thead>
<tr>
<th>Permitted Value</th>
<th>Time Zone Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>(GMT +10:00) Magadan (RTZ 9)</td>
</tr>
<tr>
<td>112</td>
<td>(GMT +10:00) Melbourne</td>
</tr>
<tr>
<td>113</td>
<td>(GMT +10:00) Sydney, Brisbane</td>
</tr>
<tr>
<td>114</td>
<td>(GMT +10:00) Hobart</td>
</tr>
<tr>
<td>115</td>
<td>(GMT +10:00) Vladivostok</td>
</tr>
<tr>
<td>116</td>
<td>(GMT +10:00) Guam, Port Moresby</td>
</tr>
<tr>
<td>117</td>
<td>(GMT +11:00) Solomon Islands</td>
</tr>
<tr>
<td>118</td>
<td>(GMT +11:00) New Caledonia</td>
</tr>
<tr>
<td>119</td>
<td>(GMT +11:00) Chokurdakh (RTZ 10)</td>
</tr>
<tr>
<td>120</td>
<td>(GMT +12:00) Fiji Islands</td>
</tr>
<tr>
<td>121</td>
<td>(GMT +12:00) Auckland, Anadyr</td>
</tr>
<tr>
<td>122</td>
<td>(GMT +12:00) Petropavlovsk-Kamchatsky (RTZ 11)</td>
</tr>
<tr>
<td>123</td>
<td>(GMT +12:00) Wellington</td>
</tr>
<tr>
<td>124</td>
<td>(GMT +12:00) Marshall Islands</td>
</tr>
<tr>
<td>125</td>
<td>(GMT +13:00) Nuku'alofa</td>
</tr>
<tr>
<td>126</td>
<td>(GMT +13:00) Samoa</td>
</tr>
</tbody>
</table>

### Time and Date

A clock and calendar display on the phones by default.

You can choose how to display the time and date for your time zone in several formats, or you can disable the display of the time and date. You can also 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.

To have the most accurate time, you have to synchronize the phone to the Simple Network Time Protocol (SNTP) time server. Until a successful SNTP response is received, the phone continuously flashes the time and date to indicate that they are not accurate.

The time and date display on the phones in PSTN mode and are set by an incoming call with a supported caller ID standard, or when the phone is connected to Ethernet and you enable the date and time display.

### Time and Date Display Parameters

Use the parameters in the following list to configure time and display options.

**up.localClockEnabled**

Specifies whether or not the date and time are shown on the idle display.

- 1 (Default) - Date and time are shown.
0 - Date and time are hidden.

**lcl.datetime.date.dateTop**
1 (default) - Displays the date above time.
0 - Displays the time above date.

**lcl.datetime.date.format**
The phone displays day and date. The field may contain 0, 1, or 2 commas which can occur only between characters and only one at a time.
For example: D,dM = Thursday, 3 July or Md,D = July 3, Thursday.
"D,dM" (default)
String

**lcl.datetime.date.longFormat**
1 (default) - Displays the day and month in long format (Friday/November).
0 - Displays the day and month in abbreviated format (Fri/Nov).

**lcl.datetime.time.24HourClock**
1 (default) - Displays the time in 24-hour clock mode.
0 - Displays the time in 12-hour clock mode.

**tcpIpApp.sntp.address**
Specifies the SNTP server address.
NULL (default)
Valid hostname or IP address.

**tcpIpApp.sntp.AQuery**
Specifies a query to return hostnames.
0 (default) - Queries to resolve the SNTP hostname are performed using DNS SRV.
1 - Query the hostname for a DNS A record.

**tcpIpApp.sntp.address.overrideDHCP**
0 (Default) - DHCP values for the SNTP server address are used.
1 - SNTP parameters override the DHCP values.

**tcpIpApp.sntp.daylightSavings.enable**
Enable or disable Daylight Savings Time rules to the displayed time.
1 (Default) - Enabled
0 - Disabled

tcpIpApp.sntp.daylightSavings.fixedDayEnable
0 (Default) - Month, date, and dayOfWeek are used in the DST calculation.
1 - Only month and date are used in the DST calculation.

tcpIpApp.sntp.daylightSavings.start.date
Start date for daylight savings time. Range is 1 to 31.
8 (Default) - Second occurrence in the month after DST starts.
0 - If fixedDayEnable is set to 0, this value specifies the occurrence of dayOfWeek when DST should start.
1 - If fixedDayEnable is set to 1, this value is the day of the month to start DST.
15 - Third occurrence.
22 - Fourth occurrence.
Example: If value is set to 15, DST starts on the third dayOfWeek of the month.

tcpIpApp.sntp.daylightSavings.start.dayOfWeek
Specifies the day of the week to start DST. This parameter is not used if fixedDayEnable is set to 1.
1 (Default) - Sunday
1-7 where the integer entered corresponds to a day of the week. For example, 1 = Sunday, 2 = Monday, and so on to 7 = Saturday.

tcpIpApp.sntp.daylightSavings.start.dayOfWeek.lastInMonth
0 (Default)
1 - DST starts on the last dayOfWeek of the month and the start.date is ignored.

Note: This parameter is not used if fixedDayEnable is set to 1.

tcpIpApp.sntp.daylightSavings.start.month
Specifies the month to start DST.
3 (Default) - March
1-12 where the integer entered corresponds to a month of the year. For example, 1 = January, 2 = February and so on to 12 = December.

tcpIpApp.sntp.daylightSavings.start.time
Specifies the time of day to start DST in 24-hour clock format. Range is 0 to 23.

2 (Default) - 2 a.m.

0 - 23 where the integer entered corresponds to the hour on in a 24 span. For example, 0 = 12 AM, 1 = 1 AM, and so on to 23 = 11 PM.

tcpIpApp.sntp.daylightSavings.stop.date

Specifies the stop date for daylight savings time. Range is 1 to 31.

1 (Default) - If fixedDayEnable is set to 1, the value of this parameter is the day of the month to stop DST. Set 1 for the first occurrence in the month.

0 - If fixedDayEnable is set to 0, this value specifies the dayOfWeek when DST should stop.

8 - Second occurrence.

15 - Third occurrence.

22 - Fourth occurrence.

Example: If set to 22, DST stops on the fourth dayOfWeek in the month.

tcpIpApp.sntp.daylightSavings.stop.dayOfWeek

Day of the week to stop DST.

1 (default) - Sunday

1-7 where the integer entered corresponds to a day of the week. For example, 1 = Sunday, 2 = Monday, and so on to 7 = Saturday.

Note: Parameter is not used if fixedDayEnable is set to 1.

tcpIpApp.sntp.daylightSavings.stop.dayOfWeek.lastInMonth

1 - DST stops on the last dayOfWeek of the month and the stop.date is ignored.

Parameter is not used if fixedDayEnable is set to 1.

tcpIpApp.sntp.daylightSavings.stop.month

Specifies the month to stop DST. Range is 1 to 12.

11 (Default) - November

1-12 where the integer entered corresponds to a month of the year. For example, 1 = January, 2 = February and so on to 12 = December.

tcpIpApp.sntp.daylightSavings.stop.time

Specifies the time of day to stop DST in 24-hour clock format. Range is 0 to 23.

2 (Default) - 2 a.m.
0 - 23 where the integer entered corresponds to the hour on in a 24 span. For example, 0 = 12 AM, 1 = 1 AM, and so on to 23 = 11 PM.

**tcpIpApp.sntp.gmtOffset**

Specifies the offset in seconds of the local time zone from GMT.

- 0 (Default) - GMT
- 3600 seconds = 1 hour
- -3600 seconds = -1 hour
- Positive or negative integer

**tcpIpApp.sntp.gmtOffset.cityID**

NULL (Default)

For descriptions of all values, refer to Time Zone Location Description.

- 0 - 127

**tcpIpApp.sntp.gmtOffset.overrideDHCP**

- 0 (Default) - The DHCP values for the GMT offset are used.
- 1 - The SNTP values for the GMT offset are used.

**tcpIpApp.sntp.resyncPeriod**

Specifies the period of time (in seconds) that passes before the phone resynchronizes with the SNTP server.

- 86400 (Default). 86400 seconds is 24 hours.
- Positive integer

**tcpIpApp.sntp.retryDnsPeriod**

Sets a retry period for DNS queries. The DNS retry period is affected by other DNS queries made on the phone. If the phone makes a query for another service during the retry period, such as SIP registration, and receives no response, the Network Time Protocol (NTP) DNS query is omitted to limit the retry attempts to the unresponsive server. If no other DNS attempts are made by other services, the retry period is not affected. If the DNS server becomes responsive to another service, NTP immediately retries the DNS query.

- 86400 (Default). 86400 seconds is 24 hours.
- 60 - 2147483647 seconds

**Related Links**

- [Time Zone Location Description](#) on page 206
Date Formats

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

<table>
<thead>
<tr>
<th>lcl.datetime.date.format</th>
<th>lcl.datetime.date.longformat</th>
<th>Date Displayed on Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>dM,D</td>
<td>0</td>
<td>19 Aug, Fri</td>
</tr>
<tr>
<td>dM,D</td>
<td>1</td>
<td>19 August, Friday</td>
</tr>
<tr>
<td>Md,D</td>
<td>0</td>
<td>Aug 19, Fri</td>
</tr>
<tr>
<td>Md,D</td>
<td>1</td>
<td>August 19, Friday</td>
</tr>
<tr>
<td>D,dM</td>
<td>0</td>
<td>Fri, 19 Aug</td>
</tr>
<tr>
<td>D,dM</td>
<td>1</td>
<td>Friday, August 19</td>
</tr>
<tr>
<td>DD/MM/YY</td>
<td>n/a</td>
<td>19/08/11</td>
</tr>
<tr>
<td>DD/MM/YYYY</td>
<td>n/a</td>
<td>19/08/2011</td>
</tr>
<tr>
<td>MM/DD/YY</td>
<td>n/a</td>
<td>08/19/11</td>
</tr>
<tr>
<td>MM/DD/YYYY</td>
<td>n/a</td>
<td>08/19/2011</td>
</tr>
<tr>
<td>YY/MM/DD</td>
<td>n/a</td>
<td>11/08/19</td>
</tr>
<tr>
<td>YYYY/MM/DD</td>
<td>n/a</td>
<td>2011/08/11</td>
</tr>
</tbody>
</table>

Phone Languages

All phones support the following languages: Arabic, Simplified Chinese, Traditional Chinese, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Norwegian, Polish, Brazilian Portuguese, Russian, Slovenian, International Spanish, and Swedish.

Each language is stored as a language file in the VVXLocalization folder, which is included with the Polycom UC Software package. If you want to edit the language files, you must use a Unicode-compatible XML editor such as XML Notepad 2007 and familiarize yourself with the guidelines on basic and extended character support.

At this time, the updater is available in English only.
Change the Phone Language and Keyboard Layouts

When you set the phone language and country, the phone uses the default keyboard layout for that language. For example, setting the phone language to French sets the phone to the AZERTY keyboard layout. You can enable multiple languages for the phone and switch between keyboard layouts.

Procedure

1. On the phone's keyboard, long-press and release the comma key and choose **Input Languages**.
2. Uncheck **Use System Language**.
3. Select one or more available languages and press the Back arrow. Each language you select is enabled along with its default keyboard layout.
   
   When you enable more than one language, a globe key displays on the phone keyboard.
4. Do one of the following:
   - Long-press the globe key to view and choose from a list of enabled languages. The phone uses the default keyboard layout for the language you choose.
   - Short-press the globe key to rotate through enabled languages. The space bar displays the current language and keyboard layout.

Phone Language Parameters

You can select the language that displays on the phone using the parameters in the following list.

**device.spProfile**

Set the default language that displays on the phone.

- NULL (default) - The default language is an empty string (lcl.ml.lang=""), which is English.
- DT - The default language is German (lcl.ml.lang="DTGerman_Germany").

**lcl.ml.lang**

Null (default) - Sets the phone language to US English.

String - Sets the phone language specified in the **lcl.ml.lang.menu.x.label** parameter.

**lcl.ml.lang.menu.x**

Specifies the dictionary files for the supported languages on the phone. Dictionary files must be sequential. The dictionary file cannot have capital letters, and the strings must exactly match a folder name of a dictionary file.

- Null (default)
- String

**lcl.ml.lang.menu.x.label**

Specifies the phone language menu label. The labels must be sequential.

- Null (default)
- String
Multilingual Parameters

The multilingual parameters included in the following list are based on string dictionary files downloaded from the provisioning server.

These files are encoded in XML format and include space for user-defined languages.

**lcl.ml.lang.charset**
- Provides the language character set.
- Null (default)
- String
- Change causes system to restart or reboot.

**lcl.ml.lang.clock.x.24HourClock**
- 1 (default) - Displays the time in 24-hour clock mode.
- 0 - Does not display the time in 24-hour clock mode.

*Note: Overrides the lcl.datetime.time.24HourClock parameter.*

**lcl.ml.lang.clock.x.dateTop**
- 1 (default) - Displays date above time.
- 0 - Displays date below time.

*Note: Overrides the lcl.datetime.date.dateTop parameter.*

**lcl.ml.lang.clock.x.format**
- "D,dM" (default)
- String
- The field may contain 0, 1 or 2 commas which can occur only between characters and only one at a time.
- For example: D,dM = Thursday, 3 July or Md,D = July 3, Thursday.

*Note: Overrides the lcl.datetime.date.format parameter to display the day and date.*

**lcl.ml.lang.clock.x.longFormat**
- 1 (default) - Displays the day and month in long format (Friday/November).
- 0 - Displays the day and month in abbreviated format (Fri/Nov).
Note: Overrides the lcl.datetime.date.longFormat parameter.

lcl.ml.lang.japanese.font.enabled
Enable or disable the use of Japanese kana format.
0 (default) - Disabled
1 - Enabled
Change causes system to restart or reboot.

lcl.ml.lang.list
Displays the list of languages supported on the phone.
All (default)
String
Change causes system to restart or reboot.

The basic character support includes the Unicode character ranges listed in the next table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0 Controls and Basic Latin</td>
<td>U+0000 - U+007F</td>
</tr>
<tr>
<td>C1 Controls and Latin-1 Supplement</td>
<td>U+0080 - U+00FF</td>
</tr>
<tr>
<td>Cyrillic (partial)</td>
<td>U+0400 - U+045F</td>
</tr>
</tbody>
</table>

Access the Country of Operation Menu in Set Language
You can view the list of countries listed in the Country of Operation menu in the language set by you on the phone.

If you set the system language as Deutsch (de-de), the list of countries under this menu will be displayed in German.

Procedure
» On the Poly Trio 8800 system Home screen, go to Settings > Advanced > Administration Settings > Network Configuration > network Interfaces > Wi-Fi Menu.

Add a Language for the Phone Display and Menu
Use the multilingual parameters to add a new language to your provisioning server directory to display on the phone screen and menu.
Procedure

1. Create a new dictionary file based on an existing one.
2. Change the strings making sure to encode the XML file in UTF-8 but also ensuring the UTF-8 characters chosen are within the Unicode character ranges indicated in the tables below.
3. Place the file in an appropriately named folder according to the format language_region parallel to the other dictionary files under the VVXLocalization folder on the provisioning server.
4. Add an lcl.ml.lang.clock.menu.x parameter to the configuration file.
5. Add lcl.ml.lang.clock.x.24HourClock, lcl.ml.lang.clock.x.format, lcl.ml.lang.clock.x.longFormat, and lcl.ml.lang.clock.x.dateTop parameters and set them according to the regional preferences.
6. (Optional) Set lcl.ml.lang to be the new language_region string.

Hide the MAC Address

You can configure the phone to hide MAC address on the phone’s display. When you enable this feature, users cannot view or retrieve the MAC address from the phone. The MAC address is available to administrators only.

Hide MAC Address Parameters

The following list includes parameters that configure the display of MAC address.

device.mac.hide.set

Enable or disable the device.mac.hide parameter to control the display of MAC address information of phones to users.

- Null (default)
- 0 – Disabled
- 1 – Enabled

device.mac.hide

- 0 (default) – MAC address displays.
- 1 – MAC address is hidden.

Unique Line Labels for Registration Lines

You can configure unique labels on line keys for registration lines.

You must configure multiple line keys on the phone for a registration in order to configure unique line labels. For example, you can set different names to display for the registration 4144 that displays on four line keys.

If you configure the line to display on multiple line keys without a unique label assigned to each line, the lines are labeled automatically in numeric order. For example, if you have four line keys for line 4144
labeled Polycom, the line keys are labeled as 1_Polycom, 2_Polycom, 3_Polycom, and 4_Polycom. This also applies to lines without labels.

**Unique Line Labels for Registration Lines Parameters**

When using this feature with the parameter `reg.x.label.y` where \( x = 2 \) or higher, multiple line keys display for the registered line address.

**reg.x.line.y.label**

Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when `up.cfgUniqueLineLabel=1`. If `reg.x.linekeys=1`, this parameter does not have any effect.

\( x \) = the registration index number starting from 1.

\( y \) = 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.

If no parameter value is set for `reg.x.line.y.label`, the phone automatically numbers multiple lines by prepending "<\( y \)>_" where \( y \) is the line index from 1 to the value set by `reg.x.linekeys`.

**up.cfgLabelElide**

Controls the alignment of the line label. By default when the line label is an alphanumeric or alphabetic string, the label aligns right. When the line label is a numeric string, the label aligns left.

None (Default)

Right

Left

**up.cfgUniqueLineLabel**

Allow unique labels for a registration that is split across multiple line keys using `reg.X.linekeys`.

0 (Default) - Use the same label on all line keys.

1 - Display a unique label as defined by `reg.X.line.Y.label`.

If `reg.X.line.Y.label` is not configured, then a label of the form `<integer>_<` will be applied in front of the applied label automatically.
Poly Trio System Number Formatting

By default, phone numbers entered on the system are automatically formatted with dashes between dialed numbers following the North American Numbering Plan (NANP), for example: 122333444 displays as 1-222-333-444.

Poly Trio System Number Formatting Parameters

Use the following parameter to enable or disable number formatting.

up.formatPhoneNumbers

1 (default) - Enable automatic number formatting.
0 - Disable automatic number formatting.

Number or Custom Label

On Poly Trio systems you can choose to display a number, an extension, or a custom label on the Home Screen below the time and date.

Configure the Number or Label from the System

You can configure the display of the number or label on the Home screen from the system menu.

Procedure

» Navigate to Settings > Advanced > Administration Settings > Home Screen Label.

Number and Label Parameters

You can configure display of the Poly Trio number or label on the Home screen using centralized provisioning parameters.

homeScreen.placeACall.enable

1 (default) - Specify Place a Call label to display on the home screen.
0 - Does not display the label on the home screen.

homeScreen.customLabel

Specify the label to display on the phone's Home screen when homeScreen.labelType="Custom". The label can be 0 to 255 characters.

Null (default)

homeScreen.labelLocation
Specify where the label displays on the screen.

StatusBar (default) - The phone displays the custom label in the status bar at the top of the screen.

BelowDate - The phone displays the custom label on the Home screen only, just below the time and date.

**homeScreen.labelType**

Specify the type of label to display on the phone’s Home screen.

PhoneNumber (default)

- When the phone is set to use Lync Base Profile, the phone number is derived from the Skype for Business server.
- When the phone is set to use the Generic Base Profile, the phone uses the number you specify in reg.1.address.

Custom - Enter an alphanumeric string between 0 and 255 characters.

PrimaryPhoneNumber – The status bar displays only the first phone number rather than all of the phone numbers.

None - Don't display a label.

**reg.1.useteluriAsLineLabel**

1 - If `reg.x.label="Null"` the tel URI/phone number/address displays as the label of the line key.

0 - If `reg.x.label="Null"` the value for `reg.x.displayName`, if available, displays as the label. If `reg.x.displayName` is unavailable, the user part of `reg.x.address` is used.

**up.formatPhoneNumbers**

1 (default) - Enables automatic number formatting.

0 - Disables automatic number formatting and numbers display separated by "-".

---

**Custom Icons for Contacts and Line Registrations**

You can configure Poly Trio systems to display custom icons for registered lines and user photos for contacts in the Local Contact Directory and favorites on the Home screen.

Poly recommends uploading PNG images that are 106 x 106 pixels with a size of 100 KB or smaller. The maximum image size you can upload is 200 x 200 pixels, however, the phone automatically scales the icons to 106 x 106 pixels. You can configure up to 24 icons for registered lines and contacts on the Poly Trio system.

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 Polycom UC Software do not violate any Intellectual Property rights.

Custom Icon Parameters

Use the following parameters to configure custom icons for favorite contacts and line registrations.

icons.x

Specify the icon filename or URL location associated with the registered line (x), where x equals 1-24. The icons display on the phone for lines configured using parameter \texttt{reg.y.icon} or favorite contacts set for <up></up> in the \texttt{Mac-directory.xml} file.

Null (default)
icon file name or URL location

For example: \texttt{icons.1="filename1" or icons.x="ftp://icons:icons@10.233.234.18/icon1.png"}
Change causes system to restart or reboot.

reg.y.icon

Assign an icon specified in \texttt{icons.x} to this registered line (y), where y equals 1-24.

Null
iconX, where x is 1-24

For example, if \texttt{icons.1="filename1" then reg.1.icon="icon1".}

Change causes system to restart or reboot.

Example: Configure an Icon for a Line Registration

Use the following example to set icons for two line registrations.

Procedure

1. Copy icons to your provisioning or FTP server.
2. Configure the following parameters:
   - \texttt{reg.1.address="7756638509"}
   - \texttt{reg.2.address="7756638708"}
   - \texttt{icons.1="blue.png"}
   - \texttt{icons.2="green.png"}
   - \texttt{reg.1.icon="icon1"}
   - \texttt{reg.2.icon="icon2"}
Example: Set Icons for Speed Dial Contacts

Use the following example to set icons as user photos for contacts set as speed dials.

Procedure
1. Copy the icons to the provisioning or FTP server.
2. Configure the following parameters:
   - icons.3="help.png"
   - icons.4="reception.png"
3. In the MAC-Directory.xml file, configure the speed dial contacts and icons.

```
<item>
  <fn>Help</fn>
  <ln>Desk</ln>
  <ct>1234567890</ct>
  <sd>1</sd>
  <up>3</up>
</item>
<item>
  <fn>Front</fn>
  <ln>Reception</ln>
  <ct>1234567899</ct>
  <sd>2</sd>
  <up>4</up>
</item>
```

Related Links
Parameter Elements for the Local Contact Directory on page 234

Capture Your Device's Current Screen

You can capture your phone current screen.

Before you can take a screen capture, you must provide power and connect the expansion module to a phone, and enable the phone's web server using the parameter httpd.enabled.

Procedure
1. Add the parameter up.screenCapture.enabled to your configuration.
2. Set the value to 1 and save.
3. On the device, go to Settings > Basic > Preferences > Screen Capture.
   Note you must repeat step 3 each time the device restarts or reboots.
4. Locate and record the phone's IP address at Status > Platform > Phone > IP Address.
5. Set the phone to the screen you want to capture.
6. In a web browser address field, enter https://<phoneIPaddress>/captureScreen where <phoneIPaddress> is the IP address you obtained in step 5.
   The web browser displays an image showing the phone's current screen. You can save the image as a BMP or JPEG file.
Capture Current Phone Screen Parameters

User the following parameters to get a screen capture of the current screen on your phone.

\texttt{up.screenCapture.enabled}

- 0 (Default) - The Screen Capture menu is hidden on the phone.
- 1 - The Screen Capture menu displays on the phone.

When the phone reboots, screen captures are disabled from the Screen Capture menu on the phone.
Change causes system to restart or reboot.

\texttt{up.screenCapture.allowed}

- 0 (Default) - The Screen Capture feature is disabled.
- 1 - The Screen Capture feature is enabled.

Default In-Call Screen

You can select the default screen that displays when your Poly Trio system is in a call.
For calls between two parties, you can display call controls or the dial pad. For conference calls (calls with more than two parties), you can display call controls or the roster view. You can also configure the default screen display for registered lines.

Default In-Call Screen Parameters

Use the following parameters to configure the default screens while the Poly Trio system is in a call.

\texttt{up.callStateView}

- Set the default screen while in a call.
- Drawer (default) – Displays the in-call controls.
- Dialpad – Displays the dial pad.

Note that \texttt{reg.X.callStateView} can override this setting.

\texttt{up.callStateView.conference}

- Set the default screen while in a conference call.
- Roster (default) – Displays the roster view.
- Drawer – Displays the in-call controls.

Note that \texttt{reg.X.callStateView.conference} can override this setting.

\texttt{reg.X.callStateView}
Set the default screen while in a call with registered line x. During the call, this parameter overrides the setting for `up.callStateView` if it's set to anything other than `Default`.

- **Drawer** – Displays the in-call controls.
- **Dialpad** – Displays the dial pad.
- **Default (default)** – Uses the `up.callStateView` setting.

### `reg.X.callStateView.conference`

Set the default screen while in a conference call with registered line x. During the call, this parameter overrides the setting for `up.callStateView.conference` if it's set to anything other than `Default`.

- **Poly Trio systems** can bridge multiple ecosystems for conference calls; in these cases, the lowest involved line determines which screen displays.
- **Roster** – Displays the roster view.
- **Dialpad** – Displays the dial pad.
- **Default (default)** – Uses the `up.callStateView.conference` setting.

### Custom Call Control Options

You can remove the **Transfer** and **Mute** options from the call control menu to free up space onscreen in the call control menu for other options.

If you remove these options from the call control menu, the **Transfer** option in the global menu is still available to use, and users can use the Mute buttons on the Poly Trio system to mute the call.

### Custom Call Control Options Parameters

Use the following parameters to customize the call control menu.

#### `up.callStateView.controlRelegation.transfer`

- **0 (Default)** – The **Transfer** option is available in the call control menu.
- **1** – The **Transfer** option is not available in the call control menu.

  Change causes the system to restart or reboot.

#### `up.callStateView.controlRelegation.mute`

- **0 (Default)** – The **Mute** option is available in the call control menu.
- **1** – The **Mute** option is not available in the call control menu.

  Change causes the system to restart or reboot.
Poly Trio Home Screen Parameters

Use the following parameters to configure the phone's Home screen display.

**homeScreen.application.enable**
1 (default) - Enable display of the Applications icon on the phone Home screen.
0 - Enable display of the Applications icon on the phone Home screen.

**homeScreen.calendar.enable**
1 (default) - Enable display of the Calendar icon on the phone Home screen.
0 - Disable display of the Calendar icon on the phone Home screen.

**homeScreen.contacts.enable**
1 (default) - The Contacts icon displays on the Home screen.
0 - The Contacts icon does not display on the Home screen.

**homeScreen.diagnostics.enable**
0 (default) - A Diagnostics icon does not show on the Home screen.
1 - A Diagnostics icon shows on the Home screen to provide quick access to the Diagnostics menu.

**homeScreen.directories.enable**
1 (default) - Enable display of the Directories menu icon on the phone Home screen.
0 - Disable display of the Directories menu icon on the phone Home screen.

**homeScreen.doNotDisturb.enable**
0 (default) - Disable display of the DND icon on the phone Home screen.
1 - Enable display of the DND icon on the phone Home screen.

**homeScreen.forward.enable**
1 (default) - Enable display of the call forward icon on the phone Home screen.
0 - Disable display of the call forward icon on the phone Home screen.

**homeScreen.messages.enable**
1 (default) - Enable display of the Messages menu icon on the phone Home screen.
0 - Disable display of the Messages menu icon on the phone Home screen.
**homeScreen.newCall.enable**

1 (default) - Enable display of the New Call icon on the phone Home screen.
0 - Disable display of the New Call icon on the phone Home screen.

**homeScreen.present.enable**

Control whether the Content icon displays on the Polycom Trio system Home screen when Content Sharing is enabled and the system is paired with a Polycom Trio Visual+, Trio VisualPro, or RealPresence Group Series system.

1 (default)
0

**homeScreen.redial.enable**

0 (default) - Disable display of the Redial menu icon on the phone Home screen.
1 - Enable display of the Redial menu icon on the phone Home screen.

**homeScreen.settings.enable**

1 (default) - Enable display of the Settings menu icon on the phone Home screen.
0 - Disable display of the Settings menu icon on the phone Home screen.

**softkey.feature.redial**

1 (default) - Displays the Redial softkey on the Home screen of the Poly Trio 8300 system.
0 - The Redial softkey doesn't display on the Home screen.
Directories and Contacts

Topics:

• Local Contact Directory
• Speed Dials on Poly Trio Systems
• Corporate Directory
• Call Lists
• Resetting Contacts and Recent Calls Lists on Poly Trio System

You can configure phones with a local contact directory and link contacts to speed dial buttons. Additionally, call logs stored in the Missed Calls, Received Calls, and Placed Calls call lists let you view user phone events like remote party identification, time and date of call, and call duration. This section provides information on contact directory, speed dial, and call log parameters you can configure on your phone.

Local Contact Directory

Poly phones feature a contact directory file you can use to store frequently used contacts.

The UC Software package includes a template contact directory file named 000000000000-directory~.xml that is loaded to the provisioning server the first time you boot up a phone with UC Software or when you reset the phone to factory default settings.

When you first boot the phone out of the box or when you reset the phone to factory default settings, 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.

In addition, make sure the dir.local.readonly parameter is enabled to restrict the users to modify speed dials.

Local Contact Directory Parameters

The following parameters configure the local contact directory.

contactPhotoIntegration.hideMyPhoto

Don't show the signed-in user's photo on the line key but still show other users' photos.

0 (Default) - Disable the Hide My Photo feature
1 - Enable the Hide My Photo feature

dir.local.contacts.maxNum
Set the maximum number of contacts that can be stored in the Local Contact Directory. The maximum number varies by phone model, refer to section 'Maximum Capacity of the Local Contact Directory'.

- 2000 (default)
- Maximum 3000 contacts

Change causes system to restart or reboot.

**dir.local.readonly**

- 0 (default) - Disable read only protection of the local Contact Directory.
- 1 - Enable read-only protection of the local Contact Directory.

**feature.directory.enabled**

- 0 - The local contact directory is disabled when the Poly Trio solution Base Profile is set to Lync.
- 1 (default)- The local directory is enabled when the Poly Trio solution Base Profile is set to Lync.

**dir.search.field**

Specify whether to sort contact directory searches by first name or last name.

- 0 (default) - Last name.
- 1 - First name.

**voIPProt.SIP.specialEvent.checkSync.downloadDirectory**

- 0 (default) - The phone downloads updated directory files after receiving a checksync NOTIFY message.
- 1 - The phone downloads the updated directory files along with any software and configuration updates after receiving a checksync NOTIFY message. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates.

*Note:* The parameter `hotelingMode.type` set to 2 or 3 overrides this parameter.

**dir.local.passwordProtected**

Specify whether you are prompted for an Admin/User password when adding, editing, or deleting contacts in the Contact Directory.

- 0 - Disabled (default)
- 1 - Enabled

**feature.pauseAndWaitDigitEntryControl.enabled**

- 1 (default) - Enable processing of control characters in the contact phone number field. When enabled, "," or "p" control characters cause a one second pause.
For example, "," or "p" control characters cause a one second pause. ";" or "w" control character cause a user prompt that allows a user-controlled wait. Subsequent digits entered to the contact field are dialed automatically.

0 - Disable processing of control characters.

**up.regOnPhone**

0 (default) – Contacts you assign to a line key display on the phone in the position assigned.
1 – Contacts you assign to a line key are pushed to the attached expansion module.

Change causes system to restart or reboot.

### Maximum Capacity of the Local Contact Directory on Poly Trio

The following table lists the maximum number of contacts and maximum file size of the local Contact Directory for each phone.

To conserve phone memory, use the parameter `dir.local.contacts.maxNum` to set a lower maximum number of contacts for the phones.

<table>
<thead>
<tr>
<th>Phone</th>
<th>Maximum File Size</th>
<th>Maximum Number of Contacts in File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio 8300</td>
<td>4MB</td>
<td>3000</td>
</tr>
<tr>
<td>Poly Trio 8500</td>
<td>4MB</td>
<td>3000</td>
</tr>
<tr>
<td>Poly Trio 8800</td>
<td>4MB</td>
<td>3000</td>
</tr>
</tbody>
</table>

### Creating Per-Phone Directory Files

To create a per-phone, personal directory file, replace `<000000000000>` in the global file name with the phone's MAC address: `<MACaddress>-directory.xml`.

Any changes users make to the contact directory from the phone are stored on the phone drive and uploaded to the provisioning server in the personal directory (`<MACaddress>-directory.xml`) file, which enables you to preserve a contact directory during reboots.

To create a global directory file that you can use to maintain the directory for all phones from the provisioning server, remove the tilde (~) from the template file name `000000000000-directory.xml`. When you update the global directory file on the provisioning server, the updates are downloaded onto the phone and combined with the phone specific directory.

### Maintaining Per-Phone Directory Files

Using the parameter `voIpProt.SIP.specialEvent.checkSync.downloadDirectory`, you can configure the phones to download updated directory files. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates.

Any changes to either the global or personal directory files are reflected in the directory on the phone after a restarts. When merging the two files, the personal directory always takes precedence over the
changes in the global directory. Thus, if a user modifies a contact from the global directory, the contact is
saved in the personal directory file, and the contact from the global directory is ignored when the files are
next uploaded.

The phone requests both the per-phone <MACaddress>-directory.xml and global contact directory
000000000000-directory.xml files and merges them for presentation to the user. If you created a per-
phone <MACaddress>-directory.xml file for a phone, and you want to use the 000000000000-directory.xml
file, add the 000000000000-directory.xml file to the provisioning server and update the phone’s
configuration.

**Note:** You can duplicate contacts in the Contact Directory on phones registered with the Ribbon
Communications server.

**Note:** To avoid users accidentally deleting the definitions in the contact directory, make the contact
directory file read only.

## Local Contact Directory File Size Parameters

Use the following parameters to set the size of the local contact directory.

The maximum local directory size is limited based on the amount of flash memory in the phone and varies
by phone model. Poly recommends that you configure a provisioning server that allows uploads to ensure
a back-up copy of the directory when the phone reboots or loses power.

**dir.local.nonVolatile.maxSize**

Set the maximum file size of the local contact directory stored on the phone’s non-volatile
memory.

1 - 100KB

**dir.local.volatile**

0 (default) - The phone uses non-volatile memory for the local contact directory.

1 - Enables the use of volatile memory for the local contact directory.

**dir.local.volatile.maxSize**

Sets the maximum file size of the local contact directory stored on the phone’s volatile memory.

1 - 200KB
Parameter Elements for the Local Contact Directory

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

**Local Contact Directory Parameter Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
<th>Permitted Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>fn</td>
<td>The contact's first name.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>ln</td>
<td>The contact's last name.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>ct</td>
<td>Contact, Used by the phone to address a remote party in the same way that a string of digits or a SIP URL are dialed manually by the user. This element is also used to associate incoming callers with a particular directory entry. The maximum field length is 128 characters. Note: This field cannot be null or duplicated.</td>
<td>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</td>
</tr>
<tr>
<td>sd</td>
<td>Speed Dial Index, Associates a particular entry with a speed dial key for one-touch dialing or dialing.</td>
<td>20</td>
</tr>
<tr>
<td>lb</td>
<td>The label for the contact. The label of a contact directory item is by default the label attribute of the item. If the label attribute does not exist or is Null, then the first and last names form the label. A space is added between first and last names.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>Element</td>
<td>Definition</td>
<td>Permitted Values</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>pt</td>
<td>Protocol, The protocol to use when placing a call to this contact.</td>
<td>SIP, H323, or Unspecified</td>
</tr>
<tr>
<td>rt</td>
<td>Ring Tone, When incoming calls match a directory entry, this field specifies the ringtone to be used.</td>
<td>Null, 1 to 21</td>
</tr>
<tr>
<td>dc</td>
<td>Divert Contact, The address to forward calls to if the Auto Divert feature is enabled.</td>
<td>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</td>
</tr>
<tr>
<td>ad</td>
<td>Auto Divert, If set to 1, callers that match the directory entry are diverted to the address specified for the divert contact element. Note: If auto-divert is enabled, it has precedence over auto-reject.</td>
<td>0 or 1</td>
</tr>
<tr>
<td>ar</td>
<td>Auto Reject, If set to 1, callers that match the directory entry specified for the auto reject element are rejected. Note: If auto divert is also enabled, it has precedence over auto reject.</td>
<td>0 or 1</td>
</tr>
<tr>
<td>bw</td>
<td>Buddy Watching, If set to 1, this contact is added to the list of watched phones.</td>
<td>0 or 1</td>
</tr>
</tbody>
</table>
### Element Definitions

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
<th>Permitted Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bb</strong></td>
<td>Buddy Block, If set to 1, this contact is blocked from watching this phone.</td>
<td>0 or 1</td>
</tr>
<tr>
<td><strong>up</strong></td>
<td>User Photo The contact's photo icon.</td>
<td>1-24</td>
</tr>
</tbody>
</table>

### Related Links

- [Example: Set Icons for Speed Dial Contacts](#) on page 225

### Speed Dials on Poly Trio Systems

You can link entries in the local contact directory to speed dial contacts to line keys on the Home screen to enable users to place calls quickly using dedicated speed dial buttons.

The number of supported speed dial entries varies by phone model.

#### Speed Dial Index Ranges

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Trio 8300</td>
<td>1 - 20</td>
</tr>
<tr>
<td>Poly Trio 8500</td>
<td>1 - 20</td>
</tr>
<tr>
<td>Poly Trio 8800</td>
<td>1 - 20</td>
</tr>
</tbody>
</table>

### Speed Dial Contacts Parameters

After setting up your per-phone directory file (<MACaddress>-directory.xml), enter a number in the speed dial `<sd>` field to display a contact directory entry as a speed dial contact on the phone. Speed dial entries automatically display on unused line keys on the phone and are assigned in numerical order.

On some call servers, enabling presence for an active speed dial contact displays that contact's status on the speed dial’s line key label.

Use the parameter below, which identifies the directory XML file and the parameters you need to set up your speed dial contacts.

**dir.local.contacts.maxFavIx**

Configure the maximum number of speed dial contacts that can display on the Poly Trio Home screen.
Enter a speed dial index number in the `<sd>` element in the `<MAC address>`-directory.xml file to display a contact directory entry as a speed dial key on the phone. Speed dial contacts are assigned to unused line keys and to entries in the phone’s speed dial list in numerical order.

**Corporate Directory**

You can connect phones to a corporate directory server that supports the Lightweight Directory Access Protocol (LDAP), version 3.

After you set up the corporate directory on the phones, users can search for contacts in the directory, place calls to directory contacts, and save entries to the local contact directory on the phone.

Poly phones support corporate directories that support server-side sorting and those that do not. For servers that do not support server-side sorting, sorting is performed on the phone.

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

**Corporate Directory Parameters**

Use the parameters in the following list to configure the corporate directory.

Note that the exact configuration of a corporate directory depends on the LDAP server you use.

**Note:** For detailed explanations and examples of all currently supported LDAP directories, see Technical Bulletin 41137: Best Practices When Using Corporate Directory on Polycom Phones at Polycom Engineering Advisories and Technical Notifications.

**dir.corp.address**

Set the IP address or hostname of the LDAP server interface to the corporate directory.

Null (default)
IP address
Hostname
FQDN

Change causes system to restart or reboot.

**dir.corp.allowCredentialsFromUI.enabled**

Enable or disable prompting users to enter LDAP credentials on the phone when accessing the Corporate Directory.
Note: Users are only prompted to enter their credentials when credentials are not added through configuration or after a login failure.

0 (default) – Disabled
1 – Enabled

dir.corp.alt.protocol
Set a directory protocol used to communicate to the corporate directory.
sopi (default)
UTF-8 encoding string

dir.corp.alt.transport
Choose a transport protocol used to communicate to the corporate directory.
TCP (default)
TLS

dir.corp.attribute.x.addstar
Determine if the wild-card character, asterisk(*), is appended to the LDAP query field.
0 - Wild-card character is not appended.
1 (default) - Wild-card character is appended.
Change causes system to restart or reboot.

dir.corp.attribute.x.filter
Set the filter string for this parameter, which is edited when searching.
Null (default)
UTF-8 encoding string
Change causes system to restart or reboot.

dir.corp.attribute.x.label
Enter the label that shows when data is displayed.
Null (default)
UTF-8 encoding string
Change causes system to restart or reboot.

dir.corp.attribute.x.name
Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8).

Null (default)
UTF-8 encoding string
Change causes system to restart or reboot.

**dir.corp.attribute.x.searchable**

Determine whether quick search on parameter x (if x is 2 or more) is enabled or disabled.

0 (default) - Disabled
1 - Enabled
Change causes system to restart or reboot.

**dir.corp.attribute.x.sticky**

Sets whether the filter string criteria for attribute x is reset or retained after a phone reboot. If you set an attribute to be sticky (set this parameter to 1), a "*" displays before the label of the attribute on the phone.

0 (default) – Reset after a phone reboot.
1 – Retain after a phone reboot.
Change causes system to restart or reboot.

**dir.corp.attribute.x.type**

Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. If the user saves the entry to the local contact directory on the phone, first_name, last_name, and phone_number are copied. The user can place a call to the phone_number and SIP_address from the global address book directory.

first_name
last_name (default)
phone_number
SIP_address
H323_address URL
other
Change causes system to restart or reboot.

**dir.corp.auth.useLoginCredentials**

0 (default)
1
**dir.corp.autoQuerySubmitTimeout**
Set the timeout in seconds between when the user stops entering characters in the quick search and when the search query is automatically submitted.
- 0 (default)
- 0 - 60
Change causes system to restart or reboot.

**dir.corp.backGroundSync**
Determine if background downloading from the LDAP server is enabled or disabled.
- 0 (default) - Disabled
- 1 - Enabled
Change causes system to restart or reboot.

**dir.corp.backGroundSync.period**
Set the time in seconds the corporate directory cache is refreshed after the corporate directory feature has not been used for the specified period of time.
- 86400 (default)
- 3600 to 604800
Change causes system to restart or reboot.

**dir.corp.baseDN**
Enter the base domain name, which is the starting point for making queries on the LDAP server.
- Null (default)
- UTF-8 encoding string
Change causes system to restart or reboot.

**dir.corp.bindOnInit**
Enable or disabled use of bind authentication on initialization.
- 1 (default) - Enabled
- 0 - Disabled
Change causes system to restart or reboot.

**dir.corp.cacheSize**
Set the maximum number of entries that can be cached locally on the phone.
- 128 (default)
- 32 to 256
Change causes system to restart or reboot.
**dir.corp.customError**

Enter the error message to display on the phone when the LDAP server finds an error.

Null (default)

UTF-8 encoding string

**dir.corp.domain**

Enter the port that connects to the server if a full URL is not provided.

0 to 255

**dir.corp.filterPrefix**

Enter the predefined filter string for search queries.

(objectclass=person) (default)

UTF-8 encoding string

Change causes system to restart or reboot.

**dir.corp.pageSize**

Set the maximum number of entries requested from the corporate directory server with each query.

32 (default)

8 to 32

Change causes system to restart or reboot.

**dir.corp.password**

Enter the password used to authenticate to the LDAP server.

Null (default)

UTF-8 encoding string

**dir.corp.persistentCredentials**

Enable to securely store and encrypt LDAP directory user credentials on the phone. Enable dir.corp.allowCredentialsFromUI.enabled to allow users to enter credentials on the phone.

Note: If you disable the feature after enabling it, then all the saved user credentials are deleted.

0 (default) - Disabled

1 - Enabled
**dir.corp.port**

Enter the port that connects to the server if a full URL is not provided.

389 (default for TCP)
636 (default for TLS)
0
Null
1 to 65535
Change causes system to restart or reboot.

**dir.corp.querySupportedControlOnInit**

Enable to make the phone make an initial query to check the status of the server when booting up.

0 - Disabled
1 (default) - Enabled

**dir.corp.scope**

sub (default) – a recursive search of all levels below the base domain name is performed.
one – a search of one level below the base domain name is performed.
base – a search at the base domain name level is performed.
Change causes system to restart or reboot.

**dir.corp.serverSortNotSupported**

0 (default) – The server supports server-side sorting.
1 – The server does not support server-side sorting, so the phone handles the sorting.

**dir.corp.sortControl**

Determine how a client can make queries and sort entries.

0 (default) – Leave sorting as negotiated between the client and server.
1 – Force sorting of queries, which causes excessive LDAP queries and should only be used to diagnose LDAP servers with sorting problems.
Change causes system to restart or reboot.

**dir.corp.transport**

Specify whether a TCP or TLS connection is made with the server if a full URL is not provided.

TCP (default)
TLS
Null
Change causes system to restart or reboot.

`dir.corp.user`

Enter the user name used to authenticate to the LDAP server.

- Null (default)
- UTF-8 encoding string

`dir.corp.viewPersistence`

- 0 (default) – The corporate directory search filters and browsing position are reset each time the user accesses the corporate directory.
- 1 – The search filters and browsing position from the previous session are displayed each time the user accesses the corporate directory.

Change causes system to restart or reboot.

`dir.corp.vlv.allow`

Determine whether virtual view list (VLV) queries are enabled and can be made if the LDAP server supports VLV.

- 0 (default)
- 1

Change causes system to restart or reboot.

`dir.corp.vlv.sortOrder`

Enter the list of parameters, in exact order, for the LDAP server to use when indexing. For example: `sn, givenName, telephoneNumber`.

- Null (default)
- list of parameters

Change causes system to restart or reboot.

`feature.contacts.enabled`

- 1 (default) - The Contacts icon displays on the Home screen, the global menu, and in the dialer.
- 0 - Disable display of the Contacts icon.

`feature.corporateDirectory.enabled`

- 0 (default) - The corporate directory feature is disabled and the icon is hidden.
- 1 (default) - The corporate directory is enabled and the icon shows.
**Call Lists**

The phone records and maintains user phone events to a call list, which contains call information such as remote party identification, time and date of the call, and call duration.

The list is stored on the provisioning server as an XML file named `<MACaddress>-calls.xml`. If you want to route the call lists to another server, use the `CALL_LISTS_DIRECTORY` field in the master configuration file. All call lists are enabled by default.

The phones automatically maintain the call lists in three separate call lists that users can access: Missed Calls, Received Calls, and Placed Calls. Users can clear lists manually on their phones, or delete individual records or all records in a group (for example, all missed calls).

**Call List Parameters**

Use the following parameters to configure call lists.

**callLists.collapseDuplicates**
- **Lync Base Profile** – 0 (default)
- **Generic Base Profile** – 1 (default)

1 – Consecutive incomplete calls to/from the same party and in the same direction are collapsed into one record in the calls list. The collapsed entry displays the number of consecutive calls.

0 – Each call is listed individually in the calls list.

**callLists.logConsultationCalls**
- **Lync Base Profile** – 1 (default)
- **Generic Base Profile** – 1 (default)

0 – Consultation calls not joined into a conference call are not listed as separate calls in the calls list.

1 – Each consultation calls is listed individually in the calls list.

**feature.callList.enabled**
- 1 (default) - Allows you to enable the missed, placed, and received call lists on all phone menus including the Home screen and dial pad.

0 - Disables all call lists.

Hiding call lists from the Home screen and dial pad requires UCS 5.4.2 RevAA or higher.

**feature.callListMissed.enabled**
- 0 (Default) - The missed call list is disabled.

1 - The missed call list is enabled.
To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

**feature.callListPlaced.enabled**

0 (Default) - The placed call list is disabled.
1 - The placed call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

**feature.callListReceived.enabled**

0 (Default) - The received call list is disabled.
1 - The received call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

**feature.exchangeCallLog.enabled**

If Base Profile is:
Generic - 0 (default)
Skype for Business - 1 (default)
1 - The Exchange call log feature is enabled, user call logs are synchronized with the server, and the user call history of Missed, Received, and outgoing calls can be retrieved on the phone.

You must also enable the parameter `feature.callList.enabled` to use the Exchange call list feature.

0 - The Exchange call list feature is disabled, the user call list history cannot be retrieved from the Exchange server, and the phone generates call lists locally.

**Call Log Elements and Attributes**

The following table describes each element and attribute that displays in the call log.
You can place the elements and attributes in any order in your configuration file.

<table>
<thead>
<tr>
<th>Call Log Elements and Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
</tr>
<tr>
<td><strong>direction</strong></td>
</tr>
<tr>
<td>Call direction with respect to the user.</td>
</tr>
<tr>
<td><strong>disposition</strong></td>
</tr>
<tr>
<td>Element</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>line</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>protocol</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>startTime</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>duration</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>count</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>destination</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>source</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Connection</td>
</tr>
<tr>
<td>Element</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>An array of connected parties in chronological order.</td>
</tr>
<tr>
<td>As a call progresses, the connected party at the far end may change, for example, if the far end transfers the call to someone else. The connected element allows the progression of connected parties, when known, to be saved for later use. All calls that contain a connected state must have at least one connection element created.</td>
</tr>
<tr>
<td>finalDestination</td>
</tr>
<tr>
<td>The final connected party of a call that has been forwarded or transferred to a third party.</td>
</tr>
</tbody>
</table>

**Resetting Contacts and Recent Calls Lists on Poly Trio System**

You can reset the Contacts list and Recent call lists stored locally on the Poly Trio systems to their default settings.

**Procedure**

1. On the phone, go to Setting > Advanced.
2. Enter the administrative password (default 456).
3. Select Reset to defaults > Reset User Data.
4. When prompted “Are you sure?”, select Yes.
Call Controls

Topics:

• Microphone Mute
• Persistent Microphone Mute
• Answer Incoming Calls with Mute Button
• Call Timer
• Called Party Identification
• Connected Party Identification
• Calling Party Identification
• Remote Party Caller ID from SIP Messages
• Calling Line Identification
• SIP Header Warnings
• Distinctive Call Waiting
• Do Not Disturb
• Remote Party Disconnect Alert Tone
• Call Waiting Alerts
• Missed Call Notifications
• Call Hold
• Call Transfer
• Call Forwarding
• Automatic Off-Hook Call Placement
• Multiple Line Keys Per Registration
• Multiple Call Appearances
• Bridged Line Appearance
• Voicemail
• Local Call Recording
• Local and Centralized Conference Calls on Poly Trio
• Conference Meeting Dial-In Options
• Hybrid Line Registration
• Local Digit Map
• Enhanced 911 (E.911)
• Multilevel Precedence and Preemption (MLPP) for Assured Services - Session Initiation Protocol (AS-SIP)
• International Dialing Prefix
This chapter shows you how to configure call control features.

**Microphone Mute**

All phones have a microphone mute button.

By default, when you activate microphone mute, a red LED glows or a mute icon displays on the phone screen, depending on the phone model you are using.

You cannot configure the microphone mute feature.

However, you can configure Poly Trio systems to play an audible tone when the mute status of the device is changed either from any of the mute buttons of the system (device and any connected devices) or far-end system (remote mute). This allows you to know if the system microphones are in a mute or un-mute state. In addition, you can set a periodic reminder which plays a tone periodically when the phone is in the mute state. The time interval can be set using configuration parameter and the value must not be less than 5 seconds.

**Microphone Mute Parameters**

The following parameters configure microphone mute status alert tones.

- **se.touchFeedback.enabled**
  - 0 - Does not play an alert tone when the mute status is changed on the Poly Trio system.
  - 1 - An alert tone is played when the mute status is changed either from the Poly Trio or far-end system.

- **call.mute.reminder.period**
  - The time interval in seconds to play an alert tone periodically when the Poly Trio system is in the mute state.
  - 5 (default)
  - 5 - 3600

**Persistent Microphone Mute**

With this feature, you can enable the microphone mute to persist across all calls managed on a phone.

By default, users can mute the microphone during an active call and it is unmuted when the active call ends. With persistent microphone mute enabled, when a user mutes the microphone during an active call, the microphone remains muted for all following calls until the user unmutes the microphone or the phone restarts.

When a user mutes the microphone when the phone is idle, the mute LED glows but no icon displays on the screen. When a user initiates a new active call with the microphone muted, the mute LED glows and a Mute icon displays on the phone screen.
Persistent Microphone Mute Parameter

Use the following parameter to enable persistent microphone mute.

```
feature.persistentMute.enabled
```

0 - The mute state ends when the active call ends or when the phone restarts.

1 (default) - When a user mutes the microphone during an active call, the microphone remains muted for all following calls until the user unmutes the microphone or the phone restarts.

Change causes system to restart or reboot.

Answer Incoming Calls with Mute Button

You can answer incoming calls using the three Mute buttons found on each side of the Poly Trio system hardware.

By default, you answer incoming calls using the touchscreen on the Poly Trio system hardware. With this feature enabled, you can also press the Mute buttons to accept incoming calls. If the phone is muted prior to the incoming call, accepting the call via the Mute buttons or the touchscreen automatically unmutes the phone. The phone can be muted once in the call using existing Mute functions.

Answer Incoming Calls with Mute Button Parameter

Use the following parameter to configure your Poly Trio system for answering calls with the Mute buttons.

```
up.callAnswerWithMuteButton
```

0 (default) – Disables using the Mute buttons to answer calls.

1 – Enables users to answer calls using the Mute buttons.

Call Timer

By default, 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.

You cannot configure the display of the call timer.

Called Party Identification

By default, the phone displays and logs the identity of all parties on outgoing calls.

The phone obtains called party identities from network signaling. Because party identification on outgoing calls is a default feature, the phone displays caller IDs matched to the call server and does not match IDs to entries in the contact directory or corporate directory.
Calling Party Identification Parameters

Use the parameters in the following list to configure calling party identification.

**call.callsPerLineKey**

Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines and can be overridden by the per-registration parameter *reg.x.callsPerLineKey*.

- 24 (default)
- 1 - 24

**up.useDirectoryNames**

- 1 (default) - The name field in the local contact directory is used as the caller ID for incoming calls from contacts in the local directory. Note: Outgoing calls and corporate directory entries are not matched.
- 0 - Names provided through network signaling are used for caller ID.

Connected Party Identification

By default, the phone displays and logs the identities of remote parties you connect to if the call server can derive the name and ID from network signaling.

In cases where remote parties have set up certain call features, the remote party you connect to—and the caller ID that displays on the phone—may be different than the intended party's. For example, Bob places a call to Alice, but Alice has call diversion configured to divert Bob's incoming calls to Fred. In this case, the phone logs and displays the connection between Bob and Fred. The phone does not match party IDs to entries in the contact directory or the corporate directory.

Calling Party Identification

By default, the phone displays the identity of incoming callers if available to the phone through the network signal.

If the incoming call address has been assigned to the contact directory, you can enable the phones to display the name assigned to contacts in the contact directory. However, the phone cannot match the identity of calling parties to entries in the corporate directory.

Calling Party Identification Parameters

Use the parameters in the following list to configure Calling Party Identification.

**up.useDirectoryNames**

- 1 (default) - The name field in the local contact directory is used as the caller ID for incoming calls from contacts in the local directory. Note: Outgoing calls and corporate directory entries are not matched.
0 - Names provided through network signaling are used for caller ID.

Remote Party Caller ID from SIP Messages
You can specify which SIP request and response messages to use to retrieve caller ID information.

Remote Party Caller ID from SIP Messages Parameters
Use the following parameters to specify which SIP request and response messages to use to retrieve caller ID information.

**voIpProt.SIP.CID.request.sourceSipMessage**
Specify which header in the SIP request to retrieve remote party caller ID from. You can use:
- voIpProt.SIP.callee.sourcePreference
- voIpProt.SIP.caller.sourcePreference
- voIpProt.SIP.CID.sourcePreference

UPDATE takes precedence over the value of this parameter.
NULL (default) - Remote party caller ID information from INVITE is used.
INVITE
PRACK
ACK
0-6
This parameter does not apply to shared lines.

**voIpProt.SIP.CID.response.sourceSipMessage**
Specify which header in the SIP request to retrieve remote party caller ID from. You can use:
- voIpProt.SIP.callee.sourcePreference
- voIpProt.SIP.caller.sourcePreference
- voIpProt.SIP.CID.sourcePreference

NULL (default) - The remote party caller ID information from the last SIP response is used.
100, 180, 183, 200
0-3
This parameter does not apply to shared lines.
Calling Line Identification

The Calling Line Identity Presentation (CLIP) displays the phone number of the caller on the phone screen.

You can configure this feature by using the parameters in the following table.

## Calling Line Identification Parameters

### `voIpProt.SIP.CID.sourcePreference`

Specify the priority order for the sources of caller ID information. The headers can be in any order.

- Null (default) - Caller ID information comes from P-Asserted-Identity, Remote-Party-ID, and From in that order.
- From, P-Asserted-Identity, Remote-Party-ID
- P-Asserted-Identity, From, Remote-Party-ID

Supported Headers Default Order: P-Asserted-Identity, Remote-Party-ID, From

**Note:** By default callee and caller will take identity order from `voIpProt.SIP.CID.sourcePreference`.

If `voIpProt.SIP.Caller.SourcePreference` or `voIpProt.SIP.Callee.SourcePreference` are configured then the order set by `voIpProt.SIP.CID.sourcePreference` is ignored.

### `voIpProt.SIP.caller.sourcePreference`

Set the priority order to display the caller's identity for incoming calls.

- Null (default)
- 0-120

Supported Headers Default Order: P-Asserted-Identity, Remote-Party-ID, From

String

### `voIpProt.SIP.callee.sourcePreference`

Set the priority order to display the callee's identity for outgoing calls.

- Null (default)

Supported Headers Default Order: P-Asserted-Identity, Remote-Party-ID, From

String
SIP Header Warnings

You can configure the warning field from a SIP header to display a pop-up message on the phone, for example, when a call transfer failed due to an invalid extension number.

You can display pop-up messages in any language supported by the phone. The messages display for three seconds unless overridden by another message or action.

For a list of supported SIP header warnings, see the article “Supported SIP Request Headers” in the Polycom Knowledge Base.

SIP Header Warning Parameters

You can use the parameters in the following list to enable the warning display or specify which warnings to display.

\[ \text{voIpProt.SIP.header.warning.enable} \]

- 0 (default) - The warning header is not displayed.
- 1 - The warning header is displayed if received.

\[ \text{voIpProt.SIP.header.warning.codes.accept} \]

Specify a list of accepted warning codes.

- Null (default) - All codes are accepted. Only codes between 300 and 399 are supported.
- For example, if you want to accept only codes 325 to 330:
  \[ \text{voIpProt.SIP.header.warning.codes.accept=325,326,327,328,329,330} \]

Distinctive Call Waiting

You can use the alert-info values and class fields in the SIP header to map calls to distinct call-waiting types.

You can apply three call waiting types: beep, ring, and silent. The following list shows you the parameters you can configure for this feature. This feature requires call server support.

Distinctive Call Waiting Parameters

You can use the alert-info values and class fields in the SIP header to map calls to distinct call-waiting types.

You can apply three call waiting types: beep, ring, and silent. The following list includes available parameters.

\[ \text{Note: This feature requires call server support.} \]

\[ \text{voIpProt.SIP.alertInfo.x.class} \]
Alert-Info fields from INVITE requests are compared as many of these parameters as are specified (x=1, 2, ..., N) and if a match is found, the behavior described in the corresponding ring class is applied.

default (default)

**voIpProt.SIP.alertInfo.x.value**

Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE.

NULL (default)

---

**Do Not Disturb**

You can enable Do Not Disturb (DND) locally on the phone or on the server.

The local DND feature is enabled by default, and users can enable or disable DND for all or individual registered lines on the phone. When enabled, users are not notified of incoming calls placed to their line.

**Server-Based Do Not Disturb**

If you want to enable server-based DND, you must enable the feature on both a registered phone and on the server.

The following conditions apply for server-based DND:

- Server-based DND can be applied to multiple registered lines on a phone; however, applying DND to individual registrations is not supported.
- Server-based DND cannot be enabled on a phone configured as a shared line.
- If server-based DND is enabled but not turned on when the DND feature is enabled on the phone, the "Do Not Disturb" message displays on the phone, but incoming calls continue to ring.
- Server-based DND disables local Call Forward and DND, however, if an incoming is not routed through the server, an audio alert still plays on the phone.

**Do Not Disturb Parameters**

Use the parameters in the following list to configure the local DND feature.

**feature.doNotDisturb.enable**

1 (default) - Enable Do Not Disturb (DND).
0 - Disable Do Not Disturb (DND).

Change causes system to restart or reboot.

**voIpProt.SIP.serverFeatureControl.dnd**

0 (default) - Disable server-based DND.
1 - Server-based DND is enabled. Server and local phone DND are synchronized.
**voIpProt.SIP.serverFeatureControl.localProcessing.dnd**

This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.dnd`.

- If set to 1 (default) and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, the phone and the server perform DND.
- If set to 0 and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, DND is performed on the server-side only, and the phone does not perform local DND.
- If both `voIpProt.SIP.serverFeatureControl.localProcessing.dnd` and `voIpProt.SIP.serverFeatureControl.dnd` are set to 0, the phone performs local DND and the localProcessing parameter is not used.

  - 1 (default) - Enabled
  - 0 - Disabled

**call.rejectBusyOnDnd**

When enabled, the phone rejects incoming calls with a busy signal while Do Not Disturb is on. When disabled, the phone gives a visual alert of incoming calls, but no audible ring, when Do Not Disturb is on.

- 1 (default) - Enabled
- 0 - Disabled

Note: This parameter does not apply to shared lines since not all users may want DND enabled.

**call.donotdisturb.perReg**

This parameter determines if the do-not-disturb feature applies to all registrations on the phone or on a per-registration basis.

- 0 (default) - DND applies to all registrations on the phone.
- 1 - Users can activate DND on a per-registration basis.

Note: If `voIpProt.SIP.serverFeatureControl.dnd` is set to 1 (enabled), this parameter is ignored.

**Remote Party Disconnect Alert Tone**

Remote Party Disconnect Alert Tone alerts users when the call has been disconnected by a remote party or network.

When a remote party or network on an active call gets disconnected, an alert is played to notify the user about the lost connection. The tone is played only for an active call.
Remote Party Disconnect Alert Tone Parameter
You can configure this feature by using the parameter below.

call.remoteDisconnect.toneType
  Choose an alert tone to play when the remote party disconnects call.
  Silent (Default)
  messageWaiting, instantMessage, remoteHoldNotification, localHoldNotification,
  positiveConfirm, negativeConfirm, welcome, misc1, misc2, misc3, misc4, misc5, misc6, misc7,
  custom1, custom2, custom3, custom4, custom5, custom6, custom7, custom8, custom9,
  custom10

Call Waiting Alerts
By default, the phone alerts users to incoming calls while a user is in an active call.
You can choose to disable these call waiting alerts and specify ringtones for incoming calls.

Call Waiting Alert Parameters
Use the parameters in the following list to configure call waiting alerts.

call.callWaiting.enable
  Enable or disable call waiting.
  1 (default) - The phone alerts you to an incoming call while you are in an active call. If 1, and
  you end the active call during a second incoming call, you are alerted to the second incoming
  call.
  0 - You are not alerted to incoming calls while in an active call and the incoming call is treated as
  if you did not answer it.

call.callWaiting.ring
  Specifies the ringtone of incoming calls when another call is active. If no value is set, the default
  value is used.
  beep (default) - A beep tone plays through the selected audio output mode on the active call.
  ring - The configured ringtone plays on the speaker.
  silent - No ringtone.

Missed Call Notifications
By default, a counter with the number of missed calls displays on the Recent Calls icon on the phone.
You can configure the phone to record all missed calls or to display only missed calls that arrive through
the SIP server. You can also enable missed call notifications for each registered line on a phone.
**Missed Call Notification Parameters**

Use the following list to configure options for missed call notifications.

**call.missedCallTracking.x.enabled**

1 (default) - Missed call tracking for a specific registration is enabled.

If `call.missedCallTracking.x.enabled` is set to 0, then the missed call counter is not updated regardless of what `call.serverMissedCalls.x.enabled` is set to (and regardless of how the server is configured) and the missed call list does not display in the phone menu.

If `call.missedCallTracking.x.enabled` is set to 1 and `call.serverMissedCalls.x.enabled` is set to 0, then the number of missed calls is incremented regardless of how the server is configured.

If `call.missedCallTracking.x.enabled` is set to 1 and `call.serverMissedCalls.x.enabled` is set to 1, then the handling of missed calls depends on how the server is configured.

Change causes system to restart or reboot.

**call.serverMissedCall.x.enabled**

0 (default) - All missed-call events increment the counter for a specific registration.

1 - Only missed-call events sent by the server will increment the counter.

Note: This feature is supported only with the BroadSoft Synergy call server (previously known as Sylantro).

Change causes system to restart or reboot.

**Call Hold**

Call hold enables users to pause activity on an active call so that they can use the phone for another task, such as searching the phone's menu for information.

When an active call is placed on hold, a message displays informing the held party that they are 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.

**Call Hold Parameters**

See the following list for the available parameters you can use to configure for Call Hold.

**voIpProt.SIP.useRFC2543hold**

0 (default) - SDP media direction parameters (such as a=sendonly) per RFC 3264 when initiating a call.
1 - the obsolete c=0.0.0.0 RFC2543 technique is used when initiating a call.

**voIPProt.SIP.useSendonlyHold**

1 (default) - The phone will send a reinvite with a stream mode parameter of “sendonly” when a call is put on hold.

0 - The phone will send a reinvite with a stream mode parameter of “inactive” when a call is put on hold.

Note: The phone will ignore the value of this parameter if set to 1 when the parameter voIPProt.SIP.useRFC2543hold is also set to 1 (default is 0).

**call.hold.localReminder.enabled**

0 (default) - Users are not reminded of calls that have been on hold for an extended period of time.

1 - Users are reminded of calls that have been on hold for an extended period of time.

Change causes system to restart or reboot.

**call.hold.localReminder.period**

Specify the time in seconds between subsequent hold reminders.

60 (default)

Change causes system to restart or reboot.

**call.hold.localReminder.startDelay**

Specify a time in seconds to wait before the initial hold reminder.

90 (default)

Change causes system to restart or reboot.

**voIPProt.SIP.musicOnHold.uri**

A URI that provides the media stream to play for the remote party on hold. This parameter is used if reg.x.musicOnHold.uri is Null.

Null (default)

SIP URI

**Hold Implementation**

The phone supports two currently accepted means of signaling hold.

The phone can be configured to use either hold signaling method. The phone supports both methods when signaled by the remote endpoint.
Call Controls

Supported Hold Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal the media directions with the &quot;a&quot; SDP media attributes sendonly, recvonly, inactive, or sendrecv.</td>
<td>Preferred method.</td>
</tr>
<tr>
<td>Set the &quot;c&quot; destination addresses for the zmedia streams in the SDP to zero. For example, c=0.0.0.0</td>
<td>No longer recommended due to RTCP problems associated with this method. Receiving sendrecv, sendonly, or inactive from the server causes the phone to revert to the other hold method.</td>
</tr>
</tbody>
</table>

Call Transfer

The call transfer feature enables users to transfer an existing active call to a third-party address.

You can configure the call transfer feature and set the default transfer type.

Users can perform the following types of call transfers:

- Blind Transfer—Users complete a call transfer without speaking with the other party first.
- Consultative Transfer—Users speak with the other party before completing the transfer.

By default, users can complete a call transfer without waiting for the other party to answer the call first, which is a Blind Transfer. In this case, Party A can transfer Party B's call to Party C before Party C answers the transferred call. You can disable the blind transfer feature so that users must wait for the other party to answer before completing the transfer.

Call Transfer Parameters

Use the following list to specify call transfer behavior.

**voIpProt.SIP.allowTransferOnProceeding**

- 1 (default) - Transfer during the proceeding state of a consultation call is enabled.
- 0 - Transfer during the proceeding state of a consultation call is disabled
- 2 - Phones will accept an INVITE with replaces for a dialog in early state. This is needed when using transfer on proceeding with a proxy call server such as openSIPS, reSIProcate or SipXecs.

**call.defaultTransferType**

Set the transfer type the phone uses when transferring a call.

Generic Base Profile: Consultative (default) - Users can immediately transfer the call to another party.

Skype Base Profile: Blind (default) - The call is placed on hold while a new call is placed to the other party.
Call Forwarding

Poly phones support a flexible call forwarding feature that enables users to forward incoming calls to another contact or phone line.

Users can enable call forwarding in the following ways:

• To all calls
• To incoming calls from a specific caller or extension
• During an incoming call
• When the phone is busy
• When do not disturb is enabled
• After a set number of rings before the call is answered
• To a predefined destination chosen by the user

If you are registering phones with the Skype for Business Server, the following call forwarding options are available on Skype for Business-enabled phones:

• Forward to a contact
• Forward to voicemail
• Forward to Delegates
• Simultaneously Ring Delegates
• Simultaneously Ring Group Contacts

Call Forward on Shared Lines

You can enable server-based call forwarding for shared lines.

If using BroadWorks R20 server, note the following:

• Local call-forwarding is not supported on shared lines.
• Dynamic call forwarding—forwarding incoming calls without answering the call—is not supported.

Note: The server-based and local call forwarding features do not work with the shared call appearance (SCA) and bridged line appearance (BLA) features. In order to enable users to use call forwarding, disable SCA or BLA enabled.

Call Forwarding Parameters

Use the parameters in the following list to configure feature options for call forwarding.

No parameters are needed to enable call forwarding on Skype for Business-enabled phones.

**feature.forward.enable**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (default)</td>
<td>Enables call forwarding.</td>
</tr>
<tr>
<td>0</td>
<td>Disables call forwarding. Users cannot use Call Forward and the option is removed from the phone's Features menu.</td>
</tr>
</tbody>
</table>
**voIpProt.SIP.serverFeatureControl.cf**

0 (default) - The server-based call forwarding is not enabled.

1 - The server-based call forwarding is enabled.

Change causes system to restart or reboot.

**voIpProt.SIP.serverFeatureControl.localProcessing.cf**

This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`.

1 (default) - If set to 1 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, the phone and the server perform call forwarding.

0 - If set to 0 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, call forwarding is performed on the server side only, and the phone does not perform local call forwarding.

If both `voIpProt.SIP.serverFeatureControl.localProcessing.cf` and `voIpProt.SIP.serverFeatureControl.cf` are set to 0, the phone performs local call forwarding and the `localProcessing` parameter is not used.

**voIpProt.SIP.header.diversion.enable**

0 (default) - If set to 0, the diversion header is not displayed.

1 - If set to 1, the diversion header is displayed if received.

Change causes system to restart or reboot.

**voIpProt.SIP.header.diversion.list.useFirst**

1 (default) - If set to 1, the first diversion header is displayed.

0 - If set to 0, the last diversion header is displayed.

Change causes system to restart or reboot.

**divert.x.contact**

All automatic call diversion features uses this forward-to contact. All automatically forwarded calls are directed to this contact. The contact can be overridden by a busy contact, DND contact, or no-answer contact as specified by the `busy`, `dnd`, and `noAnswer` parameters that follow.

Null (default)

string - Contact address that includes ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com).

Change causes system to restart or reboot.

**divert.x.sharedDisabled**

1 (default) - Disables call diversion features on shared lines.

0 - Enables call diversion features on shared lines.
divert.x.autoOnSpecificCaller

1 (default) - Enables the auto divert feature of the contact directory for calls on registration x. You can specify to divert individual calls or divert all calls.
0 - Disables the auto divert feature of the contact directory for registration x.
Change causes system to restart or reboot.

divert.busy.x.enabled

1 (default) - Diverts calls registration x is busy.
0 - Does not divert calls if the line is busy.
Change causes system to restart or reboot.

divert.busy.x.contact

Calls are sent to the busy contact's address if it is specified; otherwise calls are sent to the default contact specified by divert.x.contact.
Null (default) string - contact address.
Change causes system to restart or reboot.

divert.dnd.x.enabled

0 (default) - Divert calls when DND is enabled on registration x.
1 - Does not divert calls when DND is enabled on registration x.
Change causes system to restart or reboot.

divert.dnd.x.contact

Calls are sent to the DND contact's address if it is specified; otherwise calls are sent to the default contact specified by divert.x.contact.
Null (default)
string - contact address.
Change causes system to restart or reboot.

divert.fwd.x.enabled

1 (default) - Users can forward calls on the phone's Home screen and use universal call forwarding.
0 - Users cannot enable universal call forwarding (automatic forwarding for all calls on registration x).
Change causes system to restart or reboot.
**divert.noanswer.x.enabled**

1 (default) - Unanswered calls after the number of seconds specified by timeout are sent to the no-answer contact.

0 - Unanswered calls are diverted if they are not answered.

Change causes system to restart or reboot.

**divert.noanswer.x.contact**

Null (default) - The call is sent to the default contact specified by divert.x.contact.

string - contact address

Change causes system to restart or reboot.

**divert.noanswer.x.timeout**

55 (default) - Number of seconds for timeout.

positive integer

Change causes system to restart or reboot.

**reg.x.fwd.busy.contact**

The forward-to contact for calls forwarded due to busy status.

Null (default) - The contact specified by divert.x.contact is used.

string - The contact specified by divert.x.contact is not used

**reg.x.fwd.busy.status**

0 (default) - Incoming calls that receive a busy signal is not forwarded

1 - Busy calls are forwarded to the contact specified by reg.x.fwd.busy.contact.

**reg.x.fwd.noanswer.contact**

Null (default) - The forward-to contact specified by divert.x.contact is used.

string - The forward to contact used for calls forwarded due to no answer.

**reg.x.fwd.noanswer.ringCount**

The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20.

0 - (default)

1 to 65535

**reg.x.fwd.noanswer.status**

0 (default) - The calls are not forwarded if there is no answer.
1 - The calls are forwarded to the contact specified by `reg.x.noanswer.contact` after ringing for the length of time specified by `reg.x.fwd.noanswer.ringCount`.

**reg.x.serverFeatureControl.cf**

This parameter overrides `voIpProt.SIP.serverFeatureControl.cf`.

0 (default) - The server-based call forwarding is disabled.
1 - server based call forwarding is enabled.
Change causes system to restart or reboot.

**divert.x.sharedDisabled**

1 (default) - Disables call diversion features on shared lines.
0 - Enables call diversion features on shared lines.
Change causes system to restart or reboot.

**voIpProt.SIP.serverFeatureControl.cf**

0 (default) - Disable server-based call forwarding.
1 - Enable server-based call forwarding.
This parameter overrides `reg.x.serverFeatureControl.cf`.
Change causes system to restart or reboot.

**voIpProt.SIP.serverFeatureControl.localProcessing.cf**

1 (default) - Allows to use the value for `voIpProt.SIP.serverFeatureControl.cf`.
0 - Does not use the value for
This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`.

**reg.x.serverFeatureControl.localProcessing.cf**

This parameter overrides
`voIpProt.SIP.serverFeatureControl.localProcessing.cf`.

0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior.
1 - The phone performs local Call Forward behavior on all calls received.

**call.shared.disableDivert**

1 (default) - Enable the diversion feature for shared lines.
0 - Disable the diversion feature for shared lines. Note that this feature is disabled on most call servers.
Change causes system to restart or reboot.
Automatic Off-Hook Call Placement

You can configure the phone to automatically place a call to a specified number when the phone goes off-hook, which is sometimes referred to as Hot Dialing.

The phone goes off-hook when a user lifts the handset, selects New Call, or presses the speakerphone buttons on the phone.

Automatic Off-Hook Call Placement Parameters

As shown in the following list, you can specify an off-hook call contact, enable or disable the feature for each registration, and specify a protocol for the call.

You can specify only one line registration for the Poly Trio system.

call.autoOffHook.x.contact

Enter a SIP URL contact address. The contact must be an ASCII-encoded string containing digits, either the user part of a SIP URL (for example, 6416), or a full SIP URL (for example, 6416@polycom.com).

NULL (default)

call.autoOffHook.x.enabled

0 (default) - No call is placed automatically when the phone goes off hook, and the other parameters are ignored.

1 - When the phone goes off hook, a call is automatically placed to the contact you specify in call.autoOffHook.x.contact and using the protocol you specify in call.autoOffHook.x.protocol.

call.autoOffHook.x.protocol

Specify the calling protocol. If no protocol is specified, the phone uses the protocol specified by call.autoRouting.preferredProtocol. If a line is configured for a single protocol, the configured protocol is used.

NULL (default)

SIP

H323

Multiple Line Keys Per Registration

You can assign a single registered phone line address to multiple line keys on Poly phones.

This feature can be useful for managing a high volume of calls to a single line. This feature is not supported when registered with Microsoft Skype for Business Server.
**Multiple Line Keys Per Registration Parameter**

Use the parameter below to configure this feature.

This feature is one of several features associated with Call Appearances.

`reg.x.lineKeys`

Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model.

- 1 (default)
- 1 to max

**Multiple Call Appearances**

You can enable each registered phone line to support multiple concurrent calls and have each concurrent call display on the phone’s user interface.

For example, with multiple call appearances, users can place one call on hold, switch to another call on the same registered line, and have 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.

Poly Trio can have a maximum of 12 concurrent calls with only one active call in progress. You can register one line on the Poly Trio system.

**Multiple Call Appearance Parameters**

Use the parameters in the following list to set the maximum number of concurrent calls per registered line and the default number of calls per line key.

Note that you can set the value for the `reg.1.callsPerLineKey` parameter to a value higher than 1, for example, 3. After you set the value to 3, for example, you can have three call appearances on line 1. By default, any additional incoming calls are automatically forwarded to voicemail. If you set more than two call appearances, a call appearance counter displays at the top-right corner on the phone.

`call.callsPerLineKey`

Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines.

Note: This parameter can be overridden by the per-registration parameter `reg.x.callsPerLineKey`.

- 12 (default)
- 1 - 12

`reg.x.callsPerLineKey`
Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration.

This per-registration parameter overrides call.callsPerLineKey.

12 (default)
1 - 12

**Bridged Line Appearance**

Bridged line appearance connects calls and lines to multiple phones.

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, which is called line seize. If the answering phone places the call on hold, that call becomes available to all phones of that group. All call states—active, inactive, on hold—are displayed on all phones of a group.

---

**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 are using. In the configuration files, bridged lines are configured by shared line parameters. The barge-in feature is not available with bridged line appearances; it is available only with shared call appearances.

---

**Bridged Line Appearance Signaling**

A bridged line is an address of record managed by a server.

The server allows multiple endpoints to register locations against the address of record.

The phone supports Bridged Line Appearances (BLA) using the SUBSCRIBE-NOTIFY method in the SIP Specific Event Notification framework (RFC 3265). The event used is dialog for bridged line appearance subscribe and notify.

**Bridged Line Appearance Parameters**

To begin using Bridged Line Appearance, you must get a registered address dedicated for use with your call server provider.

This dedicated address must be assigned to a phone line in the reg.x.address parameter.

Use the parameters in the following list to configure this feature.

**call.shared.disableDivert**

1 (default) - Enable the diversion feature for shared lines.
0 - Disable the diversion feature for shared lines. Note that this feature is disabled on most call servers.

Change causes system to restart or reboot.
**reg.x.type**
- private (default) - Use standard call signaling.
- shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.

**reg.x.thirdPartyName**
- Null (default) - In all other cases.
- string address - This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).

**divert.x.sharedDisabled**
- 1 (default) - Disables call diversion features on shared lines.
- 0 - Enables call diversion features on shared lines.
  Change causes system to restart or reboot.

**voIpProt.SIP.blaGlareHonorRetryAfter**
- Controls the Retry mechanism.
  - 1 (default) – The phone honors the Retry-after header on glare and sends NOTIFY with the same state and line-id after the requested time interval.
  - 0 – The phone ignores the Retry-after header on glare and immediately sends NOTIFY with the next available line-id.

---

## Voicemail

When you configure phones with a SIP URL that integrates with a voicemail server contact, users receive a visual and audio alert when they have new voicemail messages available on their phone.

### Voicemail Parameters

Use the parameters in the following list to configure voicemail and voicemail settings.

**feature.voicemail.enabled**
- 1 (default) - Enable voicemail.
- 0 - Disable voicemail.

**msg.mwi.x.callBackMode**
- The message retrieval mode and notification for registration x.
  - registration (default) - The registration places a call to itself (the phone calls itself).
  - contact - a call is placed to the contact specified by `msg.mwi.x.callback`.  
  

disabled - Message retrieval and message notification are disabled.

**msg.mwi.x.callBack**
The contact to call when retrieving messages for this registration if `msg.mwi.x.callBackMode` is set to `contact`.

ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)

NULL (default)

**msg.mwi.x.subscribe**
Specify the URI of the message center server. ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)

If non-Null, the phone sends a SUBSCRIBE request to this contact after boot up.

NULL (default)

**mwi.backLight.disable**
Specify if the phone screen backlight illuminates when you receive a new voicemail message.

0 (default) - Disabled
1 - Enabled

Change causes system to restart or reboot.

**up.mwiVisible**
Specify if message waiting indicators (MWI) display or not.

0 (default) - If `msg.mwi.x.callBackMode=0`, MWI do not display in the message retrieval menus.
1 - MWI display.

Change causes system to restart or reboot.

**up.oneTouchVoiceMail**

1 (default) - Lync Base Profile
0 (default) - Generic Base Profile

0 (default) - The phone displays a summary page with message counts.
1 - You can call voicemail services directly from the phone, if available on the call server, without displaying the voicemail summary.

Change causes system to restart or reboot.
Local Call Recording

Local call recording enables you to record audio calls to a USB device connected to the phone.

You can play back recorded audio on the phone or devices that run applications like Windows Media Player® or iTunes® on a Windows® or Apple® computer. To use this feature, ensure that the USB port is enabled.

Audio calls are recorded in .wav format and include a date/time stamp. The phone displays the recording time remaining on the attached USB device, and users can browse all recorded files using the phone's menu.

Note: Federal, state, and/or local laws may legally require that you notify some or all of the call parties when a call recording is in progress.

Local Call Recording Parameter

Use the following parameter to configure local call recording.

**feature.callRecording.enabled**

0 (default) - Disable audio call recording.
1 - Enable audio call recording.
Change causes system to restart or reboot.

Local and Centralized Conference Calls on Poly Trio

When a Poly Trio system is paired with a Poly Trio Visual+, Trio VisualPro, or RealPresence Group Series system, users can initiate and join the following types of conferences:

- Local multipoint audio conference with up to four external connections
- Local video conferences
- Video calls on supported H.264 standards-compliant video bridges or services

Poly Trio system support for the Poly Trio Visual+ and VisualPro systems varies by model:

The Poly Trio system can send and receive one video connection and displays the far-end device that joined the call last. Poly Trio does not support locally-hosted multipoint video conferencing.

For video and content for conference calls, you must connect a supported camera and monitor(s) to a Poly Trio Visual+, Trio VisualPro, or RealPresence Group Series system. When the devices are connected and paired, users can send video and share content. For details and limitations of content sharing, refer to the section Content Sharing.

Local and Centralized Conference Call Parameters

The following list includes available call management parameters.

You can specify whether, when the host of a three-party local conference leaves the conference, the other two parties remain connected or disconnected. If you want the other two parties remain connected, the
phone performs a transfer to keep the remaining parties connected. If the host of four-party local conference leaves the conference, all parties are disconnected and the conference call ends. If the host of a centralized conference leaves the conference, each remaining party remains connected. For more ways to manage conference calls, see Conference Management.

**call.localConferenceCallHold**

0 (default) - The host cannot place parties on hold.
1 - During a conference call, the host can place all parties or only the host on hold.

**call.transferOnConferenceEnd**

1 (default) - After the conference host exits the conference, the remaining parties can continue.
0 - After the conference host exits the conference, all parties are exited and the conference ends.

**call.singleKeyPressConference**

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

0 (default) - Phone sound effects are heard only by the conference initiator.
1 - A conference is initiated when a user presses Conference the first time. Also, all sound effects (dial tone, DTMF tone while dialing and ringing back) are heard by all participants in the conference.

**voIpProt.SIP.conference.address**

Null (default) - Conferences are set up on the phone locally.
String 128 max characters - Enter a conference address. Conferences are set up by the server using the conferencing agent specified by this address. Acceptable values depend on the conferencing server implementation policy.

**video.conf.addVideoWhenAvailable**

0 (default) - When Poly Trio system is added to a conference by another participant via digit dialing, the system does not add video.
1 - When Poly Trio system is added to a conference by another participant via digit dialing, the system adds video if video is available on the conference.

**Conference Management Parameter**

Use the parameter in the following list to configure the conference management feature.

**feature.nWayConference.enabled**

0 - Users can hold three-way conferences but conference management options are not available.
1 (default) - Users can hold conferences with the maximum number of parties, and the conference management options display to enable users to add, hold, mute, and remove participants.

Conference Meeting Dial-In Options

When you enable the Calendar, the Poly Trio system displays a meeting reminder for upcoming meetings. If a dial-in number is available for the meeting, the reminder presents a Join button that enables users to join the meeting. If a meeting lists multiple dial-in numbers or URIs for the meeting, by default, the Join button automatically dials the first number.

You have the option to configure the Poly Trio system to offer users a list of available numbers when they tap the Join button instead of dialing the first number.

You can enable this feature using the exchange.meeting.join.promptWithList parameter. When enabled, the Poly Trio system provides multiple dial-in options when the user taps the Join button on the meeting reminder. You can enable users to choose any of the following dial-in options to join a meeting:

- SIP URI
- Tel URI
- PSTN number
- IP dial

Conference Meeting Dial-In Options Parameters

Use the following parameters to configure the dial-in information.

**exchange.meeting.join.promptWithList**

Specifies the behavior of the Join button on meeting reminder pop-ups.

0 (default) - Tapping Join on a meeting reminder should show a list of numbers to dial rather than immediately dialing the first one.

1 - A meeting reminder does not show a list of numbers to dial.

**exchange.meeting.parseWhen**

Specifies when to scan the meeting's subject, location, and description fields for dialable numbers.

NonSkypeMeeting (default)

Always

Never

Change causes system to restart or reboot.

**exchange.meeting.parseOption**

Specifies where to search for a dialable number.
exchange.meeting.parseEmailsAsSipUris

List instances of text like user@domain or user@ipaddress in the meeting description or subject under the More Actions pane as dialable SIP URIs.

0 (default) - it does not list the text as a dialable SIP URI
1 - it treats user@domain or user@ipaddress as a dialable SIP URI.

Change causes system to restart or reboot.

exchange.meeting.parseAllowedSipUriDomains

List of comma-separated domains that will be permitted to be interpreted as SIP URIs

Null (default)
String (maximum of 255 characters)

Change causes system to restart or reboot.

Hybrid Line Registration

Poly Trio systems support hybrid (Skype for Business / Open SIP) registration.

You can simultaneously register one line with Skype for Business or Open SIP and a second line with another Open SIP server. Similarly, you can choose to register all lines with Open SIP sever. You can also choose the number of lines you want to use by setting the value in reg.limit parameter.

If you plan to configure and register Skype for Business on one line, make sure to always use Line 1 for Skype for Business. You cannot simultaneously register two Skype for Business lines.

In addition, you can configure the line switching feature based on dial plan when the phone is on-hook. The line switching feature enables the dialed number to switch to the corresponding line. For example, when you place a call from the phone and the number corresponds to an Open SIP line, the line switching feature enables the dialed number to switch to the corresponding line.

Moreover, for dial plan based line switching, when all the lines are registered to Open SIP, the value defined in the global parameter for a dial plan takes the priority. For example, dialplan.impossibleMatchHandling and dialplan.conflictMatchHandling. Similarly, if the line is registered to Skype for Business, the value defined in the per-registration dial plan parameter takes priority over general dial plan parameter. For example, dialplan.1.conflictMatchHandling and dialplan.1.impossibleMatchHandling.

When more than one digit maps are getting matched to the dialed number - a conflict match - and the dialplan.conflictMatchHandling parameter is disabled, the first matching digit map starting from left to right takes priority. However, if the dialplan.conflictMatchHandling parameter is enabled, the matching digit map having the lowest timeout value takes priority.

Note that line switching is configurable based on dial plan when the phone is off-hook. By default, line switching for on-hook and off-hook dialing is disabled.
Alos notet hat that the Presence feature is available only on the Skype for Business line and will display the Device status. The following table list the Presence status for specific environment.

### Presence Status Indicators for Hybrid Line Registration

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Presence State on Skype for Business Line</th>
<th>Presence String</th>
<th>Presence State on Open SIP Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Skype line in a call</td>
<td>Busy</td>
<td>In a call</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Skype line in a call</td>
<td>Busy</td>
<td>In a call</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Content shared over PPCIP</td>
<td>Busy</td>
<td>In a call</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Non-Skype line in conference</td>
<td>Busy</td>
<td>In a conference</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Skype line in conference</td>
<td>Busy</td>
<td>In a conference</td>
<td>Not Supported</td>
</tr>
<tr>
<td>DND on Skype line</td>
<td>DND</td>
<td>Do Not Disturb</td>
<td>Not Supported</td>
</tr>
<tr>
<td>DND on Open SIP line</td>
<td>Available</td>
<td>Available</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

### Hybrid Line Registration Limitations

The Hybrid Registration feature include the following limitations:

- You cannot merge local conferences on Skype for Business registration lines. You can merge local conferences on Open SIP registration lines.
- You cannot bridge Skype for Business and Open SIP registration lines.
- Local merging of two point-to-point calls made using two different lines between two Poly Trio systems is not supported.
- Only call transfers between different SIP registrations with the same SIP call servers is supported. Call transfer between SIP registrations on different SIP call servers is not supported.
- To avoid unexpected phone behavior, do not use the same user name for multiple registrations. Use similar but not identical user names. For example, use: `reg 1.address="John.Smith@company.com" and reg 2.address="J.Smith@business.com"`.
- Transport Layer Security (TLS) encryption of Real-time Transport Protocol (RTP) media for secure communication in hybrid Open SIP registrations is not supported.
Hybrid Line Registration Parameters

Use the following parameters to configure dial plan and line switching for Hybrid Registration.

dialplan.digitmap.lineSwitching.enable

0 (default) - Disable the line switching in dial plan to switch the call to the dial plan matched line.
1 - Enable the line switching in dial plan to switch the call to the dial plan matched line.

This is not applicable for off-hook dialing.

reg.limit

Specify the maximum number of lines to use for registration.

1 (default)
• 3 is the maximum of registered lines.
• 12 is the maximum of unregistered lines. For all unregistered lines, make sure to set reg.x.server.y.register to 0.
• Only one H.323 line, registered or unregistered, is supported

reg.1.mergeServerDigitMapLocally

1 (default) - Allow the digit map from the in-band provisioning parameter dialplan.1.digitmap to merge with the local digit map.
0 - The digit map is not merged.

Configure Hybrid Line Registration using the Web Configuration Utility

You can configure the phone to support the Hybrid (Skype for Business/ Open SIP) Registration from phone's Web Configuration Utility page after enabling the feature using configuration parameter.

You must set the Base Profile as Skype for Business on the Poly Trio system.

Procedure

1. Sign in to the Poly Trio system's Web configuration Utility as Admin.
   If configuring Skype for Business on Line 1, sign in to the Web Configuration Utility as Skype for Business user.
   The number of lines enabled to configure is displayed.
3. Configure the Skype for Business registration on Line 1.
4. Configure the Open SIP registration on Line 2.
   You can configure other lines with Open SIP registration.
Local Digit Map

The local digit map feature allows the phone to automatically call a dialed number you configure. Dial plans apply on-hook when no Skype for Business line is registered or when line switching is enabled and at least one line has a non-empty dial plan.

Digit maps are defined by a single string or a list of strings. If a dialed number matches any string of a digit map, the call is automatically placed. If a dialed number matches no string—an impossible match—you can specify the phone's behavior. If a number ends with #, you can specify the phone's behavior, called trailing # behavior. You can also specify the digit map timeout, the period of time after you dial a number that the call is placed. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of RFC 3435.

Local Digit Maps Parameters

Poly support for digit map rules varies for open SIP servers and Microsoft Skype for Business Server. Use the following parameters to configure the local digit map.

dialplan.applyToCallListDial

Choose whether the dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus.

1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToDirectoryDial

Lync Base Profile – 1 (default)

Generic Base Profile – 0 (default)

0— The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

1— The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

Change causes system to restart or reboot.

dialplan.applyToForward

Lync Base Profile – 1 (default)

Generic Base Profile – 0 (default)

0— The dial plan does not apply to forwarded calls.

1— The dial plan applies to forwarded calls.

Change causes system to restart or reboot.
dialplan.applyToTelUriDial

Choose whether the dial plan applies to URI dialing.

1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToUserDial

Choose whether the dial plan applies to calls placed when the user presses Dial.

1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToUserSend

Choose whether the dial plan applies to calls placed when the user presses Send.

1 (default)

0

Change causes system to restart or reboot.

dialplan.conflictMatchHandling

Selects the dialplan based on more than one match with the least timeout.

0 (default for Generic Profile)

1 (default for Skype Profile)

dialplan.digitmap.timeOut

Specify a timeout in seconds for each segment of the digit map using a string of positive integers separated by a vertical bar ( | ). After a user presses a key, the phone waits this many seconds before matching the digits to a dial plan and dialing the call.

(Default) 3 | 3 | 3 | 3 | 3 | 3

If there are more digit maps than timeout values, the default value 3 is used. If there are more timeout values than digit maps, the extra timeout values are ignored.

Change causes system to restart or reboot.

dialplan.digitmap

Specify the digit map used for the dial plan using a string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. This parameter enables the phone to automatically initiate calls to numbers that match a digit map pattern.

Generic Base Profile (default) –
The string is limited to 2560 bytes and 100 segments of 64 bytes, and the following characters are allowed in the digit map.

- A comma (,), which turns dial tone back on.
- A plus sign (+) is allowed as a valid digit.
- The extension letter 'R' indicates replaced string.
- The extension letter 'Pn' indicates precedence, where 'n' range is 1-9.
  - 1—Low precedence
  - 9—High precedence

Change causes the system to restart or reboot.

**dialplan.filterNonDigitUriUsers**

Determine whether to filter out (+) from the dial plan.

0 (default)

1

Change causes the system to restart or reboot.

**dialplan.impossibleMatchHandling**

0 (default)—The digits entered up to and including the point an impossible match occurred are sent to the server immediately.

1—The phone gives a reorder tone.

2—Users can accumulate digits and dispatch the call manually by pressing Send.

3 (default) (Skype for Business) — No digits are sent to the call server until the timeout is configured by `dialplan.impossibleMatchHandling.timeout` parameter.

If a call orbit number begins with a pound (#) or asterisk (*), you need to set the value to 2 to retrieve the call using off-hook dialing.

Change causes the system to restart or reboot.

**dialplan.removeEndOfDial**

Sets if the trailing # is stripped from the digits sent out.

1 (default)

0

Change causes the system to restart or reboot.
**dialplan.routing.emergency.outboundIdentity**

Choose how your phone is identified when you place an emergency call.

- NULL (default)
- 10-25 digit number
- SIP
- TEL URI

If using a URI, the full URI is included verbatim in the P-A-I header. For example:

- `dialplan.routing.emergency.outboundIdentity = 5551238000`
- `dialplan.routing.emergency.outboundIdentity = sip:john@emergency.com`
- `dialplan.routing.emergency.outboundIdentity = tel:+16045558000`

**dialplan.routing.emergency.preferredSource**

Set the precedence of the source of emergency outbound identities.

- ELIN (default)— the outbound identity used in the SIP P-Asserted-Identity header is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN).
- Config— the parameter `dialplan.routing.emergency.outboundIdentity` has priority when enabled, and the LLDP-MED ELIN value is used if `dialplan.routing.emergency.outboundIdentity` is NULL.

**dialplan.routing.emergency.x.description**

Set the label or description for the emergency contact address.

- `x=1: Emergency, Others: NULL (default)`
- string

- `x` is the index of the emergency entry description where `x` must use sequential numbering starting at 1.

- Change causes system to restart or reboot.

**dialplan.routing.emergency.x.server.y**

Set the emergency server to use for emergency routing (`dialplan.routing.server.x.address` where `x` is the index).

- `x=1: 1, Others: Null (default)`
- positive integer

- `x` is the index of the emergency entry and `y` is the index of the server associated with emergency entry `x`. For each emergency entry (`x`), one or more server entries (`x,y`) can be configured. `x` and `y` must both use sequential numbering starting at 1.

- Change causes system to restart or reboot.

**dialplan.routing.emergency.x.value**
Set the emergency URL values that should be watched for. When the user dials one of the URLs, the call is directed to the emergency server defined by dialplan.routing.server.x.address.

x=15: 911, others: Null (default)
SIP URL (single entry)
x is the index of the emergency entry description where x must use sequential numbering starting at 15.

dialplan.routing.server.x.address

Set the IP address or hostname of a SIP server to use for routing calls. Multiple servers can be listed starting with x=1 to 3 for fault tolerance.
Null (default)
IP address
hostname
Blind transfer for 911 or other emergency calls may not work if registration and emergency servers are different entities.
Change causes system to restart or reboot.

dialplan.routing.server.x.port

Set the port of a SIP server to use for routing calls.
5060 (default)
1 to 65535
Change causes system to restart or reboot.

dialplan.routing.server.x.transport

Set the DNS lookup of the first server to use and dialed if there is a conflict with other servers.
DNSnaptr (default)
TCPpreferred
UDPOnly
TLS
TCPOnly
For example, if dialplan.routing.server.1.transport= "UDPOnly" and dialplan.routing.server.2.transport = "TLS", then UDPOnly is used.
Change causes system to restart or reboot.

dialplan.userDial.timeOut

Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook.
Generic Base Profile (default) – 0
Lync Base Profile (default) – 4
0-99 seconds
You can apply dialplan.userDial.timeOut only when its value is lower than up.IdleTimeOut.

Open SIP Digit Map

If you are using a list of strings, each string in the list can be specified as a set of digits or timers, or as an expression which the gateway uses to find the shortest possible match.

In addition, the digit map feature allows SIP URI dialing to match the URIs based on dial plan.

When making a URI call, the Poly Trio system allows dial plan matching for SIP URI calls to append strings to the dialed number. SIP URI dial plan can also be used with auto line switching in Hybrid registration scenarios to automatically select the line based on dial plan.

The following is a list of digit map string rules for open SIP environments.

- The following letters are case sensitive: x, T, R, S, and H.
- You must use only *, #, +, or 0-9 between the second and third R.
- If a digit map does not comply, it is not included in the digit plan as a valid map. That is, no match is made.
- There is no limit to the number of R triplet sets in a digit map. However, a digit map that contains less than a full number of triplet sets (for example, a total of 2 Rs or 5 Rs) is considered an invalid digit map.
- Digit map extension letter R indicates that certain matched strings are replaced. Using an RRR syntax, you can replace the digits between the first two Rs with the digits between the last two Rs. For example, $R555R604R$ would replace 555 with 604. Digit map timer letter T indicates a timer expiry. Digit map protocol letters S and H indicate the protocol to use when placing a call.
- If you use T in the left part of RRR's syntax, the digit map will not work. For example, $R0TR322R$ will not work.

The following examples illustrate the semantics of the syntax:

- R9R604Rxxxxxxx-Replaces 9 with 604
- xxR601R600Rxx-When applied to 1160122 gives 1160022
- R9RRxxxxxxx-Remove 9 at the beginning of the dialed number (replace 9 with nothing)
  - For example, if you dial 914539400, the first 9 is removed when the call is placed.
- RR604Rxxxxxxx-Prepend 604 to all seven-digit numbers (replace nothing with 604)
  - For example, if you dial 4539400, 604 is added to the front of the number, so a call to 6044539400 is placed.
- xR60xR600RxRxxxxxxx-Replace any 60x with 600 in the middle of the dialed number that matches.
  - For example, if you dial 16092345678, a call is placed to 16002345678.
- 911xxx.T-A period (.) that matches an arbitrary number, including zero, of occurrences of the preceding construct. For example:
  - 911123 with waiting time to comply with T is a match
  - 9111234 with waiting time to comply with T is a match
• 91112345 with waiting time to comply with T is a match and the number can grow indefinitely given that pressing the next digit takes less than T.

• sip:764xxxxxRR@registrar.polycomcsn.com - appends @registrar.polycomcsn.com to any URI calls matching with "764xxxxx".

For example, if you make a SIP URI call with 76412345 then @registrar.polycomcsn.com is appended to the string such that the SIP URI call INVITE becomes sip: 76412345@vc.polycom.com. Here, @domain string is required only for SIP URI calls from unregistered lines.

• sip:\xxxx@registrar.polycomcsn.com - This will match with any four digit URI calls having the domain @registrar.polycomcsn.com.

For example, if you configure three lines and has dial plan based line switching enabled. Now, if the third line's dial plan has sip:\xxxx@registrar.polycomcsn.com then call will be initiated from the third line if user dial 1234@registrar.polycomcsn.com because it matches with the third line's dial plan.

Generating Secondary Dial Tone with Digit Maps
You can regenerate a dial tone by adding a comma ,, to the digit map.

You can dial seven-digit numbers after dialing "8" as shown next in the example rule 8,[2-9]xxxxxxT : [2-9]11|0T|01lxxx.T|[0-1][2-9]xxxxxxxxx|8,[2-9]xxxxxxT|[2-9]xx.T

By adding the digit "8", the dial tone plays again, and users can complete the remaining seven-digit number. In this example, if users also have a 4-digit extension that begins with "8", then users will hear dial tone after the first "8" was dialed because "8" matches the "8" in the digit map.

If you want to generate dial tone without the need to send the "8", replace one string with another using the special character "R" as shown next in the rule R8RR. In the following example, replace "8" with an empty string to dial the seven-digit number:


Enhanced 911 (E.911)
This E.911 feature allows you to configure one of three sources the phone obtains location information from:

• LLDP-MED
• DHCP via option 99
• LIS compliant with RFC 5985

Configuring the source of location information allows the phone to share its location details in the invite sent when a 911 call is made to ensure the 911 operator dispatches emergency services to the correct address.

Enhanced 911 (E.911) Parameters
Use the following parameters to configure E.911.

feature.E911.locationInfoSchema
HYBRID (default) - SIP invites use an XML schema as per the RFC4119 and RFC5139 standards.
RFC 4119 - SIP invites use an XML schema as per the RFC4119 standards.
RFC5139 - SIP invites use an XML schema as per the RFC5139 standards.

**feature.E911.HELD.server**

NULL (default)
Set the IP address or hostname of the Location Information Server (LIS) address. For example, host.domain.com or https://xxx.xxx.xxx.xxx.
0 - 255

**feature.E911.HELD.username**

NULL (default)
Set the user name used to authenticate to the LIS.

**feature.E911.HELD.password**

NULL (default)
Set the password used to authenticate to the Location Information Server.
0-255

**feature.E911.HELD.identity**

Set the vendor-specific element to include in a location request message. For example, ‘companyID’.
NULL (default)
String 255 character max

**feature.E911.HELD.identityValue**

Set the value for the vendor-specific element to include in a location request message.
NULL (default)
String 255 character max

**feature.E911.locationRetryTimer**

Specify the retry timeout value in seconds for the location request sent to the Location Information Server (LIS).
The phone does not retry after receiving location information received through the LIS.
60 seconds (default)
60 - 86400 seconds
feature.E911.HELD.nai.enable

0 (default) – The NAI is omitted as a device identity in the location request sent to the LIS.
1 - The NAI is included as a device identity in the location request sent to the LIS.

locInfo.source

Specify the source of phone location information. This parameter is useful for locating a phone in environments that have multiple sources of location information.

LLDP (default for Generic Base Profile) – Use the network switch as the source of location information.
MS_E911_LIS (default for Lync Base Profile) – Use the Skype for Business Server as the source of location information.
CONFIG – You can manually configure the source of location information for Skype for Business.
LIS – Use the location information server as the source of location information. Generic Base Profile only.
DHCP – Use DHCP as the source of location information. Generic Base Profile only.

If location information is not available from a default or configured source, the fallback priority is as follows:
Generic Base Profile: No fallback supported for Generic Base Profile
Lync Base Profile: MS_E911_LIS > CONFIG > LLDP

locInfo.x.label

Enter a label for the location.
Null (default)

locInfo.x.country

Enter the country where the phone is located.
Null (default)

locInfo.x.A1

Enter the national subdivision where the phone is located. For example, a state or province.
Null (default)

locInfo.x.A3

Enter the city where the phone is located.
Null (default)

locInfo.x.PRD
Enter the leading direction of the street location.
Null (default)

locInfo.x.RD
Enter the name of road or street where the phone is located.
Null (default)

locInfo.x.STS
Enter the suffix of the name used in locInfo.x.RD. For example, street or avenue.
Null (default)

locInfo.x.POD
Enter the trailing street direction. For example, southwest.
Null (default)

locInfo.x.HNO
Enter the street address number of the phone's location.
Null (default)

locInfo.x.HNS
Enter a suffix for the street address used in locInfo.x.HNS. For example, A or ½.
Null (default)

locInfo.x.LOC
Enter any additional information that identifies the location.
Null (default)

locInfo.x.NAM
Enter a proper name to associate with the location.
Null (default)

locInfo.x.PC
Enter the ZIP or postal code of the phone's location.
Null (default)

feature.E911.enabled
0 (default) – Disable the E.911 feature.
1 – Enable the E.911 feature.

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 Open SIP environments.

This parameter is mutually exclusive of the Ribbon Communications E.911 feature and if this parameter and feature.genband.E911.enabled are enabled, this parameter takes precedence.

**feature.E911.HELD.requestType**

- Any (default) - Send a request to the Location Information Server (LIS) to return either ‘Location by Reference’ or ‘Location by Value’. Note this is not the ‘Any’ value referred to in RFC 5985.
- Civic – Send a request to the LIS to return a location by value in the form of a civic address for the device as defined in RFC 5985.
- RefID – Send a request to the LIS to return a set of Location URIs for the device as defined in RFC 5985.

**voIpProt.SIP.header.priority.enable**

- 0 (default) – Do not include a priority header in the E.911 INVITE message.
- 1 - Include a priority header in the E.911 INVITE message.

**voIpProt.SIP.header.geolocation-routing.enable**

- 0 (default) – Do not include the geolocation-routing header in the E.911 INVITE message.
- 1 - Include the geolocation-routing header in the E.911 INVITE message.

**feature.E911.HELD.secondary.server**

Set the IP address or hostname of the secondary Location Information Server (LIS) address. For example, host.domain.com or https://xxx.xxx.xxx.xxx.

- NULL (default)
- 0-255
- Dotted-decimal IP address
- Hostname
- Fully-qualified domain name (FQDN)

**feature.E911.HELD.secondary.username**

Set a user name to authenticate to the secondary Location information Server (LIS).

- NULL (default)
- String
- 0-255
**feature.E911.HELD.secondary.password**

Set a password to authenticate to the secondary LIS.

NULL (default)

String

**feature.E911.usagerule.retransmission**

0 (default) - The recipient of this location object is not permitted to share the enclosed location information, or the object as a whole, with other parties.

1 - Distributing this location is permitted.

**lync.E911.notificationUri.expansion.enabled**

0 (default) - Disables expansion of distribution lists.

1 - Enables users to expand distribution lists received as part of the notification URI.

**lync.E911.notificationUri.maxUrls**

Set the limit for the number of URLs in the notification URI.

30 (default)

1 - 100

---

**Multilevel Precedence and Preemption (MLPP) for Assured Services - Session Initiation Protocol (AS-SIP)**

Multilevel Precedence and Preemption (MLPP) enables you to configure a precedence level for outgoing calls, which is implemented in accordance with the standards set by Assured Services for Session Initiation Protocol (AS-SIP).

Higher precedence calls preempt—end—active calls with a lower precedence level. When an active call is preempted, the phone plays a preemption tone and displays a preemption screen. The preemption screen display time can be configured in the configuration file. The default time for the preempted screen is 0 seconds for callee and 3 seconds for caller. If the default time for the preempted screen is 0 seconds, then preemption screen is displayed until you press the OK button. The preemption screen shows that the current call was preempted, and an OK button to acknowledge the preemption. The user can then answer the incoming higher-precedence call or reject the call. If the callee doesn’t acknowledge the incoming call, the notification disappears and the current call ends.

If a lower-precedence call is on hold, and you receive a higher-precedence call, the preemption screen doesn’t display, and the preemption tone doesn’t play.

MLPP treats incoming calls with the same precedence level as the active call depending on the call state, as shown in the following table.
## MLPP Behavior

<table>
<thead>
<tr>
<th>Current Call State</th>
<th>New call—same precedence: one active call</th>
<th>New call—same precedence: multiple active calls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One call per line</td>
<td>Multiple calls per line</td>
</tr>
<tr>
<td>Active Call</td>
<td>Rejected</td>
<td>If you accept the new call, it’s placed in the first slot. The active call is placed on hold and moved to the second slot. If all lines and call appearances are at capacity, new incoming call with the same precedence will get rejected.</td>
</tr>
<tr>
<td>Ringing State</td>
<td>Rejected</td>
<td>The new call displays in the top center corner and the current call is in the main screen.</td>
</tr>
<tr>
<td>Call on Hold</td>
<td>Rejected</td>
<td>If the user acknowledges the new call, the current call is moved to the second slot. The new call is placed in the first slot.</td>
</tr>
</tbody>
</table>

The caller’s phone displays the precedence of the outgoing call. Callee phones display call precedence on each phone line: 1 indicates the lowest precedence and 5 indicates the highest precedence.

Phone models vary in how they display precedence:

- Trio 8300: Priority-1, Priority-2, Priority-3
- Trio 8500: Priority-1, Priority-2, Priority-3
- Trio 8800: Priority-1, Priority-2, Priority-3

### Preemption Behavior on Low Priority Calls

A 180 ringing response is sent to the far end only when a call appearance is allocated for the incoming precedence call.

The following table illustrates the preemption behavior of the low priority call’s status.

#### Preemption Behavior on Low Priority Calls

<table>
<thead>
<tr>
<th>Low Priority Call's Status for Preemption</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>The call is terminated with a BYE request containing a preemption Reason header, and a local preemption tone is played for a configurable duration or until the user hangs up, whichever comes first.</td>
</tr>
<tr>
<td>Locally Held</td>
<td>The call may be terminated with a BYE request containing a preemption Reason header.</td>
</tr>
</tbody>
</table>
### Low Priority Call's Status for Preemption

<table>
<thead>
<tr>
<th>Low Priority Call's Status for Preemption</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerting</td>
<td>A 486 Busy Here response is sent to the far end containing a preemption Reason header.</td>
</tr>
<tr>
<td>Dial Tone or Setup</td>
<td>When the final call appearance is in the dial tone or setup (digit collection) state (including consultation calls) and a precedence call arrives, no action is taken until the new outgoing call is of higher priority or is not is determined. If the call is of lower priority, then the call is not placed and a preemption tone is played for a configurable duration or until the user hangs up, whichever is less. If the call is of the same or higher priority, then the incoming call is terminated by sending a 486 Busy Here response to the far end containing a preemption Reason header.</td>
</tr>
<tr>
<td>Preceding</td>
<td>If the final call appearance is in the preceding (digit collection) state (including consultation calls) when a precedence call arrives, no action is taken until it can be determined whether the new outgoing call is of higher priority or not. If the call is determined to be of lower priority, then the call is not placed and a preemption tone should be played for a configurable duration or until the user hangs up, whichever is less. If the call is determined to be of the same or higher priority, then the incoming call is terminated by sending a 486 Busy Here response to the far end containing a preemption Reason header.</td>
</tr>
</tbody>
</table>

### MLPP with AS-SIP Parameters

The following parameters configure MLPP with AS-SIP.

**voIpProt.SIP.assuredService.defaultPriority**

Default priority assigned to an outgoing call.

- 1 (default)
- 1 to 10

This value is overridden if priority is assigned from the dial plan for that number.

**voIpProt.SIP.assuredService.enable**

- 0 (default) - Disables the AS-SIP feature.
- 1 - Enables the AS-SIP feature

**voIpProt.SIP.assuredService.namespace.custom.name**

The name for the custom namespace label.

Null (default)
**voIpProt.SIP.assuredService.namespace.custom.priority.x**

The namespace precedence values, lowest to highest.

- Null (default)

**voIpProt.SIP.assuredService.precedenceThreshold**

The minimum call priority required for a call to be treated as a precedence call.

- 2 (default)
- 1 to 10

**voIpProt.SIP.assuredService.preemptionAutoTerminationDelay.local**

Set the duration after a callee preemption event that a call appearance is automatically cleared.

- 0 (default)
- 0-3600

**voIpProt.SIP.assuredService.preemptionAutoTerminationDelay.remote**

Set the duration after a caller preemption event that a call appearance is automatically cleared.

- 3 (default)
- 0-3600

**voIpProt.SIP.assuredService.serverControlled**

1 (default) - The precedence level of outgoing calls is set by the server or non-EI equipment.

0 - The precedence level is set by the phone and must not change if it is an outgoing call.

---

**International Dialing Prefix**

Enter a plus (+) symbol before you dial an international phone numbers to identify to the switch that the phone number you are dialing is international.

**International Dialing Prefix Parameters**

The following parameters configure the international dialing prefixes.

- **call.internationalDialing.enabled**
This parameter applies to all numeric dial pads on the phone, including for example, the contact directory.

Changes you make to this parameter cause a restart or reboot.

1 (default) - Disable the key tap timer that converts a double tap of the asterisk "**" symbol to the "+" symbol to indicate an international call. By default, this parameter is enabled so that a quick double tap of "**" converts immediately to "+". To enter a double asterisk "**", tap "**" once and wait for the key tap timer to expire to enter a second "**".

0 - When you disable this parameter, you cannot dial "+" and you must enter the international exit code of the country you are calling from to make international calls.

Change causes system to restart or reboot.

**call.internationalPrefix.key**

The phone supports international call prefix (+) with both "0" and "**".

0 (default) - Set the international prefix with "**".

1 - Set the international prefix with "0".
Shared Lines

Topics:

- Shared Call Appearances
- Private Hold on Shared Lines
- Intercom Calls
- Group Paging

This section shows you how to configure shared line features.

Shared Call Appearances

Shared call appearance enables an active call to display simultaneously on multiple phones in a group. All call states —active, inactive, on hold—are displayed on all phones of a group.

By default, the answering phone has sole access to the incoming call, which is called line seize. If the answering phone places the call on hold, that call becomes available for pickup to all phones in that group. You can enable other phones in the group the ability to enter a conversation on one of the group phones, which is referred to as a barge in.

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 you are using.

Shared Call Appearances Parameters

This feature is dependent on support from a SIP call server. To enable shared call appearances on your phone, you must obtain a shared line address from your SIP service provider.

A shared line is an address of record managed by a call server. The server allows multiple endpoints to register locations against the address of record.

Poly devices support Shared Call Appearance (SCA) using the SUBSCRIBE-NOTIFY method specified in RFC 6665. The events used are:

- call-info for call appearance state notification
- line-seize for the phone to ask to seize the line

Use the parameters in the following list to configure options for this feature.

reg.x.address

The user part (for example, 1002) or the user and the host part (for example, 1002@polycom.com) of the registration SIP URI.

Null (default)

string address
reg.x.type

private (default) - Use standard call signaling.
shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.

call.shared.reject

For shared line calls on the BroadWorks server.
0 - The phone displays a Reject soft key to reject an incoming call to a shared line.
1 - The Reject soft key does not display.

call.shared.exposeAutoHolds

0 (default) - No re-INVITE is sent to the server when setting up a conference on a shared line.
1 - A re-INVITE is sent to the server when setting up a conference on a shared line.
Change causes system to restart or reboot.

call.shared.oneTouchResume

0 (default) - Selecting the shared line opens all current calls that the user can choose from.
1 - All users on a shared line can resume held calls by pressing the shared line key. If more than one call is on hold, the first held call is selected and resumed.
A quick press and release of the line key resumes a call whereas pressing and holding down the line key shows a list of calls on that line.
Change causes system to restart or reboot.

call.shared.preferCallInfoCID

0 (default) - The Caller-ID information received in the 200 OK status code is not ignored if the NOTIFY message received with caller information includes display information.
1 - The Caller-ID information received in the 200 OK status code is ignored if the NOTIFY message received with caller information includes display information.

call.shared.remoteActiveHoldAsActive

1 (default) - Shared remote active/hold calls are treated as a active call on the phone.
0 - Shared remote active/hold calls are not treated as a active call on the phone.

call.shared.seizeFailReorder

1 (default) - Play a re-order tone locally on shared line seize failure.
0 - Do not play a re-order tone locally on shared line seize failure.
Change causes system to restart or reboot.
voIpProt.SIP.specialEvent.lineSeize.nonStandard

Controls the response for a line-seize event SUBSCRIBE.

1 (default) - This speeds up the processing of the response for line-seize event.
0 - This will process the response for the line seize event normally

Change causes system to restart or reboot.

reg.x.ringType

The ringer to be used for calls received by this registration. The default is the first non-silent ringer.

If you use the configuration parameters ringer13 and ringer14 on a single registered line, the phone plays SystemRing.wav.

default (default)

ringer1 to ringer24

reg.x.line.y.label

Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when u p.cfgUniqueLineLabel=1 . If reg.x.linekeys=1 , this parameter does not have any effect.

x = the registration index number starting from 1.

y = 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.

If no parameter value is set for reg.x.line.y.label , the phone automatically numbers multiple lines by prepending "<y>_", where <y> is the line index from 1 to the value set by reg.x.linekeys .

reg.x.callsPerLineKey

Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration.

12 (default)

1-24

Note: This per-registration parameter overrides call.callsPerLineKey.

reg.x.header.pearllymedia.support

0 (Default) - The p-early-media header is not supported on the specified line registration.

1 - The p-early-media header is supported by the specified line registration.

reg.X.insertOBPAddressInRoute

Shared Lines
1 (Default) - The outbound proxy address is added as the topmost route header.
0 - The outbound proxy address is not added to the route header.

**reg.x.path**

0 (Default) - The path extension header field in the Register request message is not supported for the specific line registration.
1 - The phone supports and provides the path extension header field in the Register request message for the specific line registration.

**reg.x.regevent**

0 (default) - The phone is not subscribed to registration state change notifications for the specific phone line.
1 - The phone is subscribed to registration state change notifications for the specific phone line.
This parameter overrides the global parameter volpProt.SIP.regevent.

**reg.x.rejectNDUBInvite**

Specify whether or not the phone accepts a call for a particular registration in case of a Network Determined User Busy (NDUB) event advertised by the SIP server.
0 (Default) - If an NDUB event occurs, the phone does not reject the call.
1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code.

**reg.x.server.y.specialInterop**

Specify the server-specific feature set for the line registration.
Standard (Default)
Standard
GENBAND
ALU-CTS
ocs2007r2
lync2010
lcs2005

**reg.x.gruu**

1 - The phone sends sip.instance in the REGISTER request.
0 (default) - The phone does not send sip.instance in the REGISTER request.

**reg.x.serverFeatureControl.securityClassification**

0 (default) - The visual security classification feature for a specific phone line is disabled.
1 - The visual security classification feature for a specific phone line is enabled.
**reg.x.acd-login-logout reg.x.acd-agent-available**

0 (default) - The ACD feature is disabled for registration.
1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.

**reg.x.auth.domain**

The domain of the authorization server that is used to check the user names and passwords.
Null (default) string

**reg.x.auth.optimizedInFailover**

The destination of the first new SIP request when failover occurs.
0 (default) - The SIP request is sent to the server with the highest priority in the server list.
1 - The SIP request is sent to the server which sent the proxy authentication request.

**reg.x.auth.password**

The password to be used for authentication challenges for this registration.
Null (default)
string - It overrides the password entered into the Authentication submenu on the Settings menu of the phone.

**reg.x.auth.userId**

User ID to be used for authentication challenges for this registration.
Null (default)
string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication submenu on the Settings menu of the phone.

**reg.x.auth.useLoginCredentials**

0 - (default) The Login credentials are not used for authentication to the server on registration x.
1 - The login credentials are used for authentication to the server.

**reg.x.broadsoft.userId**

Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface.
Null (default)
string

**reg.x.broadsoft.useXspCredentials**

If this parameter is disabled, the phones use standard SIP credentials to authenticate.
1 (default) - Use this value, if phone lines are registered with a server running BroadWorks R19 or earlier.
0 - Set to 0, if phone lines are registered with a server running BroadWorks R19 SP1 or later.

**reg.x.broadsoft.xsp.password**
Enter the password associated with the BroadSoft user account for the line. Required only when `reg.x.broadsoft.useXspCredentials=1`.
Null (default)
string

**reg.x.displayName**
The display name used in SIP signaling as the default caller ID.
Null (default)
UTF-8 encoded string

**reg.x.enablePvtHoldSoftKey**
This parameter applies only to shared lines.
0 (default) - To disable user on a shared line to hold calls privately.
1 - To enable users on a shared line to hold calls privately.

**reg.x.filterReflectedBlaDialogs**
1 (default) - bridged line appearance NOTIFY messages are ignored.
0 - bridged line appearance NOTIFY messages is not ignored

**reg.x.fwd.busy.contact**
The forward-to contact for calls forwarded due to busy status.
Null (default) - The contact specified by `divert.x.contact` is used.
string - The contact specified by `divert.x.contact` is not used

**reg.x.fwd.busy.status**
0 (default) - Incoming calls that receive a busy signal is not forwarded
1 - Busy calls are forwarded to the contact specified by `reg.x.fwd.busy.contact`.

**reg.x.fwd.noanswer.contact**
Null (default) - The forward-to contact specified by `divert.x.contact` is used.
string - The forward to contact used for calls forwarded due to no answer.
**reg.x.fwd.noanswer.ringCount**

The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20.

0 - (default)
1 to 65535

**reg.x.fwd.noanswer.status**

0 (default) - The calls are not forwarded if there is no answer.
1 - The calls are forwarded to the contact specified by **reg.x.noanswer.contact** after ringing for the length of time specified by **reg.x.fwd.noanswer.ringCount**.

**reg.x.gruu**

Specify if the phone sends sip.instance in the REGISTER request.

0 (default)
1

**reg.x.label**

The text label that displays next to the line key for registration x.

The maximum number of characters for this parameter value is 256; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters you use. Parameter values that exceed the phone's maximum display length are truncated by ellipses (...). The rules for parameter up.cfgLabelElide determine how the label is truncated.

Null (default) - the label is determined as follows:

- If **reg.1.useteluriAsLineLabel=1**, then the tel URI/phone number/address displays as the label.
- If **reg.1.useteluriAsLineLabel=0**, then the value for **reg.x.displayName** if available, displays as the label. If **reg.x.displayName** is unavailable, the user part of **reg.x.address** is used.

UTF-8 encoded string

**reg.x.lineAddress**

The line extension for a shared line. This parameter applies to private lines and BroadSoft call park and retrieve. If there is no extension provided for this parameter, the call park notification is ignored for the shared line.

Null (default)
String

**reg.x.lineKeys**
Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model.

1 (default)
1 to max

**reg.x.lisdisclaimer**

This parameter sets the value of the location policy disclaimer. For example, the disclaimer may be “Warning: If you do not provide a location, emergency services may be delayed in reaching your location should you need to call for help.”

Null (default)
string, 0 to 256 characters

**reg.x.musicOnHold.uri**

A URI that provides the media stream to play for the remote party on hold.

Null (default) - This parameter does not overrides voIpProt.SIP.musicOnHold.uri.
a SIP URI - This parameter overrides voIpProt.SIP.musicOnHold.uri.

**reg.x.offerFullCodecListUponResume**

1 (default) - The phone sends full audio and video capabilities after resuming a held call irrespective of the audio and video capabilities negotiated at the initial call answer.
0 - The phone does not send full audio and video capabilities after resuming a held call.

**reg.x.outboundProxy.address**

The IP address or hostname of the SIP server to which the phone sends all requests.

Null (default)
IP address or hostname

**reg.x.outboundProxy.failOver.failBack.mode**

The mode for failover failback (overrides reg.x.server.y.failOver.failBack.mode).

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 configured for the server that the phone is registered to.

**reg.x.outboundProxy.failOver.failBack.timeout**

3600 (default) - The time to wait (in seconds) before failback occurs (overrides reg.x.server.y.failOver.failBack.timeout).
0, 60 to 65535 - The phone does not fail back until a failover event occurs with the current server.

**reg.x.outboundProxy.failOver.failRegistrationOn**

1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration.
0 - The reRegisterOn parameter is enabled, existing registrations remain active.

**reg.x.outboundProxy.failOver.onlySignalWithRegistered**

1 (default) - The reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs.
0 - The reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed.

**reg.x.outboundProxy.failOver.reRegisterOn**

This parameter overrides `reg.x.server.y.failOver.reRegisterOn`.

0 (default) - The phone won't attempt to register with the secondary server.
1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server.

**reg.x.outboundProxy.port**

The port of the SIP server to which the phone sends all requests.

0 - (default)
1 to 65535

**reg.x.outboundProxy.transport**

The transport method the phone uses to communicate with the SIP server.

DNSnapt (default)
DNSnapt, TCPpreferred, UDPOnly, TLS, TCPOnly

**reg.x.proxyRequire**

Null (default) - No Proxy-Require is sent.
string - Needs to be entered in the Proxy-Require header.

**reg.x.ringType**

The ringer to be used for calls received by this registration.

ringer2 (default) - Is the first non-silent ringer.
ringer1 to ringer24 - To play ringer on a single registered line.
**reg.x.serverFeatureControl.callRecording**

1 (default) - BroadSoft BroadWorks v20 call recording feature for individual phone lines is enabled.

0 - BroadSoft BroadWorks v20 call recording feature for individual phone lines is disabled.

**reg.x.serverFeatureControl.cf**

0 (default) - The server-based call forwarding is disabled.

1 - server based call forwarding is enabled.

Note: This parameter overrides `voIpProt.SIP.serverFeatureControl.cf`.

Change causes system to restart or reboot.

**reg.x.serverFeatureControl.dnd**

0 (default) - server-based do-not-disturb (DND) is disabled.

1 - server-based DND is enabled and the call server has control of DND.

Note: This parameter overrides `voIpProt.SIP.serverFeatureControl.dnd`.

Change causes system to restart or reboot.

**reg.x.serverFeatureControl.localProcessing.cf**

0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior.

1 - The phone performs local Call Forward behavior on all calls received.

Note: This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.cf`.

**reg.x.serverFeatureControl.localProcessing.dnd**

0 (default) - If `reg.x.serverFeatureControl.dnd` is set to 1, the phone does not perform local DND call behavior.

1 - The phone performs local DND call behavior on all calls received.

Note: This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.dnd`.

**reg.x.serverFeatureControl.securityClassification**

0 (default) - The visual security classification feature for a specific phone line is disabled.

1 - The visual security classification feature for a specific phone line is enabled.
reg.x.serverFeatureControl.signalingMethod

Controls the method used to perform call forwarding requests to the server.

serviceMsForwardContact (default)
string

reg.x.srtp.enable

1 (default) - The registration accepts SRTP offers.
0 - The registration always declines SRTP offers.
Change causes system to restart or reboot.

reg.x.srtp.offer

This parameter applies to the registration initiating (offering) a phone call.
0 (default) - No secure media stream is included in SDP of a SIP INVITE.
1 - The registration includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE.
Change causes system to restart or reboot.

reg.x.srtp.require

0 (default) - Secure media streams are not required.
1 - The registration is only allowed to use secure media streams.
Change causes system to restart or reboot.

reg.x.srtp.simplifiedBestEffort

1 (default) - Negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported.
0 - No SRTP is supported.

Note: This parameter overrides sec.srtp.simplifiedBestEffort.

reg.x.strictLineSeize

0 (default) - Dial prompt is provided immediately without waiting for a successful OK from the call server.
1 - The phone is forced to wait for 200 OK on registration x when receiving a TRYING notify.

Note: This parameter overrides voIpProt.SIP.strictLineSeize for registration x.

reg.x.tcpFastFailover
0 (default) - A full 32 second RFC compliant timeout is used.
1 - failover occurs based on the values of `reg.x.server.y.retryMaxCount` and `voIpProt.server.x.retryTimeOut`.

### `reg.x.thirdPartyName`
Null (default) - In all other cases.
string address - This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).

### `reg.x.useCompleteUriForRetrieve`
1 (default) - The target URI in BLF signaling uses the complete address as provided in the XML dialog document.
0 - Only the user portion of the XML dialog document is used and the current registrar’s domain is appended to create the full target URI.

Note: This parameter overrides `voipPort.SIP.useCompleteUriForRetrieve`.

### `reg.x.server.y.address`
If this parameter is set, it takes precedence even if the DHCP server is available.
Null (default) - SIP server does not accepts registrations.
IP address or hostname - SIP server that accepts registrations. If not Null, all of the parameters in this list override the parameters specified in `voIpProt.server.*`.

### `reg.x.server.y.expires`
The phone’s requested registration period in seconds.
The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period.
3600 - (default)
positive integer, minimum 10

### `reg.x.server.y.expires.lineSeize`
Requested line-seize subscription period.
30 - (default)
0 to 65535

### `reg.x.server.y.expires.overlap`
The number of seconds before the expiration time returned by server x at which the phone should try to re-register.
The phone tries to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value.

60 (default)
5 to 65535

**reg.x.server.y.failOver.failBack.mode**

duration (default) - The phone tries the primary server again after the time specified by `reg.x.server.y.failOver.failBack.timeout`.

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 configured for the server that the phone is registered to.

registration - The phone tries the primary server again when the registration renewal signaling begins.

This parameter overrides `voIPProt.server.x.failOver.failBack.mode`.

**reg.x.server.y.failOver.failBack.timeout**

3600 (default) - The time to wait (in seconds) before failback occurs.

0 - The phone does not fail back until a failover event occurs with the current server.

60 to 65535 - If set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again.

**reg.x.server.y.failOver.failRegistrationOn**

1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over.

0 - The reRegisterOn parameter is disabled, existing registrations remain active.

**reg.x.server.y.failOver.onlySignalWithRegistered**

1 (default) - Set to this value and 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 - Set to this value and 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).

**reg.x.server.y.failOver.reRegisterOn**

0 (default) - The phone does not attempt to register with the secondary server, since the phone assumes that the primary and secondary servers share registration information.
1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server.

This parameter overrides voIpProt.server.x.failOver.reRegisterOn.

**reg.x.server.y.port**

Null (default) - The port of the SIP server does not specifies registrations.

0 - The port used depends on reg.x.server.y.transport.

1 to 65535 - The port of the SIP server that specifies registrations.

**reg.x.server.y.register**

1 (default) - Calls can not be routed to an outbound proxy without registration.

0 - Calls can be routed to an outbound proxy without registration.

See voIpProt.server.x.register for more information, see SIP Server Fallback Enhancements on Polycom Phones - Technical Bulletin 5844 on Polycom Engineering Advisories and Technical Notifications.

**reg.x.server.y.registerRetry.baseTimeOut**

For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Used in conjunction with reg.x.server.y.registerRetry.maxTimeOut to determine how long to wait.

60 (default)

10 - 120 seconds

**reg.x.server.y.registerRetry.maxTimeout**

For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Use in conjunction with reg.x.server.y.registerRetry.baseTimeOut to determine how long to wait. The algorithm is defined in RFC 5626.

180 - (default)

60 - 1800 seconds

**reg.x.server.y.retryMaxCount**

The number of retries attempted before moving to the next available server.

3 - (default)

0 to 20 - 3 is used when the value is set to 0.

**reg.x.server.y.retryTimeOut**

0 (default) - Use standard RFC 3261 signaling retry behavior.
0 to 65535 - The amount of time (in milliseconds) to wait between retries.

**reg.x.server.y.subscribe.expires**

The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period.

3600 seconds - (default)

10 - 2147483647 (seconds)

You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`.

**reg.x.server.y.subscribe.expires.overlap**

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.

60 seconds (default)

5 - 65535 seconds

**reg.x.server.y.transport**

The transport method the phone uses to communicate with the SIP server.

- DNSSnaptr (default) - If `reg.x.server.y.address` is a hostname and `reg.x.server.y.port` is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If `reg.x.server.y.address` is an IP address, or a port is given, then UDP is used.
- TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails.
- UDPOnly - Only UDP is used.
- TLS - If TLS fails, transport fails. Leave port field empty (defaults to 5061) or set to 5061.
- TCPOnly - Only TCP is used.

**reg.x.server.y.useOutboundProxy**

1 (default) - Enables to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.

0 - Disable to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.

**divert.x.sharedDisabled**

1 (default) - Disables call diversion features on shared lines.

0 - Enables call diversion features on shared lines.

Change causes system to restart or reboot.
Private Hold on Shared Lines

Enable the private hold feature to enable users to hold calls without notifying other phones registered with the shared line.

When you enable the feature, users can hold a call, transfer a call, or initiate a conference call and the shared line displays as busy to others sharing the line.

Private Hold on Shared Lines Parameters

You can configure private hold only using configuration files; you cannot configure the feature on the Web Configuration Utility or from the local phone interface.

Use the parameters in the following list to configure this feature.

`call.shared.exposeAutoHolds`

Enable to send a re-INVITE to the server when setting up a conference on a shared line.

0 (default) - Disabled
1 - Enabled

Change causes system to restart or reboot.

`reg.x.enablePvtHoldSoftKey`

Enable to allow users on a shared line to hold calls privately.

0 (default) - Disabled
1 - Enabled

Note: This parameter applies only to shared lines.

Intercom Calls

The Intercom feature enables users to place an intercom call that is answered automatically on the dialed contact's phone.

This is a server-independent feature provided the server does not alter the Alert-Info header sent in the INVITE.

Creating a Custom Intercom Soft Key

By default, an Intercom soft key displays on the phone, but you have the option to provide users the ability to initiate intercom calls directly to a specified contact using enhanced feature keys (EFKs).

You do not need to disable the default Intercom soft key to create a custom soft key.

For example, you can create an intercom action string for a custom soft key in one of the following ways:

\- `$FIntercom$`
This is an F type macro that behaves as a custom Intercom soft key. Pressing the soft key opens the Intercom dial prompt users can use to place an Intercom call by entering the destination’s digits and using a speed dial or BLF button.

- `<number>$Tintercom$`

This is a T type macro that enables you to specify a Direct intercom button that always calls the number you specify in `<number>`. No other input is necessary.

**Intercom Calls Parameters**

Use the parameters in the list below to configure the behavior of the calling and answering phone.

**feature.intercom.enable**

Enable or disable the Intercom feature.

- 0 (default) - Disabled
- 1 - Enabled

**homeScreen.intercom.enable**

Enable to display the Intercom icon on the phone's home screen.

- 1 (default) - Enabled
- 0 - Disabled

**voIpProt.SIP.intercom.alertInfo**

The string you want to use in the Alert-Info header. You can use the following characters: '@', ',', '-', '_' , '.' .

If you use any other characters, NULL, or empty spaces, the call is sent as normal without the Alert-Info header.

- Intercom (default)
- Alpha - Numeric string

**Group Paging**

Group Paging enables users to make pages—one-way audio announcements—to users subscribed to a page group.

There are 25 groups/channels users can subscribe to. If you are using Group Paging with Poly Trio solution, you can only receive incoming pages. You cannot use Poly Trio solution to send outgoing pages.

Group paging users can send announcements to recipients subscribed to any of the 25 paging groups. Any announcements sent to the paging group 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 paging mode.
Note: The push-to-talk and group paging features use an IP multicast address. If you want to change the default IP multicast address, ensure that the new address does not already have an official purpose as specified in the [IPv4 Multicast Address Space Registry].

Group Paging Parameters
Administrators must enable paging and PTT before users can subscribe to a page group.

Use the parameters in the following list to configure this feature.

Note: The default port used by Group Paging conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Poly Trio system. Since the port used by People+Content is fixed and cannot be configured, configure one of the following workarounds:

- Configure a different port for Group Paging using parameter ptt.port or
- Disable People+Content IP using parameter content.ppcipServer.enabled='0'.

ptt.address
The multicast IP address to send page audio to and receive page audio from.

224.0.1.116 (default)
Multicast IP address.

ptt.pageMode.allowOffHookPages
Enable to play group pages on handsets while they are on active calls.

0 (default) - Disabled. Priority and Emergency pages still play while handsets are on active calls.
1 - Enabled.

ptt.pageMode.defaultGroup
The paging group used to transmit an outgoing page if the user does not explicitly specify a group.

1 (default)
1 to 25

ptt.pageMode.transmit.timeout.continuation
The time (in seconds) to add to the initial timeout (ptt.pageMode.transmit.timeout.initial) for terminating page announcements. If this value is non-zero, Extend displays on the phone. Pressing Extend continues the initial timeout for the time specified by this parameter. If 0, announcements cannot be extended.

60 (default)
0 to 65535
**ptt.pageMode.transmit.timeout.initial**

The number of seconds to wait before automatically terminating an outgoing page announcement.

- 0 (default) - The page announcements do not automatically terminate.
- 0 to 65535 - The page announcements automatically terminate.

**ptt.pageMode.priorityGroup**

The paging group to use for priority pages.

- 24 (default)
- 1 to 25

**ptt.pageMode.payloadSize**

The page mode audio payload size.

- 20 (default)
- 10, 20, ..., 80 milliseconds

**ptt.pageMode.emergencyGroup**

The paging group used for emergency pages.

- 25 (default)
- 1 to 25

**ptt.pageMode.codec**

The audio codec to use for outgoing group pages. Incoming pages are decoded according to the codec specified in the incoming message.

- G.722 (default)
- G.711Mu, G.726QI, or G.722

**ptt.pageMode.displayName**

This display name is shown in the caller ID field of outgoing group pages. If Null, the value from `reg.1.displayName` is used.

- NULL (default)
- up to 64 octet UTF-8 string

**ptt.pageMode.enable**

Enable or disable group paging.

- 0 (default) - Disabled
- 1 - Enabled
**ptt.pageMode.group.x.available**
Enable to make the group (x) available to the user.

- 1 (default) - Enabled
- 0 - Disabled

**ptt.pageMode.group.x.allowReceive**
Enable to allow the phone to receive pages from the group (x).

- 1 (default) - Enabled
- 0 - Disabled

**ptt.pageMode.group.x.allowTransmit**
Enable to allow outgoing announcements to the group.

- 1 (default) - Enabled
- 0 - Disabled

**ptt.pageMode.group.x.label**
The label to identify the group

- ch24: Priority, ch25: Emergency, others: Null
- ch1, 24, 25: 1, others: 0 (default)
- string

**ptt.pageMode.group.x.subscribed**
Subscribe the phone to the group.

A page mode group x, where x= 1 to 25. The **label** is the name used to identify the group during pages.

- If **available** is disabled (0), the user cannot access the group or subscribe and the other page mode group parameters is ignored. If enabled, the user can access the group and choose to subscribe.

- If **allowTransmit** is disabled (0), the user cannot send outgoing pages to the group. If enabled, the user may send outgoing pages.

- 1 (default) - If enabled, the phone subscribes to the group.
- 0 - If disabled, the phone does not subscribe to the group.
When you set up user profiles, you enable users to access their personal phone settings, including their contact directory, speed dials, and other phone settings from any phone on the network. This feature is particularly useful for remote and mobile workers who do not have a dedicated work space and conduct their business in more than one location. This feature is also useful if an office has a common conference phone from which multiple users need to access their personal settings.

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.

If you set up the user profile feature, a user can log in to a phone by entering their user ID and password. The default password is 123. If the user profile feature is set up on your company's phones, users can:

• Log in to a phone to access their personal phone settings.
• Place a call to an authorized number from a phone that is in the logged out state.
• Change their user password.
• Log out of a phone after they finish using it.

If a user changes any settings while logged in to a phone, the settings save and display the next time the user logs in to another phone. When a user logs out, the user's personal phone settings are no longer displayed.

User Profile Parameters

Before you configure user profiles, you must complete the following:

• Create a phone configuration file, or update an existing file, to enable the feature's settings.
• Create a user configuration file in the format <user>.cfg to specify the user's password, registration, and other user-specific settings that you want to define.

Important: You can reset a user's password by removing the password parameter from the override file. This causes the phone to use the default password in the <user>.cfg file.

When you set up the user profile feature, you can set the following conditions:

• If users are required to always log in to use a phone and access their personal settings.
• If users are required to log in and have the option to use the phone as is without access to their personal settings.
• If users are automatically logged out of the phone when the phone restarts or reboots.
• If users remain logged in to the phone when the phone restarts or reboots.

Use the parameters in the following list to enable users to access their personal phone settings from any phone in the organization.

**prov.login.automaticLogout**

Specify the amount of time before a non-default user is logged out.

- 0 minutes (default)
- 0 to 46000 minutes

**prov.login.defaultOnly**

- 0 (default) - The phone cannot have users other than the default user.
- 1 - The phone can have users other than the default user.

**prov.login.defaultPassword**

Specify the default password for the default user.

NULL (default)

**prov.login.defaultUser**

Specify the name of the default user. If a value is present, the user is automatically logged in when the phone boots up and after another user logs out.

NULL (default)

**prov.login.enabled**

- 0 (default) - The user profile is disabled.
- 1 - The user profile feature is enabled.

**prov.login.localPassword.hashed**

- 0 (default) - The user's local password is formatted and validated as clear text.
- 1 - The user's local password is created and validated as a hashed value.

**prov.login.localPassword**

Specify the password used to validate the user login. The password is stored either as plain text or as an encrypted SHA1 hash.

123 (default)

**prov.login.persistent**

- 0 (default) - Users are logged out if the handset reboots.
1 - Users remain logged in when the phone reboots.

**prov.login.required**

Set whether the phone requires the user to log in to the phone to use it.
- 0 (default) - Login not required.
- 1 - Login is required.

**prov.login.useProvAuth**

- 0 (default) - The phone does not use server authentication.
- 1 - The phones use server authentication and user login credentials are used as provisioning server credentials.

**voIpProt.SIP.specialEvent.checkSync.downloadCallList**

- 0 (default) - The phone does not download the call list for the user after receiving a checksync event in the NOTIFY.
- 1 - The phone downloads the call list for the user after receiving a checksync event in the NOTIFY.

### Remotely Logging Out Users

Note that if an unexpected reboot occurs while a user is logged in, the user is not logged out and the phone returns to the user profile after reboot.

If a user is not logged out from a phone and other users are not prevented from logging in, the user can ask the administrator to log out remotely. Administrators can log out a user remotely with a checksync event in the NOTIFY by setting the parameter `profileLogout=remote`.

### Authentication of User Profiles

When using the User Profiles feature, you can 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.

### Server Authentication of User Profiles

Instead of phone-based authentication of user profiles, you can configure server authentication.

When you enable server authentication, you set up user accounts on the provisioning server and each user can authenticate their phone 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.
Create a Generic Profile Using Server Authentication

Create a generic profile and generic credentials on the provisioning server when a user is not logged into the phone.

If you enable server authentication of user profiles, the following parameters do not apply and you do not need to configure them:

- prov.login.defaultUser
- prov.login.defaultPassword
- prov.login.defaultOnly
- prov.login.localPassword
- prov.login.localPassword.hashed

Procedure

1. On the server, create an account and directory for the generic profile, for example, Generic_Profile.
2. In the Generic_Profile directory, create a configuration file for a generic profile the phone uses by default, for example, genericprofile.cfg.
3. In genericprofile.cfg, include registration and server details and set all phone feature parameters.

You must set the following parameters to use server authentication:

- prov.login.enabled="1"
- prov.login.useProvAuth="1"
- prov.login.persistent="1" Note that if you enable prov.login.enabled=1 and do not enable prov.login.useProvAuth=0, users are authenticated by a match with credentials you store in the user configuration file <user>.cfg.

4. Create a master configuration file 000000000000.cfg for all the phones, or a <MACAddress>.cfg for each phone, and add genericprofile.cfg to the CONFIG_FILES field.
5. Set the provisioning server address and provisioning server user name and password credentials for the generic user account on the phone at Settings > Advanced > Provisioning Server details and inform users of their user profile credentials.

The following override files are uploaded to the generic profile directory:

- Log files
- Phone menu settings
- Web Configuration Utility settings
- Call logs
- Contact directory file

Create a User Profile Using Server Authentication

Create a user profile in the Home directory of each user with a user-specific configuration file that you store on the provisioning server with a unique name as well as user-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.
Procedure

1. On the server, create an account and a directory for each user, for example, User1, User2.
2. In each user directory, create a configuration file for each user, for example, User1.cfg, User2.cfg, that contains the user's registration details and feature settings.

The following override files are uploaded to the generic profile account on the server:
- Log files
- Web Configuration Utility settings

The following override files are uploaded to the user profile account on the server:
- Phone menu settings
- Contact directory file

Phone Authentication of User Profiles

You can create default credentials and user profiles without use of server authentication.

Create Default Credentials and a Profile for a Phone

You can choose to define default credentials for a phone, which the phone uses to automatically log itself in each time an actual user logs out or the phone restarts or reboots.

When the phone logs itself in using the default login credentials, a default phone profile displays, and users retain the option to log in and view their personal settings.

You can create a new phone configuration file for the default profile, then add and set the attributes for the feature. Or, you can update an existing phone configuration file to include the user login parameters you want to change.

Important: Poly recommends that you create a single default user password for all users.

Procedure

1. Add the prov.login* parameters you want to use to your configuration.
2. Set values for the user login parameters and save.

Create a User Configuration File

Create a configuration file for each user that you want to enable to log in to the phone.

The name of the file should specify the user's login ID. In the file, specify any user-specific settings that you want to define for the user.

If a user updates their password or other user-specific settings on the phone, the updates are stored in <user>-phone.cfg, not <MACaddress>-phone.cfg.

If a user updates their contact directory while logged in to a phone, the updates are stored in <user>-directory.xml. Directory updates display each time the user logs in to a phone. For certain phones, an up-to-date call lists history is defined in <user>-calls.xml. This list is retained each time the user logs in to their phone. The following is a list of configuration parameter precedence (from first to last) for a phone that has the user profile feature enabled:
- <user>-phone.cfg
- Web Configuration Utility
• Configuration files listed in the master configuration file (including <user>.cfg)
• Default values

**Note:** To convert a phone-based deployment to a user-based deployment, copy the <MACaddress>-phone.cfg file to <user>-phone.cfg and copy phoneConfig<MACaddress>.cfg to <user>.cfg.

---

**Procedure**

1. On the provisioning server, create a user configuration file for each user.
2. Name each file the ID the user will use to log in to the phone.
   
   For example, if the user's login ID is user100, the name of the user's configuration file is user100.cfg.
3. In each <user>.cfg file, you are required to add and set values for the user's login password.
4. Add and set values for any user-specific parameters, such as:
   
   • Registration details such as the number of lines the profile displays and line labels.
   • Feature settings such as microbrowser settings).

**Caution:** If you add optional user-specific parameters to <user>.cfg, add only those parameters that will not cause the phone to restart or reboot when the parameter is updated.
Network

Topics:

• Two-Way Active Measurement Protocol
• System and Model Names
• Incoming Network Signaling Validation
• SIP Subscription Timers
• Enhanced IPv4 ICMP Management
• Provisional Polling of Phones
• SIP Instance Support
• IP Type-of-Service
• Static DNS Cache
• DNS SIP Server Name Resolution
• Server Redundancy
• Network Address Translation (NAT)
• Real-Time Transport Protocol (RTP) Ports
• Wireless Network Connectivity (Wi-Fi)
• Bluetooth and NFC-Assisted Bluetooth for Poly Trio Systems

Polycom UC Software allows you to make custom network configurations.

Related Links

Supported Network Configurations

Two-Way Active Measurement Protocol

Poly UC Software supports Two-Way Active Measurement Protocol (TWAMP), which is RFC 5357 compliant, to check network performance by measuring the round-trip time between two devices using TWAMP protocols.

TWAMP defines the following protocols:

• TWAMP Control protocol, which uses TCP.
• TWAMP Test protocol, which uses UDP.

TWAMP Limitations

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 is limited to handle a maximum of 10 sessions per client
Two-Way Active Measurement Protocol Configuration Parameters

The following list includes the new or modified parameters for the two-way active measurement protocol feature.

**feature.twamp.enabled**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (default)</td>
<td>Disable TWAMP protocol support.</td>
</tr>
<tr>
<td>1</td>
<td>Enable TWAMP protocol support.</td>
</tr>
</tbody>
</table>

**twamp.port.udp.PortRangeEnd**

Set the TWAMP UDP session max port range value.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>60000 (default)</td>
<td></td>
</tr>
<tr>
<td>1024 - 65486</td>
<td></td>
</tr>
</tbody>
</table>

**twamp.port.udp.PortRangeStart**

Set the TWAMP UDP session start port range value.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000 (default)</td>
<td></td>
</tr>
<tr>
<td>1024 - 65485</td>
<td></td>
</tr>
</tbody>
</table>

**twamp.udp.maxSession**

Set the maximum UDP session supported by TWAMP.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (default)</td>
<td></td>
</tr>
<tr>
<td>1 - 10</td>
<td></td>
</tr>
</tbody>
</table>

System and Model Names

The following table outlines the system and model names that Poly phones transmit with network protocols. If you need to customize your network for a specific phone model, you can parse the network packets for these strings.

<table>
<thead>
<tr>
<th>Poly Trio System and Model Names</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
</tr>
<tr>
<td>Poly Trio 8300</td>
</tr>
<tr>
<td>Poly Trio 8500</td>
</tr>
<tr>
<td>Poly Trio 8800</td>
</tr>
</tbody>
</table>
Incoming Network Signaling Validation

You can choose from the following optional levels of security for validating incoming network signaling:

- Source IP address validation
- Digest authentication
- Source IP address validation and digest authentication

Network Signaling Validation Parameters

The following list includes the parameters you can use to specify the validation type, method, and the events for validating incoming network signaling.

**voIPProt.SIP.requestValidation.x.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.

Change causes system to restart or reboot.

**voIPProt.SIP.requestValidation.x.request**

Sets the name of the method for which validation will be applied.

Null (default)

INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE

Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.

Change causes system to restart or reboot.

**voIPProt.SIP.requestValidation.x.request.y.event**
Determines which events specified with the Event header should be validated; only applicable when `voIpProt.SIP.requestValidation.x.request` is set to SUBSCRIBE or NOTIFY.

Null (default) - all events will be validated.
A valid string - specified event will be validated.
Change causes system to restart or reboot.

**SIP Subscription Timers**

You can configure a subscription expiry independently of the registration expiry.
You can also configure an overlap period for a subscription independently of the overlap period for the registration, and a subscription expiry and subscription overlap for global SIP servers and per-registration SIP servers. Note that per-registration configuration parameters override global parameters. If you have not explicitly configured values for any user features, the default subscription values are used.

**SIP Subscription Timers Parameters**

Use the parameters in the following list to configure when a SIP subscription expires and when expirations overlap.

- **`voIpProt.server.x.subscribe.expires`**
  The phone’s requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period.
  - 3600 - (default)
  - 10 - 2147483647

- **`voIpProt.server.x.subscribe.expires.overlap`**
  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.
  - 60 - (default)
  - 5 - 65535 seconds

- **`reg.x.server.y.subscribe.expires`**
  The phone’s requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period.
  - 3600 seconds - (default)
  - 10 - 2147483647 (seconds)
  You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`. 
reg.x.server.y.subscribe.expires.overlap

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.

60 seconds (default)
5 - 65535 seconds

Enhanced IPv4 ICMP Management

Poly phones support IPv4 by enabling the phone to ignore Internet Control Message Protocol (ICMP) redirect requests for an alternate path from the router or gateway.

IPv4 Parameters

You can configure IPv4 using parameters listed below.

device.icmp.ipv4IcmpIgnoreRedirect.set

0 (default) - The phone does not allow to use device.icmp.ipv4IcmpIgnoreRedirect parameter to configure Enhanced IPv4 ICMP Management feature.

1 - The phone allows to use device.icmp.ipv4IcmpIgnoreRedirect parameter to configure Enhanced IPv4 ICMP Management feature.

device.icmp.ipv4IcmpIgnoreRedirect

1 (default) - The phone ignores ICMP redirect requests for an alternate path from the router or gateway.

0 - The phone allows ICMP redirects.

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 to be greater than one day with the period rounded up to the nearest day, the phone polls on a random day based on the phone's MAC address and within a random time set by the start and end polling time.
Provisional Polling Parameters

Use the parameters in the following list to configure provisional polling.

Note: If `prov.startupCheck.enabled` is set to 0, then the phones do not look for the sip.ld or the configuration files when they reboot, lose power, or restart. Instead, they look only when receiving a checksync message, a polling trigger, or a manually started update from the menu or web UI.

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

**prov.polling**

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

**prov.polling.enabled**

0 (default) - Disables the automatic polling for upgrades.
1 - Initiates the automatic polling for upgrades.

**prov.polling.mode**

The polling modes for the provisioning server.
- **abs** (default) - The phone polls every day at the time specified by `prov.polling.time`.
- **rel** - The phone polls after the number of seconds specified by `prov.polling.period`.
- **random** - The phone polls at random between a starting time set in `prov.polling.time` and an end time set in `prov.polling.timeRandomEnd`.

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 day within the period is decided based upon the phone’s MAC address and does not change with a reboot whereas the time within the start and end is calculated again with every reboot.

**prov.polling.period**

The polling period is calculated in seconds and is rounded up to the nearest number of days in an absolute and random mode. If this is set to a time greater than 86400 (one day) polling occurs on a random day based on the phone’s MAC address.

86400 (default) - Number of seconds in a day.
Integer - An integer value greater than 3600 seconds.

**prov.polling.time**

The start time for polling on the provisioning server.

03:00 (default)

hh:mm
**prov.polling.timeRandomEnd**

The stop time for polling on the provisioning server.

Null (default)

hh:mm

**Example Provisional Polling Configuration**

The following are examples of polling configurations you can set up:

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

**SIP Instance Support**

In environments where multiple phones are registered using the same address of record (AOR), the phones are identified by their IP address.

However, firewalls set up in these environments can regularly change the IP addresses of phones for security purposes. You can configure SIP instance to identify individual phones instead of using IP addresses. This feature complies with RFC 3840.

**SIP Instance Parameter**

The parameter `reg.x.gruu` 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. Refer to the following list for the parameters to configure this feature.

**reg.x.gruu**

1 - The phone sends sip.instance in the REGISTER request.

0 (default) - The phone does not send sip.instance in the REGISTER request.
**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.

Each TOS bit can be set to either 0 or 1. The precedence field can be set to a value from 0 through 7. The type of service can be configured specifically for RTP packets and call control packets, such as SIP signaling packets.

**IP Type-of-Service Parameters**

You can configure the IP TOS feature specifically for RTP and call control packets, such as SIP signaling packets.

Type of Service (ToS) and the Differentiated Services Code Point (DSCP) allows specification of a datagrams 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.

The parameters listed below configure the type of service field RTP and call control packets for Quality of Service (QoS).

**qos.ethernet.tcpQosEnabled**

- **0** (default) - The phone does not send configured QoS priorities for SIP over TCP transport.
- **1** - The phone sends configured QoS priorities for SIP over TCP transport.

Change causes system to restart or reboot.

**qos.ip.callControl.dscp**

Specify the DSCP of packets.

- If the value is set to the default NULL the phone uses qos.ip.callControl.* parameters.
- If the value is not NULL, this parameter overrides qos.ip.callControl.* parameters.

Change causes system to restart or reboot.

**qos.ip.callControl.max_reliability**

Set the max reliability bit in the IP ToS field of the IP header used for call control.

- **0** (default) - The bit in the IP ToS field of the IP header is not set.
- **1** - The bit is set.

Change causes system to restart or reboot.

**qos.ip.callControl.max_throughput**

Set the throughput bit in the IP ToS field of the IP header used for call control.

- **0** (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

qos.ip.callControl.min_cost
Set the min cost bit in the IP ToS field of the IP header used for call control.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

qos.ip.callControl.min_delay
Set the min delay bit in the IP ToS field of the IP header used for call control.
1 (default) - The bit is set.
0 - The bit in the IP ToS field of the IP header is not set.
Change causes system to restart or reboot.

qos.ip.callControl.precedence
Set the min delay bit in the IP ToS field of the IP header used for call control.
5 (default)
0 - 7
Change causes system to restart or reboot.

qos.ip.rtp.dscp
Specify the DSCP of packets.
If the value is set to the default NULL, the phone uses quality.ip.rtp.* parameters.
If the value is not NULL, this parameter overrides quality.ip.rtp.* parameters.
• Null (default)
• 0 to 63
• EF
• Any of AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43
Change causes system to restart or reboot.

qos.ip.rtp.max_reliability
Set the max reliability bit in the IP ToS field of the IP header used for RTP.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.
**qos.ip.rtp.max_throughput**
Set the throughput bit in the IP ToS field of the IP header used for RTP.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

**qos.ip.rtp.min_cost**
Set the min cost bit in the IP ToS field of the IP header used for RTP.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

**qos.ip.rtp.min_delay**
Set the min delay bit in the IP ToS field of the IP header used for RTP.
1 (default) - The bit is set.
0 - The bit in the IP ToS field of the IP header is not set.
Change causes system to restart or reboot.

**qos.ip.rtp.precedence**
Set the precedence bit in the IP ToS field of the IP header used for RTP.
5 (default)
0 - 7
Change causes system to restart or reboot.

**qos.ip.rtp.video.dscp**
Allows you to specify the DSCP of packets.
If the value is set to the default NULL, the phone uses qos.ip.rtp.video.* parameters.
If the value is not NULL, this parameter overrides qos.ip.rtp.video.* parameters.
- NULL (default)
- 0 to 63
- EF
- Any of AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43
Change causes system to restart or reboot.

**qos.ip.rtp.video.max_reliability**
Set the reliability bits in the IP ToS field of the IP header used for RTP video.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

**qos.ip.rtp.video.max_throughput**
Set the throughput bits in the IP ToS field of the IP header used for RTP video.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

**qos.ip.rtp.video.min_cost**
Set the min cost bits in the IP ToS field of the IP header used for RTP video.
0 (default) - The bit in the IP ToS field of the IP header is not set.
1 - The bit is set.
Change causes system to restart or reboot.

**qos.ip.rtp.video.min_delay**
Set the min delay bits in the IP ToS field of the IP header used for RTP video.
1 (default) - The bit is set.
0 - The bit in the IP ToS field of the IP header is not set.
Change causes system to restart or reboot.

**qos.ip.rtp.video.precedence**
Set the precedence bits in the IP ToS field of the IP header used for RTP video.
5 (default)
0 - 7
Change causes system to restart or reboot.

**Static DNS Cache**
Failover redundancy can be used only when the configured IP server hostname resolves (through SRV or A record) to multiple IP addresses.
Unfortunately, the DNS cache cannot always be configured to take advantage of failover redundancy.
You can statically configure a set of DNS NAPTR SRV and/or A records into the phone. You can enter a maximum of 12 record entries for DNS-A, DNS-NAPTR, and DNS-SRV. records.
Support for negative DNS caching as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server. For more information, see RFC2308.

Configuring Static DNS

If a phone is not configured with a DNS server, when the phone attempts to resolve a hostname within the static DNS cache, it always returns the results from the static cache.

Phones configured with a DNS server behave as follows:

1. The phone makes an initial attempt to resolve a hostname that is within the static DNS cache. For example, a query is made to the DNS if the phone registers with its SIP registrar.

2. If the initial DNS query returns no results for the hostname or cannot be contacted, then the values in the static cache are used for their configured time interval.

3. After the configured time interval has elapsed, a resolution attempt of the hostname again results in a query to the DNS.

4. If a DNS query for a hostname that is in the static cache returns a result, the values from the DNS are used and the statically cached values are ignored.

Static DNS Parameters

Use the following parameters to configure static DNS settings.

**reg.x.address**

The user part (for example, 1002) or the user and the host part (for example, 1002@polycom.com) of the registration SIP URI or the H.323 ID/extension.

Null (default)

string address

**reg.x.server.y**

Specify the call server used for this registration.

**reg.x.server.y.specialInterop**

Specify the server-specific feature set for the line registration.

All other phones: Standard (default), GENBAND, ALU-CTS, ocs2007r2, lync2010, lcs2005

**reg.x.server.y.address**

If this parameter is set, it takes precedence even if the DHCP server is available.

Null (default) - SIP server does not accepts registrations.

IP address or hostname - SIP server that accepts registrations. If not Null, all of the parameters in this list override the parameters specified in voIpProt.server.*.

**reg.x.server.y.expires**
The phone's requested registration period in seconds. The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period.

3600 - (default)
positive integer, minimum 10

**reg.x.server.y.expires.lineSeize**

Requested line-seize subscription period.

30 - (default)
0 to 65535

**reg.x.server.y.expires.overlap**

The number of seconds before the expiration time returned by server x at which the phone should try to re-register. The phone tries to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value.

60 (default)
5 to 65535

**reg.x.server.y.failOver.failBack.mode**

duration (default) - The phone tries the primary server again after the time specified by reg.x.server.y.failOver.failBack.timeout.

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 configured for the server that the phone is registered to.

registration - The phone tries the primary server again when the registration renewal signaling begins.

Note: This parameter overrides voIpProt.server.x.failOver.failBack.mode.

**reg.x.server.y.failOver.failBack.timeout**

3600 (default) - The time to wait (in seconds) before failback occurs.

0 - The phone does not fail back until a failover event occurs with the current server.

60 to 65535 - If set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again.

**reg.x.server.y.failOver.failRegistrationOn**

1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over.

0 - The reRegisterOn parameter is disabled, existing registrations remain active.
**reg.x.server.y.failOver.onlySignalWithRegistered**

1 (default) - Set to this value and `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 - Set to this value and `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).

**reg.x.server.y.failOver.reRegisterOn**

0 (default) - The phone does not attempt to register with the secondary server, since the phone assumes that the primary and secondary servers share registration information.

1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server.

Note: This parameter overrides `voIpProt.server.x.failOver.reRegisterOn`.

**reg.x.server.y.port**

Null (default) - The port of the SIP server does not specify registrations.

0 - The port used depends on `reg.x.server.y.transport`.

1 to 65535 - The port of the SIP server that specifies registrations.

**reg.x.server.y.register**

1 (default) - Calls can not be routed to an outbound proxy without registration.

0 - Calls can be routed to an outbound proxy without registration.

See `voIpProt.server.x.register` for more information, see *SIP Server Fallback Enhancements on Polycom Phones - Technical Bulletin 5844* on Polycom Engineering Advisories and Technical Notifications.

**reg.x.server.y.registerRetry.baseTimeOut**

For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Used in conjunction with `reg.x.server.y.registerRetry.maxTimeOut` to determine how long to wait.

60 (default)

10 - 120 seconds

**reg.x.server.y.registerRetry.maxTimeOut**
For registered line x, set y to the maximum time period the phone waits before trying to re-
register with the server. Use in conjunction with r
gx.server.y.registerRetry.baseTimeOut to determine how long to wait. The
algorithm is defined in RFC 5626.
180 - (default)
60 - 1800 seconds

reg.x.server.y.retryMaxCount
The number of retries attempted before moving to the next available server.
3 - (default)
0 to 20 - 3 is used when the value is set to 0.

reg.x.server.y.retryTimeOut
0 (default) - Use standard RFC 3261 signaling retry behavior.
0 to 65535 - The amount of time (in milliseconds) to wait between retries.

reg.x.server.y.subscribe.expires
The phone’s requested subscription period in seconds after which the phone attempts to
resubscribe at the beginning of the overlap period.
3600 seconds - (default)
10 - 2147483647 (seconds)
You can use this parameter in conjunction with
reg.x.server.y.subscribe.expires.overlap.

reg.x.server.y.subscribe.expires.overlap
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.
60 seconds (default)
5 - 65535 seconds

reg.x.server.y.transport
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, do 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 a port is given, then UDP is used.
TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails.
UDPOnly - Only UDP is used.

TLS - If TLS fails, transport fails. Leave port field empty (defaults to 5061) or set to 5061.

TCPOnly - Only TCP is used.

`reg.x.server.y.useOutboundProxy`

1 (default) - Enables to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.
0 - Disable to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.

`divert.x.sharedDisabled`

1 (default) - Disables call diversion features on shared lines.
0 - Enables call diversion features on shared lines.
Change causes system to restart or reboot.

`dns.cache.A.x`

Specify the DNS A address, hostname, and cache time interval.

`dns.cache.A.x.address`

Null (default)
IP version 4 address

`dns.cache.A.x.name`

Null (default)
valid hostname

`dns.cache.A.x.ttl`

The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again.

300 (default)
300 to $536870912$ ($2^{29}$), seconds

`dns.cache.NAPTR.x`

Specify the DNS NAPTR parameters, including: name, order, preference, regexp, replacement, service, and ttl.

`dns.cache.NAPTR.x.flags`
The flags to control aspects of the rewriting and interpretation of the fields in the record. Characters are case-sensitive. At this time, only 'S', 'A', 'U', and 'P' are defined as flags. See RFC 2915 for details of the permitted flags.

Null (default)

A single character from [A-Z, 0-9]

dns.cache.NAPTR.x.name
Null (default)
domain name string - The domain name to which this resource record refers.

dns.cache.NAPTR.x.order
0 (default)
0 to 65535 - An integer that specifies the order in which the NAPTR records must be processed to ensure the correct ordering of rules.

dns.cache.NAPTR.x.preference
0 (default)
0 to 65535 - A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed. Low numbers are processed before high numbers.

dns.cache.NAPTR.x.regexp
This parameter is currently unused. Applied to the original string held by the client. The substitution expression is applied in order to construct the next domain name to lookup. The grammar of the substitution expression is given in RFC 2915.
Null (default) string containing a substitution expression

dns.cache.NAPTR.x.replacement
The next name to query for NAPTR records depending on the value of the flags field. It must be a fully qualified domain-name.
Null (default)
domain name string with SRV prefix

dns.cache.NAPTR.x.service
Specifies the service(s) available down this rewrite path. For more information, see RFC 2915.
Null (default)
string

dns.cache.NAPTR.x.ttl
The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again. 300 (default) 300 to 536870912 (2^29), seconds

**dns.cache.A.networkOverride**

0 (default) - Does not allow the static DNS A record entry to take priority over dynamic network DNS.

1 – Allows the static DNS cached A record entry to take priority over dynamic network DNS. Moreover, the DNS TTL value is ignored.

**dns.cache.SRV.x.**

Specify DNS SRV parameters, including: name, port, priority, target, ttl, and weight.

**dns.cache.SRV.x.name**

Null (default)

Domain name string with SRV prefix

**dns.cache.SRV.x.port**

The port on this target host of this service. For more information, see [RFC 2782](https://tools.ietf.org/html/rfc2782).

0 (default)

0 to 65535

**dns.cache.SRV.x.priority**

The priority of this target host. For more information, see [RFC 2782](https://tools.ietf.org/html/rfc2782).

0 (default)

0 to 65535

**dns.cache.SRV.x.target**

Null (default)

domain name string - The domain name of the target host. For more information, see [RFC 2782](https://tools.ietf.org/html/rfc2782).

**dns.cache.SRV.x.ttl**

The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again.
300 (default)
300 to 536870912 (2^29), seconds

dns.cache.SRV.x.weight
A server selection mechanism. For more information, see RFC 2782.
0 (default)
0 to 65535

tcpIpApp.dns.address.overrideDHCP
Specifies how DNS addresses are set.
0 (default) - DNS address requested from the DHCP server.
1 - DNS primary and secondary address is set using the parameters tcpIpApp.dns.server and tcpIpApp.dns.altServer.
Change causes system to restart or reboot.

tcpIpApp.dns.domain.overrideDHCP
Specifies how the domain name is retrieved or set.
0 (default) - Domain name retrieved from the DHCP server, if one is available.
1 - DNS domain name is set using the parameter tcpIpApp.dns.domain.
Change causes system to restart or reboot.

dns.cache.dynamicRestore.enable
1 – Allows the phone to restore the expired cache entries to a specified TTL when the DNS server isn’t reachable.
0 (default) – Doesn’t allow the phone to restore the expired cache entries to a specified TTL when the DNS server isn’t reachable.

dns.cache.dynamicRestore.ttl
Specify a TTL value to restore the expired cache entries when the DNS server isn’t reachable.
120 (default)
90 to 600 seconds

reg.x.secureTransportRequiresSrtp
0 (default) – Doesn’t allow the phone to dynamically overwrite the configured values of reg.x.srtp.offer parameter and reg.x.srtp.require parameter based on the NAPTR response for per line registration.
1 – Allows the phone to dynamically overwrite the configured values of `reg.x.srtp.offer` parameter and `reg.x.srtp.require` parameter based on the NAPTR response for per line registration to enable SRTP only.

Example Static DNS Cache Configuration

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

The addresses listed in this example are read by Polycom UC Software in the order listed.

When the static DNS cache is not used, the `site.cfg` configuration looks as follows:

When the static DNS cache is used, the `site.cfg` configuration looks as follows:

Example: Static DNS Cache with A Records

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

When the static DNS cache is not used, the `site.cfg` configuration looks as follows:

When the static DNS cache is used, the `site.cfg` configuration looks as follows:
The `reg.1.server.1.port` and `reg.1.server.2.port` values in this example are set to null to force SRV lookups.

**Example: Static DNS Cache with NAPTR and SRV Records**

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

When the static DNS cache is not used, the `site.cfg` configuration looks as follows:

```plaintext
Network

| reg | 1002
|-----|-----
| reg.1.address | sipserver.example.com
| reg.1.server.1.address | 172.23.0.140
| reg.1.server.1.port | 5075
| reg.1.server.1.transport | UDPOnly
| reg.1.server.2.address | 172.23.0.150
| reg.1.server.2.port | 5075
| reg.1.server.2.transport | UDPOnly
```

When the static DNS cache is used, the `site.cfg` configuration looks as follows:
Note: The `reg.1.server.1.port`, `reg.1.server.2.port`, `reg.1.server.1.transport`, and `reg.1.server.2.transport` values in this example are set to null to force NAPTR lookups.

**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 [RFC3263](https://tools.ietf.org/html/rfc3263).

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 does not 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.

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.

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.
VoIP Server Parameters
The list below describes VoIP server configuration parameters.

voIpProt.server.dhcp.available
0 (default) - Do not check with the DHCP server for the SIP server IP address.
1 - Check with the server for the IP address.
Change causes system to restart or reboot.

voIpProt.server.dhcp.option
The option to request from the DHCP server if voIpProt.server.dhcp.available = 1.
128 (default) to 254
If reg.x.server.y.address is non-Null, it takes precedence even if the DHCP server is available.
Change causes system to restart or reboot.

voIpProt.server.dhcp.type
Type to request from the DHCP server if voIpProt.server.dhcp.available is set to 1.
0 (default) - Request IP address
1 - Request string
Change causes system to restart or reboot.

voIpProt.OBP.dhcpv4.type
Define the type of Outbound Proxy address.
0 (default) - IP address
1 - String
Change causes system to restart or reboot.

voIpProt.OBP.dhcpv4.option
The phone requests for DHCP option 120 and applies the outbound proxy obtained in DHCP to
120 (default)
Change causes system to restart or reboot.

voIpProt.OBP.dhcpv6.option
Define the type of Outbound Proxy address from DHCPv6.
21 (default) - list of domain name
22 - list of IP address
Change causes system to restart or reboot.

Phone Operation for Registration

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

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 is established only with Server 1.

Upon the registration timer expiry of each server registration, the phone attempts to re-register. If this is unsuccessful, normal SIP re-registration 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.

Note: If `reg.x.server.y.register` is set to 0, the phone does not register to that server. However, the INVITE fails over to that server if all higher priority servers are down.

Recommended Practices for Fallback Deployments

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

- Deploy an on-site DNS server to avoid long call initiation delays that can result if the DNS server records expire.
- Do not use OutBoundProxy configurations on the phone if the OutBoundProxy could be unreachable when the fallback occurs.
- Avoid using too many servers as part of the redundancy configuration as each registration generates more traffic.
- Educate users as to the features that are not available when in fallback operating mode.

Note: The concurrent/registration failover/fallback feature is not compatible with Microsoft environments.

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service if, for example, the call server is taken offline for maintenance, the server fails, or the connection between the phone and the server fails.

Poly phones support failover and fallback server redundancy types. 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 that the default value of the new parameters `reg.x.server.y.failOver.concurrentRegistration` and `volpProt.server.y.failOver.concurrentRegistration=0` effective UC Software 5.5.2 for Poly Trio systems change default behavior in previous releases. Prior to UC Software 5.5.2, the server you
specify in \( y \) concurrently registers with other configured servers. As of UC Software 5.5.2, server \( y \) is added to the set of redundant failover servers. If you want to register the server concurrently with other servers set \( \text{reg.x.server.y.failOver.concurrentRegistration}=1 \) or \( \text{voIpProt.server.y.failOver.concurrentRegistration}=1 \).

**Note:** The concurrent failover/fallback feature is not 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.

**Server Redundancy Parameters**

Use the parameters in the following list to set up server redundancy for your environment.

**\( \text{reg.x.auth.optimizedInFailover} \)**

Set the destination for the first new SIP request when failover occurs.

- 0 (default) - The SIP request is sent to the server with the highest priority in the server list.
- 1 - The SIP request is sent to the server that sent the proxy authentication request.

**\( \text{reg.x.outboundProxy.failOver.failBack.mode} \)**

The mode for failover failback (overrides \( \text{reg.x.server.y.failOver.failBack.mode} \)).

- duration (default) - The phone tries the primary server again after the time specified by \( \text{reg.x.outboundProxy.failOver.failBack.timeout} \) 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.

**\( \text{reg.x.outboundProxy.failOver.failBack.timeout} \)**

- 3600 (default) - The time to wait (in seconds) before failback occurs (overrides \( \text{reg.x.server.y.failOver.failBack.timeout} \)).
- 0, 60 to 65535 - The phone does not fail back until a failover event occurs with the current server.

**\( \text{reg.x.outboundProxy.failOver.failRegistrationOn} \)**

- 1 (default) - The global and per-line reRegisterOn parameter is enabled and the phone silently invalidates an existing registration.
- 0 - The global and per-line reRegisterOn parameter is enabled and existing registrations remain active.

**\( \text{reg.x.outboundProxy.failOver.onlySignalWithRegistered} \)**
1 (default) - The global and 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.

0 - The global and per-line reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed.

**reg.x.outboundProxy.failOver.reRegisterOn**

This parameter overrides reg.x.server.y.failOver.reRegisterOn.

- 0 (default) - The phone won't attempt to register with the secondary server.
- 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server.

**reg.x.outboundProxy.port**

The port of the SIP server to which the phone sends all requests.

- 0 - (default)
- 1 to 65535

**reg.x.outboundProxy.transport**

The transport method the phone uses to communicate with the SIP server.

- DNSnaptr (default)
- DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly

**reg.x.server.y.failOver.concurrentRegistration**

- 0 (default) - If 0 and failOver.reRegisterOn is set to 1, add this server to the set of redundant failover servers.
- 1 - This server registers concurrently with other servers for this registration.

Note that the default value of the new parameter

reg.x.server.y.failOver.concurrentRegistration=0 effective UC Software 5.5.2

for Poly Trio systems changes default behavior in previous releases. Prior to UC Software 5.5.2, the server you specify in y concurrently registers with other configured servers. As of UC Software 5.5.2, server y is added to the set of redundant failover servers. If you want to register the server concurrently with other servers set

reg.x.server.y.failOver.concurrentRegistration=1.

**voIpProt.server.y.failOver.concurrentRegistration**

- 0 (default) - If 0 and failOver.reRegisterOn is set to 1, add this server to the set of redundant failover servers.
- 1 - This server registers concurrently with other servers.

The default value of the new parameter

voIpProt.server.y.failOver.concurrentRegistration=0 effective UC Software
5.5.2 for Poly Trio systems changes default behavior in previous releases. Prior to UC Software 5.5.2, the server you specify in y concurrently registers with other configured servers. As of UC Software 5.5.2, server y is added to the set of redundant failover servers. If you want to register the server concurrently with other servers set `voIpProt.server.y.failOver.concurrentRegistration=1`.

**voIpProt.server.x.failOver.failBack.mode**

Specify the failover failback mode.

- **duration** (default) - The phone tries the primary server again after the time specified by `voIpProt.server.x.failOver.failBack.timeout`
- **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 configured for the server that the phone is registered to.
- **registration** - The phone tries the primary server again when the registration renewal signaling begins.

**voIpProt.server.x.failOver.failBack.timeout**

If `voIpProt.server.x.failOver.failBack.mode` is set to duration, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests. Values between 1 and 59 result in a timeout of 60. 0 means do not fail-back until a fail-over event occurs with the current server.

- 3600 (default)
- 0, 60 to 65535

**voIpProt.server.x.failOver.failRegistrationOn**

- 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.onlySignalWithRegistered**

- 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.reRegisterOn

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.

Network Address Translation (NAT)

Network Address Translation (NAT) enables a local area network (LAN) to use one set of IP addresses for internal traffic and another set for external traffic.

The phone's signaling and RTP traffic use symmetric ports. Note that the source port in transmitted packets is the same as the associated listening port used to receive packets.

Network Address Translation Parameters

You can configure the external IP addresses and ports used by the NAT on the phone's behalf on a per-phone basis.

Use the parameters in the following list to configure NAT.

nat.ip

Specifies the IP address to advertise within SIP signaling. This should match the external IP address used by the NAT device.

Null (default)
IP address

Change causes system to restart or reboot.

nat.keepalive.interval

The keep-alive interval in seconds. Sets the interval at which phones sends a keep-alive packet to the gateway/NAT device to keep the communication port open so that NAT can continue to function. If Null or 0, the phone does not send out keep-alive messages.

0 (default)
0 - 3600

nat.mediaPortStart

The initially allocated RTP port. Overrides the value set for tcpIpApp.port.rtp.mediaPortRangeStart parameter.

0 (default)
0 - 65440

Change causes system to restart or reboot.
nat.signalPort
The port used for SIP signaling. Overrides the voIpProt.local.port parameter.
0 (default)
1024 - 65535

Real-Time Transport Protocol (RTP) Ports
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 the source port is not set to the negotiated remote sink port, arriving packets are rejected.
• 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 is sent to and arrives on that specified port. Incoming packets are sorted by the source IP address and port, which allows multiple RTP streams to be multiplexed.
• Specify the phone's RTP port range.
  Since the phone supports conferencing and multiple RTP streams, the phone can use several ports concurrently. Consistent with RFC 1889, 3550, and 3551, the next-highest odd-numbered port is used to send and receive RTP.

RTP Ports Parameters
Use the parameters in the following list to configure RTP packets and ports.

tcpIpApp.port.rtp.feccPortRange.enable
0 (default) – Use the Open SIP far-end camera control media port range.
1 - Use the far-end camera control port range configuration for Open SIP-registered lines.

tcpIpApp.port.rtp.feccPortRangeEnd
Specify the far-end camera control port range end port for Open SIP registrations.
2419 (default)
1024 - 65486

tcpIpApp.port.rtp.feccPortRangeStart
Specify the far-end camera control port range start port for Open SIP registrations.
2372 (default)
1024 – 65486
**tcpIpApp.port.rtp.filterByIp1**

IP addresses can be negotiated through the SDP or H.323 protocols.
1 (Default) - Phone rejects RTP packets that arrive from non-negotiated IP addresses.
Change causes system to restart or reboot.

**tcpIpApp.port.rtp.filterByPort1**

Ports can be negotiated through the SDP protocol.
0 (Default)
1 - Phone rejects RTP packets arriving from (sent from) a non-negotiated port.
Change causes system to restart or reboot.

**tcpIpApp.port.rtp.forceSend1**

Send all RTP packets to, and expect all RTP packets to arrive on, this port. Range is 0 to 65535.
0 (Default) - RTP traffic is not forced to one port.
Both tcpIpApp.port.rtp.filterByIp and tcpIpApp.port.rtp.filterByPort must be set to 1.
Change causes system to restart or reboot.

**tcpIpApp.port.rtp.mediaPortRangeEnd**

Determines the maximum supported end range of audio ports. Range is 1024 to 65485.
2269 (Default)
Change causes system to restart or reboot.

**tcpIpApp.port.rtp.mediaPortRangeStart1**

Set the starting port for RTP port range packets. Use an even integer ranging from 1024 to 65440.
2222 (Default)
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.
Change causes system to restart or reboot.

**tcpIpApp.port.rtp.videoPortRange.enable**

Specifies the range of video ports.
0 - Video ports are chosen within the range specified by tcpIpApp.port.rtp.mediaPortRangeStart and tcpIpApp.port.rtp.mediaPortRangeEnd.
1 - Video ports are chosen from the range specified by tcpIpApp.port.rtp.videoPortRangeStart and tcpIpApp.port.rtp.videoPortRangeEnd.

Skype = 1 (Default)
Generic = 0 (Default)

tcpIpApp.port.rtp.videoPortRangeEnd
Determines the maximum supported end range of video ports. Range is 1024 to 65535.
2319 (Default)
Change causes system to restart or reboot.

tcpIpApp.port.rtp.videoPortRangeStart
Determines the start range for video ports. Range is 1024 to 65486.
2272 (Default)
Used only if value of tcpIpApp.port.rtp.videoPortRange.enable is 1.
Change causes system to restart or reboot.

Wireless Network Connectivity (Wi-Fi)
Poly Trio systems support several wireless modes, security options, radio controls, and Quality of Service monitoring.

To ensure the best performance in your location, set a proper country code with the parameter device.wifi.country before enabling Wi-Fi.

You can configure Wi-Fi options to display in the phone’s basic settings menu to allow users to manually add a Wi-Fi network. You can also configure the phone to display the Wi-Fi icon on the phone’s status bar and home screen.

Enabling Wi-Fi automatically disables the Ethernet port. You cannot use Wi-Fi and Ethernet simultaneously to connect phones to your network. When you connect the system to your network over Wi-Fi, only audio-only calls are available. The phones do not support Wi-Fi captive portals or Wireless Display (WiDi).

Note: When you provision via 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.

The following wireless modes are supported:
• 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
Wi-Fi Parameters

Poly Trio 8300 and Poly Trio 8800 solutions are shipped with a security-restrictive worldwide safe Wi-Fi country code setting.

Use the following parameters to configure wireless network settings for your organization, which is dependent on the security mode for your organization and whether or not you enable DHCP. The Poly Trio solution supports the following Wi-Fi security modes:

- WEP
- WPA PSK
- WPA2 PSK
- WPA2 Enterprise

**Note:** The Poly Trio 8500 solution does not support Wi-Fi connectivity.

**device.wifi.country**

Enter the two-letter code for the country where you are operating the Poly Trio system with Wi-Fi enabled.

NULL (default)

Two-letter country code

**device.wifi.dhcpBootServer**

0 (default)

1

2

V4

V6

Static

**device.wifi.dhcpEnabled**

Enable or disable DHCP for Wi-Fi.

0 (default)

1

**device.wifi.enabled**

Enable or disable Wi-Fi.
device.wifi.ipAddress

Enter the IP address of the wireless device if you are not using DHCP.
0.0.0.0 (default)
String

device.wifi.ipGateway

Enter the IP gateway address for the wireless interface if not using DHCP.
0.0.0.0 (default)
String

device.wifi.psk.key

Enter the hexadecimal key or ASCII passphrase.
0xFF (default)
String

device.wifi.radio.enable2ghz

device.wifi.radio.enable5ghz

device.wifi.securityMode

Specify the wireless security mode.
NULL (default)
None
WEP
WPA-PSK
WPA2-PSK
WPA2-Enterprise

device.wifi.ssid

Set the Service Set Identifier (SSID) of the wireless network.
SSID1 (default)
SSID
device.wifi.subnetMask
Set the network mask address of the wireless device if not using DHCP.
255.0.0.0 (default)
String

device.wifi.wep.key
Set the length of the hexadecimal WEP key.
0 = 40-bits (default)
1 = 104-bits

device.wifi.wpa2Ent.method
Set the Extensible Authentication Protocol (EAP) to use for 802.1X authentication.
NULL (default)
EAP-PEAPv0/MSCHAPv2
EAP-FAST
EAP-TLS
EAP-PEAPv0-GTC
EAP-TTLS-MSCHAPv2
EAP-TTLS-GTC
EAP-PEAPv0-NONE
EAP-TTLS-NONE
EAP-PWD

device.wifi.wpa2Ent.password
The WPA2-Enterprise password.

device.wifi.wpa2Ent.user
The WPA2-Enterprise user name.

Enable Wi-Fi
You can wirelessly connect phones to your network using Wi-Fi, which is disabled by default.
When you enable Wi-Fi, the system reboots.

Procedure
1. Go to Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu, and turn Wi-Fi to On.
The phone restarts.
2. When the phone completes restart, go to Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu to view available networks.
3. Select a network you want to connect to and press Connect.

Configure Wireless Network Settings

Polycom UC Software supports wireless network connectivity.

You can manually configure the phone to connect to a wireless network by selecting an enterprise-based network and EAP method for better security.

Procedure

1. Go to Settings > Advanced > Administrator Settings > Network Configuration > Network Interfaces > Wi-Fi Menu.
2. Turn Wi-Fi to On.
3. The phone restarts.
4. When the phone completes restart, go to Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu to view available networks.
5. Select a network you want to connect to and press Connect.
6. Select the SSID name of the wireless network.
7. Select the security type of the wireless network. If you have an enterprise-based network, enter the User ID and Password and select one of the following EAP-Method types for authentication:
   - EAP-TLS
   - EAP-PEAP-MSCHAPv2
   - EAP-PEAP-GTC
   - EAP-TTLS-MSCHAPv2
   - EAP-TTLS-GTC
   - EAP-MD5
   - EAP-FAST
8. Save the settings to apply your changes.

Wi-Fi Settings in Basic Menu Parameter

Use the parameter below to allow access to Wi-Fi settings in the Basic menu on Poly Trio 8300 and Poly Trio 8800 systems.

**feature.basicWifiMenu.enabled**

Enable to allow access to Wi-fi Menu in Basic settings.

0 (default) - Disabled
1 - Enabled
Bluetooth and NFC-Assisted Bluetooth for Poly Trio Systems

Poly Trio systems support Bluetooth connection and pairing with a compatible Bluetooth device such as a mobile phone, tablet, laptop, or headset. The Poly Trio 8800 system supports near-field communication (NFC).

When you enable Bluetooth, users can connect a Bluetooth-capable device, such as a mobile phone, tablet, or laptop to the Poly Trio system. You can make calls from the connected device and play audio from calls, video, or music from the Poly Trio system speaker. Note you can connect one device at a time to the Poly Trio system via Bluetooth. You cannot connect via Bluetooth during an active call. The Poly Trio 8800 conference phone can remember up to 10 previously paired devices.

When NFC is enabled on the Poly Trio 8800 system and you connect a personal device to the Poly Trio 8800, the NFC logo displays on the device screen. When your device is connected over Bluetooth during an audio or a video call, you can use the Poly Trio system microphones for audio instead of the microphone(s) of your connected device.

Note that using a Bluetooth headset can affect voice quality on the phone due to inherent limitations with Bluetooth technology. You may not experience the highest voice quality when using a Bluetooth headset while the 2.4 GHz band is enabled or while you are in an environment with many other Bluetooth devices.

**Note:** The Poly Trio system does not automatically reconnect to paired devices after the device Bluetooth connection is disconnected or after a reboot of the Poly Trio system. If the paired Bluetooth device is disconnected or the Poly Trio system reboots, you must manually reconnect and pair the device to the Trio system.

Bluetooth and NFC-Assisted Bluetooth Parameters

Use the following parameters to configure Bluetooth on Poly Trio systems and NFC on the Poly Trio 8800 system.

**bluetooth.beacon.ipAddress.enabled**

Set to send the IP address of the system over Bluetooth.

1 (default) - Enables sending the system IP address over Bluetooth. Turns Bluetooth radio on when `feature.bluetooth.enabled = 1`.

0 - Disables sending the system IP address over Bluetooth

**Note:** Enable the parameter `feature.bluetooth.enabled` to use this feature.

**bluetooth.device.discoverable**

1 (default) - This device is discoverable for Bluetooth pairing.

0 - This device is not discoverable for Bluetooth pairing.

**bluetooth.device.name**
Enter the name of the device that broadcasts over Bluetooth to other devices.

`bluetooth.discoverableTimeout`
- 0 (default) - Other devices can always discover this device over Bluetooth.
- 0 - 3600 seconds
  - Set the time in seconds after which other devices can discover this device over Bluetooth.

`bluetooth.pairedDeviceMemorySize`
- 10 (default)
- 0 - 10

`bluetooth.radioOn`
- 0 - The Bluetooth radio (transmitter/receiver) is off.
- 1 (default) - The Bluetooth radio is on. The Bluetooth radio must be turned on before other devices can connect to this device over Bluetooth.

`feature.bluetooth.enabled`
- For high security environments.
- 1 (default) - Bluetooth connection is enabled and the Bluetooth menu displays.
- 0 - Bluetooth connection is disabled and the Bluetooth icon does not display.

`feature.nfc.enabled`
- 0 - The NFC pairing feature for the Poly Trio 8800 system is disabled.
- 1 - The NFC pairing is enabled and users can pair NFC-capable devices to the Poly Trio 8800 solution.
Third-Party Servers

Topics:

• BroadSoft BroadWorks Server
• Microsoft Exchange Integration

This section provides information on configuring phones and features with third-party servers.

BroadSoft BroadWorks Server

This section shows you how to configure Poly devices with BroadSoft Server options.

Note that you cannot register lines with the BroadWorks R18 server and the R20 and later server on the same phone. All lines on the phone must be registered to the same BroadWorks server.

Some BroadSoft features require you to authenticate the phone with the BroadWorks XSP service interface as described in the section Authentication with BroadWorks Xtended Service Platform (XSP) Service Interface.

Authentication with BroadWorks Xtended Service Platform (XSP) Service Interface

You can configure Poly 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

To use these features on Polycom devices with a BroadWorks server, you must authenticate the phone with the BroadSoft XSP service interface.

Authentication for BroadWorks XSP Parameters

The authentication method you use depends on which version of BroadWorks you are running.

If your server is running BroadWorks R19 or earlier, enable the following parameters to authenticate on the BroadWorks server using separate XSP credentials:

• dir.broadsoft.xsp.address
• reg.x.broadsoft.userId
• reg.x.broadsoft.xsp.password
• reg.x.broadsoft.useXspCredentials

If your server is running BroadWorks R19 Service Pack 1 or later, enable the following parameters to authenticate on the BroadWorks server using the same SIP credentials you used to register the phone lines:
• dir.broadsoft.xsp.address
• reg.x.auth.userId
• reg.x.auth.password
• reg.x.broadsoft.userId

See the following list for additional details on these parameters.

**reg.x.broadsoft.xsp.password**

Enter the password associated with the BroadSoft user account for the line. Required only when reg.x.broadsoft.useXspCredentials=1.

Null (default)

string

**reg.x.broadsoft.userId**

Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface.

Null (default)

string

**reg.x.broadsoft.useXspCredentials**

If this parameter is disabled, the phones use standard SIP credentials to authenticate.

1 (default) - Use this value, if phone lines are registered with a server running BroadWorks R19 or earlier.

0 - Set to 0, if phone lines are registered with a server running BroadWorks R19 SP1 or later.

**reg.x.auth.userId**

User ID to be used for authentication challenges for this registration.

Null (default)

string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication sub-menu on the Settings menu of the phone.

**reg.x.auth.password**

The password to be used for authentication challenges for this registration.

Null (default)

string - It overrides the password entered into the Authentication sub-menu on the Settings menu of the phone.

---

**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—to provide 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.

These features require support from the BroadSoft BroadWorks R18 SP1 platform with patches and BroadSoft BroadCloud services. For details on how to set up and use these features, see the latest Polycom VVX Business Media Phones - User Guide at [Latest Polycom UC Software Release](#).

Polycom’s BroadSoft UC-One application enables you to:

• Access the BroadSoft Directory
• Search for contacts in BroadSoft Directory
• View BroadSoft UC-One contacts and groups
• View the presence status of BroadSoft UC-One contacts
• View and filter BroadSoft UC-One contacts
• Activate and control BroadSoft UC-One personal call control features.

### BroadSoft UC-One Configuration Parameters

The following list includes all parameters available to configure features in the BroadSoft UC-One application.

#### feature.qml.enabled

0 (default) - Disable the QML viewer on the phone. Note that the UC-One directory user interface uses QML as the user interface framework and the viewer is used to load the QML applications.

1 - Enable the QML viewer on phone.

Change causes system to restart or reboot.

#### feature.broadsoftdir.enabled

0 (default) - Disable simple search for Enterprise Directories.

1 - Enable simple search for Enterprise Directories.

Change causes system to restart or reboot.

#### feature.broadsoftUcOne.enabled

0 (default) - Disables the BroadSoft UC-One feature.

1 - Enables the BroadSoft UC-One feature.

Change causes system to restart or reboot.

#### feature.presence.enabled
0 (default) - Disable the presence feature – including buddy managements and user status.
1 - Enable the presence feature with the buddy and status options.

**homeScreen.UCOne.enable**
1 (default) - Enable the UC-One Settings icon to display on the phone Home screen.
0 - Disable the UC-One Settings icon to display on the phone Home screen.

**dir.broadsoft.xsp.address**
Set the IP address or hostname of the BroadSoft directory XSP home address.
Null (default)
IP address
Hostname
FQDN

**dir.broadsoft.xsp.username**
To set the BroadSoft Directory XSP home address.

**dir.broadsoft.xsp.password**
Set the password used to authenticate to the BroadSoft Directory XSP server.
Null (default)
UTF-8 encoding string

**xmpp.1.auth.password**
Specify the password used for XMPP registration.
Null (Default)
UTF-8 encoded string

**xmpp.1.dialMethod**
For SIP dialing, the destination XMPP URI is converted to a SIP URI, and the first available SIP line is used to place the call.
SIP (default)
String min 0, max 256

**xmpp.1.jid**
Enter the Jabber identity used to register with the presence server, for example:
presence.test2@polycom-alpha.eu.bc.im.
Null (default)
String min 0, max 256

**xmpp.1.roster.invite.accept**
Choose how phone users receive the BroadSoft XMPP invitation to be added to a buddy list.
- prompt (default) - phone displays a list of users who have requested to add you as a buddy and you can accept or reject the invitation.
- Automatic

**xmpp.1.server**
Sets the BroadSoft XMPP presence server to an IP address, host name, or FQDN, for example: `polycom-alpha.eu.bc.im`.
- Null (default)
- dotted-decimal IP address, host name, or FQDN.

**xmpp.1.verifyCert**
Enable or disable verification of the TLS certificate provided by the BroadSoft XMPP presence server.
- 1 (default) - Enabled
- 0 - Disabled

**Configuring BroadSoft UC-One**
You can configure the UC-One Call Settings menu and feature options on the phone, in the Web Configuration Utility, and using configuration parameters.

**Configure BroadSoft UC-One on the Phone**
You can enable the BroadSoft UC-One feature directly from the phone.

**Procedure**
1. Navigate to **Settings > UC-One**.
2. Under General, click **Enable for BroadSoft UC-One**.
   This enables the UC-One Call Settings menu to display on the phone.

**Configure BroadSoft UC-One in the Web Configuration Utility**
You can enable the BroadSoft UC-One feature and feature options in the Web Configuration Utility.

**Procedure**
1. In the Web Configuration Utility, navigate to **Settings > UC-One**.
2. Under **Call Settings Features**, enable each feature menu you want available on the phone.
BroadSoft UC-One Directory Parameters

Use the parameters in the following list to configure the Polycom BroadSoft UC-One directory.

**dir.broadsoft.regMap**

Specify the registration line credentials you want to use for BroadSoft R20 Server or later to retrieve directory information from the BroadSoft UC-One directory when dir.broadsoft.useXspCredentials =0.

1 (default)
0 - Const_NumLineReg

**dir.broadsoft.useXspCredentials**

Specify which method of credentials the phone uses to sign in with the BroadSoft server.

1 (default) – Uses BroadSoft XSP credentials.
0 – Uses SIP credentials from dir.broadsoft.regMap.

Anonymous Call Rejection

Anonymous Call Rejection enables users to automatically reject incoming calls from anonymous parties who have restricted their caller identification.

After you enable the feature for users, users can turn call rejection on or off from the phone. When a user turns Anonymous Call Rejection on, the phone gives no indication that an anonymous call was received.

You can configure this option in the Web Configuration Utility.

**Configure Anonymous Call Rejection using the Web Configuration Utility**

You can configure Anonymous Call Rejection in the Web Configuration Utility.

**Procedure**

1. Navigate to Settings > UC-One.
2. Under the Call Setting Features, click Enable for Anonymous Call Rejection.

**Anonymous Call Rejection Parameters**

Use the parameters below to configure Anonymous Call Rejection Parameters.

Use the parameters in the following list to enable this feature.

**feature.broadsoft.xsi.AnonymousCallReject.enabled**

0 (default) - Does not display the Anonymous Call Rejection menu to users.
1 - Displays the Anonymous Call Rejection menu and the user can turn the feature on or off from the phone.

**feature.broadsoftUcOne.enabled**
0 (default) - Disables the BroadSoft UC-One feature.
1 - Enables the BroadSoft UC-One feature.
Change causes system to restart or reboot.

reg.x.broadsoft.userId
Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface.
Null (default)
string

Simultaneous Ring Personal
The Simultaneous Ring feature enables users to add phone numbers to a list of contacts whose phones ring simultaneously when the user receives an incoming call.
When you enable the display of the Simultaneous Ring menu option on the phone, users can turn the feature on or off from the phone and define which numbers should be included in the Simultaneous Ring group.

Simultaneous Ring Parameters
Use the parameters below to configure Simultaneous Ring.
Use the parameters in the following list to enable this feature.

feature.broadsoft.xsi.SimultaneousRing.enabled
0 (default) - Disables and does not display the Simultaneous Ring Personal feature menu on the phone.
1 - Enables the Simultaneous Ring Personal feature menu on the phone.

feature.broadsoftUcOne.enabled
Enable or disable all BroadSoft UC-One features.
0 - Disabled
1 - Enabled

Line ID Blocking
You can enable or disable the display of the Line ID Blocking menu option on the phone.
When you enable the menu for users, users can choose to hide their phone number before making a call.

Line ID Blocking Parameters
Use the parameters below to configure Line ID Blocking.
Use the parameters in the following list to enable this feature.

feature.broadsoft.xsi.LineIdblock.enabled
0 (default) - Disables and does not display the Line ID Blocking feature menu on the phone.
1 - Enables the Line ID Blocking feature menu on the phone.

**feature.broadsoftUcOne.enabled**
0 (default) - Disables the BroadSoft UC-One feature.
1 - Enables the BroadSoft UC-One feature.
Change causes system to restart or reboot.

**BroadWorks Anywhere**
BroadWorks Anywhere enables users to use one phone number to receive calls to and dial out from their desk phone, mobile phone, or home office phone.

When you enable this feature, users can move calls between phones and perform phone functions from any phone. When enabled, the BroadWorks Anywhere settings menu displays on the phone and users can turn the feature on or off and add BroadWorks Anywhere locations on the phone.

**BroadWorks Anywhere Parameters**
You can configure BroadWorks Anywhere using configuration files or the Web Configuration Utility. Use the parameters in the following list to enable this feature.

**feature.broadsoft.xsi.BroadWorksAnywhere.enabled**
0 (default) - Disables and does not display the BroadWorks Anywhere feature menu on the phone.
1 - Enables the BroadWorks Anywhere feature menu on the phone.

**feature.broadsoftUcOne.enabled**
0 (default) - Disables the BroadSoft UC-One feature.
1 - Enables the BroadSoft UC-One feature.
Change causes system to restart or reboot.

**Remote Office**
Remote Office enables 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, this feature enables users to answer incoming calls to the office phone on the phone, and any calls placed from that phone show the office phone number.

**Remote Office Parameters**
Use the parameters in the following list to enable this feature.

**feature.broadsoft.xsi.RemoteOffice.enabled**
0 (default) - Disables the Remote Office feature menu on the phone.
1 - Enables and displays the Remote Office feature menu on the phone.

`reg.x.broadsoft.userId`

Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface.
Null (default)
string

`feature.broadsoftUcOne.enabled`

0 (default) - Disables the BroadSoft UC-One feature.
1 - Enables the BroadSoft UC-One feature.
Change causes system to restart or reboot.

`dir.broadsoft.xsp.password`

Set the password used to authenticate to the BroadSoft Directory XSP server.
Null (default)
UTF-8 encoding string

**BroadSoft UC-One Credentials**

Enabling this feature allows users to enter their BroadWorks UC-One credentials on the phone instead of in the configuration files.

The parameters `reg.x.broadsoft.useXspCredentials` , and `feature.broadsoftUcOne.enabled` must be enabled to display the UC-One Credentials menu option on the phone.

**BroadSoft UC-One Credential Parameters**

Use the parameters in the following list to enable this feature.

`dir.broadsoft.xsp.address`

Set the IP address or hostname of the BroadSoft directory XSP home address.
Null (default)
IP address
Hostname
FQDN

`reg.x.broadsoft.userID`

Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface.
Null (default)
string

**feature.broadsoftUcOne.enabled**

0 (default) - Disables the BroadSoft UC-One feature.
1 - Enables the BroadSoft UC-One feature.
Change causes system to restart or reboot.

**dir.broadsoft.xsp.username**

To set the BroadSoft Directory XSP home address.

**dir.broadsoft.xsp.password**

Set the password used to authenticate to the BroadSoft Directory XSP server.
Null (default)
UTF-8 encoding string

**feature.broadsoftdir.enabled**

0 (default) - Disable simple search for Enterprise Directories.
1 - Enable simple search for Enterprise Directories.
Change causes system to restart or reboot.

**BroadSoft Server-Based Call Forwarding**

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, other registrations are not affected.

The following conditions apply for server-based call forwarding:

- If server-based call forwarding is enabled, but inactive, when a user presses the **Forward** soft key, the moving arrow icon does not display on the phone and incoming calls are not forwarded.

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 allows the receiving phone to indicate who the call was from, and the phone number it was forwarded from.

**Microsoft Exchange Integration**

If you have a Skype for Business, Office 365, Lync Server 2010 or 2013 deployment, you can integrate with Microsoft Exchange Server.

You can set up visual voicemail, call log synchronization, Outlook contact search, and Skype for Business Address Book Service (ABS) adaptive search. Each of these features is enabled by default on Poly phones registered with Skype for Business.

After the phone is connected with the Exchange Server, you can:
• Verify the status of Exchange Server services on each phone.
• View the status of each service in the Web Configuration Utility.

**Integrating with Microsoft Exchange**

You can integrate with Microsoft Exchange using one of the following methods:

• Exchange Server auto-discover
• Provision the phone with the Microsoft Exchange address
• Web Configuration Utility

**Note:** If you enter sign-in credentials to the configuration file, phone users must enter credentials to the phone Sign In screen.

**Provision the Microsoft Exchange Calendar**

You can provision your phones with the Microsoft Exchange calendar.

**Procedure**

» Add the following parameters to one of your configuration files:
  
  • feature.exchangeCalendar.enabled=1
  • exchange.server.url=https://<example URL>

**Enable Microsoft Exchange Calendar Using the Web Configuration Utility**

You can use the Web Configuration Utility to manually enable your phones with the Microsoft Exchange calendar.

This is useful for troubleshooting if auto-discovery is not working or mis-configured. This method applies only to a single phone at a time.

**Procedure**

1. Enable access to the Web Configuration Utility if the phone is registered with Skype for Business.
   For instructions, see Accessing the Web Configuration Utility.
2. Log in to the Web Configuration Utility as Admin (default password 456).
4. In the Exchange Calendar field, select Enable.
5. Enter the exchange web services URL using a Microsoft Exchange Server URL, for example https://<mail.com>/ews/exchange.asmx.
   In this example, the URL part <mail.com> is specific to an organization.
6. At the bottom of the browser page, click Save.
7. When the confirmation dialog displays, click Yes.
   Your Exchange Calendar is successfully configured and the Calendar icon displays on your phone screen.
Calendar Meeting Details

You can use `exchange.meeting.show*` parameters to show or hide the following meeting details from the calendar display on the Poly Trio system screen and monitor(s) connected to the paired Poly Trio Visual+, Trio VisualPro, or RealPresence Group Series system:

- Subject.
- Location.
- Invitee(s).
- Agenda/Notes. When you hide Agenda/Notes, a message indicates the meeting is private.
- Meeting organizer. The organizer does not display for meetings displayed on the monitor.
- Show More Actions. If multiple numbers are available to dial into a meeting, More Actions displays in Meeting Details to allow users to choose the dial-in number.

Meeting Reminder Messages

Poly Trio systems display several meeting reminder messages.

A meeting reminder displays on the Poly Trio system screen at five minutes and one minute before the start of a meeting. The five-minute reminder disappears after 30 seconds if not dismissed. If the one-minute reminder has not been dismissed, the reminder message displays on the Poly Trio system Home Screen during the duration of the meeting. The one-minute reminder disappears when the meeting ends or when the next meeting reminder pops up, whichever comes first.

When multiple meetings are booked at the same time or overlap, a message displays available meetings. Users can tap the message to display the calendar day view and choose which meeting to join.

You can also show or hide all-day events, configure the maximum number of future meetings, or configure a user requirement to enter the Skype for Business conference ID when a meeting organizer marks a meeting as ‘Private’. When meeting organizers mark a meeting invitation as Private in Outlook, the Poly Trio system displays the meeting invite on the Poly Trio system calendar and TV screens with ‘Private Meeting’ in the subject line and a lock icon. The conference ID is included in the Outlook invitation.

Verify the Microsoft Exchange Integration

You can verify if all of the Exchange services are working.

Procedure

1. Go to Status > Diagnostics > Warnings on the phone.
2. View the status of each service in the Web Configuration Utility.

Poly Trio Solution with Skype for Business

You can deploy a Poly Trio system with Skype for Business Online, Skype for Business 2013, and Lync 2010 on-premises.

For a list of available features and instructions on deploying Poly Trio solution with Skype for Business and Lync Server, see the latest Poly Trio Solution in Microsoft Environments Administrator Guide on Poly Trio.

When you register a Poly Trio system with Skype for Business, a Calendar icon displays on the phone Home screen that enables users to access features. Users can view and join Outlook calendar events directly from the Poly Trio system. This displays the day and meeting view for scheduled events; the
month view is not currently available. Note you cannot schedule calendar events or view email from the phone.

When you pair a Poly Trio system registered with Skype for Business to a Poly Trio Visual+ system, the monitor’s Home screen automatically displays the Calendar and up to five meetings scheduled within the next 24-48 hours. You can configure whether or not users receive reminder notifications on the display monitor and whether or not an alert sound accompanies reminder notifications.

**Private Meetings in Microsoft Exchange**

When a Skype for Business meeting is set to Private, you can choose which meeting information to show or hide.

**Skype for Business Private Meeting Parameters**

Use the following parameters to configure Skype for Business private meetings.

**exchange.meeting.private.showAttendees**

0 (default) - Meetings marked as private in Outlook do not show the list of meeting attendees and invitees on the Poly Trio calendar.

1 - Meetings marked as private in Outlook show the list of meeting attendees and invitees on the Poly Trio calendar.

**exchange.meeting.private.showDescription**

0 (default) - Meetings marked as private in Outlook do not display a meeting description on the Poly Trio calendar.

1 - Meetings marked as private in Outlook display a meeting description on Poly Trio calendar.

**exchange.meeting.private.showLocation**

0 (default) - Meetings marked as private in Outlook do not display the meeting location on the Poly Trio calendar.

1 - Meetings marked as private in Outlook display the meeting location on the Poly Trio calendar.

**exchange.meeting.private.showSubject**

0 (default) - Meetings marked as private in Outlook do not display a subject line on Poly Trio calendar.

1 - Meetings marked as private in Outlook display a subject line on Poly Trio calendar.

**exchange.meeting.private.showMoreActions**

1 (default) - Meetings marked as private in Outlook display the More Actions button, when applicable.

0 - Meetings marked as private in Outlook do not display the More Actions button.
exchange.meeting.private.showOrganizer

1 (default) - Meetings marked as private in Outlook display the name of the meeting organizer on the Poly Trio calendar.
0 - Meetings marked as private in Outlook display the name of the meeting organizer on the Poly Trio calendar.

exchange.meeting.private.enabled

1 (default) - The Poly Trio considers the private meeting flag for meetings marked as private in Outlook.
0 - Treat meetings marked as private in Outlook the same as other meetings.

exchange.meeting.private.promptForPIN

0 (default) - Disable the Skype for Business Conference ID prompt that allows users to join meetings marked as private.
1 - Enable the Skype for Business Conference ID prompt that allows users to join meetings marked as private.

Configuring the Microsoft Exchange Server

You can configure the following settings to take advantage of Microsoft Exchange services on your phones.

Note: For help with Lync Server 2010, refer to Microsoft Configure Exchange Services for the Autodiscover Service.
For help with Lync Server 2013, refer to Microsoft Configuring Unified Messaging on Microsoft Exchange Server to work with Lync Server 2013.

Visual Voicemail

On the exchange server, enable unified messaging and enable messages to play on the phone for each user.

If you disable feature.exchangeVoiceMail.enabled, the Message Center and Skype for Business Voice mail menus display the message: Skype for Business Server only plays voicemail and you cannot download voicemails or play locally on the phone.

Synchronizing Call Logs

On the Exchange server, you can enable the option to save calls logs to each user’s conversation history in Outlook.

Address Book Service (ABS) Adaptive Search

You can enable the ABS service on the Exchange server.

There are three possible configurations.

• Outlook and ABS are both enabled by default. When both are enabled, the phone displays the Skype for Business Directory.
• If you disable Outlook and enable only ABS, the phone displays the Skype for Business Directory.
• If you enable Outlook and disable ABS, the Outlook Contact Search displays in Directories.

Poly Trio systems registered with Skype for Business server display a one-touch Join button that allows you to join a Skype for Business conference in a federated environment, even if you haven’t configured Transport Neutral Encapsulation Format (TNEF).

Microsoft Exchange Parameters
The following parameters configure Microsoft Exchange integration.

`exchange.meeting.alert.followOfficeHours`
1 (default) - Enable audible calendar alerts during business hours.
0 - Disable audible calendar alerts.

`exchange.meeting.alert.tonePattern`
positiveConfirm (default) - Set the tone pattern of the reminder alerts using any tone specified by se.pat.*.

`exchange.meeting.alert.toneVolume`
10 (default) - Set the volume level of reminder alert tones.
0 - 17

`exchange.meeting.allowScrollingToPast`
0 (default) - Do not allow scrolling up in the Day calendar view to see recently past meetings.
1 - Allow scrolling up in the Day calendar view to see recently past meetings.

`exchange.meeting.hideAllDayNotification`
0 (default) - All-day and multi-day meeting notifications display on the Calendar screen.

`exchange.meeting.parseOption`
Select a meeting invite field to fetch a VMR or meeting number from.
Location (default)
All
LocationAndSubject
Description

`exchange.meeting.parseWhen`
NonSkypeMeeting (default) - Disable number-searching on the Calendar for additional numbers to dial while in Skype Meetings.
Always - Enable number-searching on the Calendar for additional numbers to dial while in Skype Meetings.

**exchange.meeting.phonePattern**

NULL (default)

string

The pattern used to identify phone numbers in meeting descriptions, where "x" is a digit and "|" separates alternative patterns (for example, xxx-xxx-xxxx|604.xxx.xxxx).

**exchange.meeting.realConnectProcessing.outboundRegistration**

Choose a line number to use to make calls on Polycom RealConnect technology.

2 (default)

1 - 34

Change causes system to restart or reboot.

**exchange.meeting.realConnectProcessing.prefix.domain**

Define the One-Touch Dial meeting invite prefix domain. Example: "mypolycom.com"

**exchange.meeting.realConnectProcessing.prefix.value**

Define the One-Touch Dial meeting invite prefix value.

**exchange.meeting.realConnectProcessing.skype.enabled**

0 (default) – Disable the Skype for Business meeting on Polycom RealConnect technology.

1 - Enable the Skype for Business meeting on Polycom RealConnect technology.

Change causes system to restart or reboot.

**exchange.meeting.reminderEnabled**

1 (default) - Meeting reminders are enabled.

0 - Meeting reminders are disabled.

**exchange.meeting.reminderInterval**

300 seconds (default)

60 - 900 seconds

Set the interval at which phones display reminder messages.

**exchange.meeting.reminderSound.enabled**
1 (default) - The phone makes an alert sound when users receive reminder notifications of calendar events. Note that when enabled, alert sounds take effect only if `exchange.meeting.reminderEnabled` is also enabled.

0 - The phone does not make an alert sound when users receive reminder notifications of calendar events.

**exchange.meeting.reminderType**

Customize the calendar reminder and tone.

2 (default) - The reminder is always audible and visual.

1 - The first reminder is audible and visual reminders are silent.

0 - All reminders are silent.

**exchange.meeting.reminderWake.enabled**

1 (default) - The phone wakes from low power mode after receiving a calendar notification.

0 - The phone stays in low power mode after receiving a calendar notification.

**exchange.meeting.showAttendees**

1 (default) - Show the names of the meeting invitees.

0 - Hide the names of the meeting invitees.

**exchange.meeting.showDescription**

1 (default) - Show Agenda/Notes in Meeting Details that display after you tap a scheduled meeting on the Poly Trio system calendar.

0 - Hide the meeting Agenda/Notes.

**exchange.meeting.showLocation**

1 (default) - Show the meeting location.

0 - Hide the meeting location.

**exchange.meeting.showMoreActions**

1 (default) - Show More Actions in Meeting Details to allow users to choose a dial-in number.

0 - Hide More Actions in Meeting Details.

**exchange.meeting.showOnlyCurrentOrNext**

0 (default) - Disable the limitation to display only the current or next meeting on the Calendar.

1 - Display only the current or next meeting on the Calendar.

**exchange.meeting.showOrganizer**
1 (default) - Show the meeting organizer in the meeting invite.
0 - Hide the meeting organizer in the meeting invite.

**exchange.meeting.showSubject**

1 (default) - Show the meeting Subject.
0 - Hide the meeting Subject.

**exchange.meeting.showTomorrow**

1 (default) - Show meetings scheduled for tomorrow as well as for today.
0 - Show only meetings scheduled for today.

**exchange.menu.location**

Features (default) - Displays the Calendar in the global menu under Settings > Features.
Administrator - Displays the Calendar in the Admin menu at Settings > Advanced > Administration Settings.

**exchange.pollInterval**

The interval, in seconds, to poll the Exchange server for new meetings.
30000 (default)
4000 minimum
60000 maximum

**exchange.reconnectOnError**

1 (default) - The phone attempts to reconnect to the Exchange server after an error.
0 - The phone does not attempt to reconnect to the Exchange server after an error.

**exchange.server.url**

NULL (default)
string
The Microsoft Exchange server address.

**feature.EWSAutodiscover.enabled**

If you configure `exchange.server.url` and set this parameter to 1, preference is given to the value of `exchange.server.url`.

Lync Base Profile default is 1.
Generic Base Profile default is 0.
1 - Exchange autodiscovery is enabled and the phone automatically discovers the Exchange server using the email address or SIP URI information.
0 - Exchange autodiscovery is disabled on the phone and you must manually configure the Exchange server address.

**feature.exchangeCalendar.enabled**

Lync Base Profile default is 1.
Generic Base Profile default is 0.
0 - The calendaring feature is disabled.
1 - The calendaring feature is enabled.
You must enable this parameter if you also enable **feature.exchangeCallLog.enabled**. If you disable **feature.exchangeCalendar.enabled**, also disable **feature.exchangeCallLog.enabled** to ensure call log functionality.

**feature.exchangeContacts.enabled**

Lync Base Profile default is 1.
Generic Base Profile default is 0.
1 - The Exchange call log feature is enabled and users can retrieve the call log histories for missed, received, and outgoing calls.
0 - The Exchange call log feature is disabled and users cannot retrieve call logs histories.
You must also enable the parameter **feature.exchangeCallLog.enabled** to use the Exchange call log feature.

**feature.exchangeVoiceMail.enabled**

Lync Base Profile default is 1.
Generic Base Profile default is 0.
1 - The Exchange voicemail feature is enabled and users can retrieve voicemails stored on the Exchange server from the phone.
0 - The Exchange voicemail feature is disabled and users cannot retrieve voicemails from Exchange Server on the phone.
You must also enable **feature.exchangeCalendar.enabled** to use the Exchange contact feature.

**feature.exchangeVoiceMail.skipPin.enabled**

0 (default) - Enable PIN authentication for Exchange Voicemail. Users are required to enter their PIN before accessing Exchange Voicemail.
1 - Disable PIN authentication for Exchange Voicemail. Users are not required to enter their PIN before accessing Exchange Voicemail.
feature.lync.abs.enabled

Lync Base Profile default is 1.
Generic Base Profile default is 0.
1 - Enable comprehensive contact search in the Skype for Business address book service.
0 - Disable comprehensive contact search in the Skype for Business address book service.

feature.lync.abs.maxResult

Define the maximum number of contacts to display in a Skype for Business address book service contact search.

12 (default)
5 - 50

feature.wad.enabled

Do not disable this parameter if you are using Skype Online or Web Sign-In.
1 (default) – The phone attempts to use Web auto-discovery and if no FQDN is available, falls back to DNS.
0 - The phone uses DNS to locate the server FQDN and does not use Web auto-discovery. does not recommend disabling this parameter when using Skype for Business Online and Web Sign In.

feature.contacts.readonly

0 (default) - Skype for Business Contacts are editable.
1 - Skype for Business are read-only.

up.oneTouchVoiceMail

Lync Base Profile default is 1.
Generic Base Profile default is 0.
0 - The phone displays a summary page with message counts. The user must press the Connect soft key to dial the voicemail server.
1 - The phone dials voicemail services directly (if available on the call server) without displaying the voicemail summary.

Join a Meeting with a SIP URI

When you set up a meeting in the Calendar, the Poly Trio system displays a meeting reminder pop up.

If a dial-in number is available for the meeting, the reminder pop-up presents a Join button that joins you to the meeting. If a meeting lists multiple dial-in numbers or URIs for the meeting, by default the Join button automatically dials the first number.

- SIP URI
- Tel URI
• PSTN number
• IP dial

**Join a Meeting with SIP URI Parameters**

The following table lists the parameters that configure dial-in information.

**exchange.meeting.join.promptWithList**

Specifies the behavior of the Join button on meeting reminder pop-ups.

- 0 (default) - Tapping Join on a meeting reminder should show a list of numbers to dial rather than immediately dialing the first one.
- 1 - A meeting reminder does not show a list of numbers to dial.

**exchange.meeting.parseWhen**

Specifies when to scan the meeting’s subject, location, and description fields for dialable numbers.

- NonSkypeMeeting (default)
- Always
- Never

**exchange.meeting.parseOption**

Specifies where to search for a dialable number.

- All (default)

**exchange.meeting.parseEmailsAsSipUris**

List instances of text like user@domain or user@ipaddress in the meeting description or subject under the More Actions pane as dialable SIP URIs.

- 0 (default) - it does not list the text as a dialable SIP URI
- 1 - it treats user@domain

**exchange.meeting.parseAllowedSipUriDomains**

List of comma-separated domains that will be permitted to be interpreted as SIP URIs

- Null (default)
- String (maximum of 255 characters)

**Microsoft Exchange Advanced Login**

You can configure your phone to support the Advanced Login feature which enables a dual sign-in mode for users to make calls and join meetings separately.

When you enable the Advanced Login feature, users can log in to multiple phones using one account to access the Exchange calendar and another account for making calls.
Microsoft Exchange Advanced Login Parameters

Use the following parameters to configure Microsoft Exchange Advanced Login.

**exchange.showSeparateAuth**
0 (default) - Phone disables the dual user sign-in mode.
1 - Phone enables the dual user sign-in mode.

**exchange.auth.email**
This parameter configures the email address of the Exchange account.
NULL (default)
String (maximum of 255 characters)

**device.loginAltCred.domain**
This parameter configures the domain of the Exchange account.
NULL (default)
String (maximum of 255 characters)

**device.loginAltCred.user**
This parameter configures the User ID of Exchange account.
NULL (default)
String (maximum of 255 characters)

**device.loginAltCred.password**
This parameter configures the password of Exchange Account.
NULL (default)
String (maximum of 32 characters)

**device.loginAltCred.domain.set**
This parameter overrides the value set for device.loginAltCred.domain using other configuration methods like the phone menu or the Web Configuration Utility.
0 (default)

**device.loginAltCred.user.set**
This parameter overrides the value set for device.loginAltCred.user using other configuration methods like the phone menu or the Web Configuration Utility.
0 (default)
device.loginAltCred.password.set

This parameter overrides the value set for `device.loginAltCred.password` using other configuration methods like the phone menu or the Web Configuration Utility.

0 (default)
Device Parameters

Topics:

- Changing Device Parameters
- Parameter List Conventions
- Device Parameters

The `<device/>` parameters—also known as device settings—contain default values you can use to configure settings for large-scale device deployments within your network.

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

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

The `<device/>` parameters are designed to be stored in flash memory and for this reason, the phone does not upload `<device/>` parameters to the `<MAC>-web.cfg` or `<MAC>-phone.cfg` override files that store settings you make using the Web Configuration Utility or phone menu. This design protects your ability to manage and access the phones using the standard set of parameters on a provisioning server after the initial software installation. If you configure any parameter values using the `<device/>` parameters, subsequent configuration changes you make from the Web Configuration Utility or phone menu do not take effect after a phone reboot or restart.

Changing Device Parameters

Keep the following in mind when modifying device parameters:

- Note that some parameters may be ignored. For example, if DHCP is enabled, it will still override the value set with `device.net.ipAddress`.
- Though individual parameters are checked to see whether they are in range, the interaction between parameters is not checked. If a parameter is out of range, an error message displays in the log file and the parameter is not used.
- Incorrect configuration can put the phones into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, and server B has a configuration file that specifies that server A should be used.

To detect errors, including IP address conflicts, test the new configuration files on two phones before initializing to all phones.
Types of Device Parameters

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

**device.set**

0 (default) - Don’t use any `device.xxx` fields to set any parameters. Set this to 0 when you are not making changes to device parameters.

1 - Use the `device.xxx` fields that have `device.xxx.set=1`. Set this to 1 when you are making changes to device parameters.

Change may cause system to restart or reboot.

**device.xxx**

  Configuration parameter.

  String

  Change may cause system to restart or reboot.

**device.xxx.set**

0 (default) - Don’t use the `device.xxx` value.

1 - Use the `device.xxx` value.

For example, if `device.net.ipAddress.set=1`, then use the value set for `device.net.ipAddress`.

Change may cause system to restart or reboot.

Parameter List Conventions

For each feature, Poly provides a list of parameters you can use to configure feature settings. Poly provides parameters in XML. This guide documents parameters using parameter lists. Take a moment to familiarize yourself with basic XML and parameter list conventions to successfully perform configuration changes.

**Using XML**

Poly parameters are attributes of XML elements. Element names do not affect the behavior of parameters or operation of your phone and you can customize as needed. When configuring Poly parameters as XML, you must enter parameter names as attributes of a well-formed XML syntax. You can organize parameters into any well-formed XML element structure.

A Poly parameter="value" pair is equivalent to an XML attribute="value" pair. For example:

```xml
<element1>
  <element2 feature.acousticFenceUI.enabled="1" />
</element1>
```
Understanding Parameter Lists
The following describes a general convention for details you can find in parameter lists. Parameter details can vary depending on the complexity of the parameter.

parameter.name
A parameter’s description, applicability, or dependencies, as needed.
The parameter’s permitted values, the default value, and the value’s unit of measure, such as seconds, Hz, or dB.
An indication when a change in a parameter’s value causes a phone restart or reboot.

Note: A note that highlights critical information you need to know.

Examples
To illustrate, the following lists a few example parameters you’ll find in this guide and some XML representations showing how to use them.

feature.acousticFenceUI.enabled
0 (default) - Hide the Acoustic Fence configuration setting on the phone.
1 - Display the Acoustic Fence configuration setting on the phone.
Change causes system to reboot or restart.

XML Representation
<element feature.acousticFenceUI.enabled="1" />

video.enable
1 (default) - Enables video calling capabilities for outgoing and incoming calls.
0 - Disables video calling capabilities.
The G.722.1C and Siren 14 codecs are disabled when you enable video on the VVX 500 and 600 business media phones.

Note: To ensure the USB port is disabled when you set
feature.usbTop.power.enabled to 0, you must also disable this parameter.

XML Representation
<myElement>
  <subElement video.enable="1" />
</myElement>

reg.x.callsPerLineKey
Set the maximum number of concurrent calls for a single registration x you specify. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration.

This per-registration parameter overrides the global parameter call.callsPerLineKey.

All phones except VVX 101 and 201:
24 (default)
1-24

VVX 101 and 201:
8 (default)
1 - 8

XML Representation

```
<registration
  reg.1.callsPerLineKey="3"
  reg.2.callsPerLineKey="1"
  reg.3.callsPerLineKey="1"
/>
```

Device Parameters

Use the following `<device/>` parameters to configure some device settings.

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

---

**device.auth.localAdminPassword**

Set the phone's local administrative password. The minimum length is defined by sec.pwd.length.admin.

string (32 character max)

**device.auth.localUserPassword**

Set the phone user's local password. The minimum length is defined by sec.pwd.length.user.

string (32 character max)

**device.auxPort.enable**

Enable or disable the phone auxiliary port.

0

1 (default)
Change causes system to restart or reboot.

**device.baseProfile**

NULL (default)

Generic — Sets the base profile to Generic for OpenSIP environments.

Lync — Sets this Base Profile for Skype for Business deployments.

SkypeUSB — Sets the Base Profile for connecting the Poly Trio solution to a Microsoft Room System or a Microsoft Surface Hub.

MSTeams — Sets the base profile for Microsoft Teams deployments.

**device.dhcp.bootSrvOpt**

When the boot server is set to Custom or Custom+Option66, specify the numeric DHCP option that the phone looks for.

Null

128 to 254

Change causes system to restart or reboot.

**device.dhcp.bootSrvOptType**

Set the type of DHCP option the phone looks for to find its provisioning server if device.dhcp.bootSrvUseOpt is set to Custom.

IP address — The IP address provided must specify the format of the provisioning server.

String — The string provided must match one of the formats specified by device.prov.serverName.

Change causes system to restart or reboot.

**device.dhcp.bootSrvUseOpt**

Default — The phone looks for option number 66 (string type) in the response received from the DHCP server. The DHCP server should send address information in option 66 that matches one of the formats described for device.prov.serverName.

Custom — The phone looks for the option number specified by device.dhcp.bootSrvOpt, and the type specified by device.dhcp.bootSrvOptType in the response received from the DHCP server.

Static — The phone uses the boot server configured through the provisioning server device.prov.* parameters.

Custom and Default — The phone uses the custom option first or use Option 66 if the custom option is not present.

Change causes system to restart or reboot.

**device.dhcp.dhcpVlanDiscOpt**
Set the DHCP private option to use when device.dhcp.dhcpVlanDiscUseOpt is set to Custom.
128 to 254
Change causes system to restart or reboot.

device.dhcp.dhcpVlanDiscUseOpt
Set how VLAN Discovery occurs.
Disabled—no VLAN discovery through DHCP.
Fixed—use predefined DHCP vendor-specific option values of 128, 144, 157 and 191 (device.dhcp.dhcpVlanDiscOpt is ignored). Custom—use the number specified by device.dhcp.dhcpVlanDiscOpt.
Change causes system to restart or reboot.

device.dhcp.enabled
Enable or disable DHCP.
0
1
Change causes system to restart or reboot.

device.dhcp.option60Type
Set the DHCP option 60 type.
Binary—vendor-identifying information is in the format defined in RFC 3925.
ASCII—vendor-identifying information is in ASCII format.
Change causes system to restart or reboot.

device.dns.altSrvAddress
Set the secondary server to which the phone directs domain name system (DNS) queries.
Server Address
Change causes system to restart or reboot.

device.dns.domain
Set the phone's DNS domain.
String
Change causes system to restart or reboot.

device.dns.serverAddress
Set the primary server to which the phone directs DNS queries.
Device Parameters

Server Address
Change causes system to restart or reboot.

device.hostname
Specify a hostname for the phone when using DHCP by adding a hostname string to the phone’s configuration.

If `device.host.hostname.set` = 1, and `device.host.hostname` = Null, the DHCP client uses Option 12 to send a predefined hostname to the DHCP registration server using Polycom_<MACaddress>.

String — The maximum length of the hostname string is <=255 bytes, and the valid character set is defined in RFC 1035.
Change causes system to restart or reboot.

device.net.cdpEnabled
Determine if the phone attempts to determine its VLAN ID and negotiate power through CDP.

0
1
Change causes system to restart or reboot.

device.net.dot1x.anonid
EAP-TTLS and EAP-FAST only. Set the anonymous identity (user name) for 802.1X authentication.

String
Change causes system to restart or reboot.

device.net.dot1x.enabled
Enable or disable 802.1X authentication.

0
1
Change causes system to restart or reboot.

device.net.dot1x.identity
Set the identity (user name) for 802.1X authentication.

String
Change causes system to restart or reboot.

device.net.dot1x.method
Specify the 802.1X authentication method, where EAP–NONE means no authentication.
device.net.dot1x.password
Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.
String
Change causes system to restart or reboot.

device.net.etherModeLAN
Set the LAN port mode that sets the network speed over Ethernet.
Poly does not recommend you change this setting.
Auto
10HD
10FD
100HD
100FD
1000FD
HD means half-duplex and FD means full duplex.
Change causes system to restart or reboot.

device.net.etherModePC
Set the PC port mode that sets the network speed over Ethernet.
Auto (default)
Disabled—disables the PC port.
10HD
10FD
100HD
100FD
1000FD
HD means half-duplex and FD means full duplex.
Change causes system to restart or reboot.

**device.net.etherStormFilter**
1—DoS storm prevention is enabled and received Ethernet packets are filtered to prevent TCP/IP stack overflow caused by bad data or too much data.
0—DoS storm prevention is disabled.
Change causes system to restart or reboot.

**device.net.etherStormFilterPpsValue**
Set the corresponding packets per second (pps) for storm filter and to control the incoming network traffic.
17 to 40
38 (default)

**device.net.etherStormFilterPpsValue.set**
0 (default) - You cannot configure the `device.net.etherStormFilterPpsValue` parameter.
1 - You can configure the `device.net.etherStormFilterPpsValue` parameter.

**device.net.etherVlanFilter**
VLAN filtering for phones is done by the Linux operating system and it cannot be disabled.
0
1
Change causes system to restart or reboot.

**device.net.ipAddress**
Set the phone's IP address.
This parameter is disabled when `device.dhcp.enabled` is set to 1.
String
Change causes system to restart or reboot.

**device.net.IPgateway**
Set the phone's default router.
IP address
Change causes system to restart or reboot.
device.net.lldpEnabled
0—The phone doesn’t attempt to determine its VLAN ID.
1—The phone attempts to determine its VLAN ID and negotiate power through LLDP.
Change causes system to restart or reboot.

device.net.lldpFastStartCount
Specify the number of consecutive LLDP packets the phone sends at the time of LLDP discovery, which are sent every one second.
5 (default)
3 to 10

device.net.subnetMask
Set the phone’s subnet mask.
This parameter is disabled when device.dhcp.enabled is set to 1.
Change causes system to restart or reboot.

device.net.vlanId
Set the phone’s 802.1Q VLAN identifier.
Null—No VLAN tagging.
0 to 4094
Change causes system to restart or reboot.

device.prov.maxRedunServers
Set the maximum number of IP addresses to use from the DNS.
1 - 8
Change causes system to restart or reboot.

device.prov.password
Set the password for the phone to log in to the provisioning server, which may not be required.
If you modify this parameter, the phone re-provisions. The phone may also reboot if the configuration on the provisioning server has changed.
string
Change causes system to restart or reboot.

device.prov.redunAttemptLimit
Set the maximum number of attempts to attempt a file transfer before the transfer fails. When multiple IP addresses are provided by DNS, 1 attempt is considered to be a request sent to each server.

1 to 10
Change causes system to restart or reboot.

**device.prov.redunInterAttemptDelay**
Set the number of seconds to wait after a file transfer fails before retrying the transfer. When multiple IP addresses are returned by DNS, this delay only occurs after each IP has been tried.

0 to 300
Change causes system to restart or reboot.

**device.prov.serverName**
Enter the IP address, domain name, or URL of the provisioning server followed by an optional directory and optional configuration filename. This parameter is used if (device.dhcp.enabled is 0), if the DHCP server does not send a boot server option, or if the boot server option is static (device.dhcp.bootSrvUseOpt is static).

IP address
Domain name string
URL
If you modify this parameter, the phone re-provisions. The phone also reboots if the configuration on the provisioning server has changed.

**device.prov.serverType**
Set the protocol the phone uses to connect to the provisioning server. Active FTP is not supported for BootROM version 3.0 or later, and only implicit FTPS is supported.

FTP (default)
TFTP
HTTP
HTTPS
FTPS
Change causes system to restart or reboot.

**device.prov.tagSerialNo**
0—The phone's serial number (MAC address) is not included in the User-Agent header of HTTPS/HTTPS transfers and communications to the microbrowser and web browser.
1—the phone's serial number is included.

**device.prov.upgradeServer**
Specify the URL or path for a software version to download to the device.
On the Web Configuration Utility, the path to the software version you specify displays in the drop-down list on the Software Upgrade page.

NULL (default)
string
0 -255 characters

device.prov.user
The user name required for the phone to log in to the provisioning server (if required).
If you modify this parameter, the phone re-provisions, and it may reboot if the configuration on the provisioning server has changed.
string

device.prov.ztpEnabled
Enable or disable Zero Touch Provisioning (ZTP).
0
1
For information, see Zero-Touch Provisioning: https://support.polycom.com/content/support/North_America/USA/en/support/voice/Zero_Touch_Provisioning/zero_touch_provisioning_solution.html.

device.sec.configEncryption.key1
Set the configuration encryption key used to encrypt configuration files.
string
For more information, see the section Configuration File Encryption.
Change causes system to restart or reboot.

device.sec.coreDumpEncryption.enabled
Determine whether to encrypt the core dump or bypass the encryption of the core dump.
0—encryption of the core dump is bypassed.
1 (default)—the core dump is encrypted

device.sec.TLS.customCaCert1( TLS Platform Profile 1 )
Set the custom certificate to use for TLS Platform Profile 1 and TLS Platform Profile 2 and TLS Application Profile 1 and TLS Application Profile 2. The parameter device.sec.TLS.profile.caCertList must be configured to use a custom certificate.
Custom CA certificate cannot exceed 4096 bytes total size.
string
PEM format

device.sec.TLS.customDeviceCert1.privateKey
device.sec.TLS.customDeviceCert2.privateKey

Enter the corresponding signed private key in PEM format (X.509).
Size constraint: 4096 bytes for the private key.

device.sec.TLS.customDeviceCert1.publicCert
device.sec.TLS.customDeviceCert2.publicCert

Enter the signed custom device certificate in PEM format (X.509).
Size constraint: 8192 bytes for the device certificate.

device.sec.TLS.customDeviceCert1.set
device.sec.TLS.customDeviceCert2.set

Use to set the values for parameters device.sec.TLS.customDeviceCertX.publicCert
and device.sec.TLS.customDeviceCertX.privateKey.
Size constraints are: 4096 bytes for the private key, 8192 bytes for the device certificate.
0 (default)
1

device.sec.TLS.profile.caCertList1 ( TLS Platform Profile 1 )

Choose the CA certificate(s) to use for TLS Platform Profile 1 and TLS Platform Profile 2 authentication:
Builtin—The built-in default certificate
BuiltinAndPlatform—The built-in and Custom #1 certificates
BuiltinAndPlatform2—The built-in and Custom #2 certificates
All—Any certificate (built in, Custom #1 or Custom #2)
Platform1—Only the Custom #1 certificate
Platform2—Only the Custom #2 certificate
Platform1AndPlatform2—Either the Custom #1 or Custom #2 certificate

device.sec.TLS.profile.cipherSuite1 ( TLS Platform Profile 1 )

Enter the cipher suites to use for TLS Platform Profile 1 and TLS Platform Profile 2
string

device.sec.TLS.profile.cipherSuiteDefault1 ( TLS Platform Profile 1 )
Determine the cipher suite to use for TLS Platform Profile 1 and TLS Platform profile 2.
0—The custom cipher suite is used.
1—The default cipher suite is used.

device.sec.TLS.profile.deviceCert1 ( TLS Platform Profile 1 )
Choose the device certificate(s) for TLS Platform Profile 1 and TLS Platform Profile 2 to use for authentication.
Builtin
Platform1
Platform2

device.sec.TLS.profileSelection.dot1x
Choose the TLS Platform Profile to use for 802.1X.
PlatformProfile1
PlatformProfile2

device.sec.TLS.profileSelection.provisioning
Set the TLS Platform Profile to use for provisioning.
PlatformProfile1
PlatformProfile2
Change causes system to restart or reboot.

device.sec.TLS.profileSelection.syslog
Set the TLS Platform Profile to use for syslog.
PlatformProfile1
PlatformProfile2
Change causes system to restart or reboot.

device.sec.TLS.prov.strictCertCommonNameValidation
0
1 (default)—Provisioning server always verifies the server certificate for the commonName/SubjectAltName match with the server hostname that the phone is trying to connect.

device.sec.TLS.syslog.strictCertCommonNameValidation
0
1—Syslog always verifies the server certificate for the commonName/SubjectAltName match with the server hostname that the phone is trying to connect.
**device.sntp.gmtOffset**

Set the GMT offset—in seconds—to use for daylight savings time, corresponding to -12 to +13 hours.

-43200 to 46800

**device.sntp.gmtOffsetcityID**

Sets the correct time zone location description that displays on the phone menu and in the Web Configuration Utility.

NULL (default)

0 to 126 (The maximum range for Poly Trio system is 127.)

For descriptions of all values, refer to Time Zone Location Description.

**device.sntp.serverName**

Enter the SNTP server from which the phone obtains the current time.

IP address

Domain name string

**device.syslog.facility**

Determine a description of what generated the log message.

0 to 23

For more information, see RFC 3164.

**device.syslog.prependMac**

0

1—The phone's MAC address is prepended to the log message sent to the syslog server.

Change causes system to restart or reboot.

**device.syslog.renderLevel**

Specify the logging level for the lowest severity of events to log in the syslog. When you choose a log level, the log includes all events of an equal or greater severity level, but it excludes events of a lower severity level.

0 or 1—SeverityDebug(7).

2 or 3—SeverityInformational(6).

4—SeverityError(3).

5—SeverityCritical(2).

6—SeverityEmergency(0).

Change causes system to restart or reboot.
**device.syslog.serverName**
Set the syslog server IP address or domain name string.
- **IP address**
- **Domain name string**

**device.syslog.transport**
Set the transport protocol that the phone uses to write to the syslog server.
- **None**—Transmission is turned off but the server address is preserved.
- **UDP**
- **TCP**
- **TLS**

**device.wifi.country**
Enter the two-letter code for the country where you are operating the Poly Trio 8300 or Poly Trio 8800 solution with Wi-Fi enabled.

**Note:** The Poly Trio 8500 does not support Wi-Fi connectivity.
- **NULL (default)**
- **Two-letter country code**

**device.wifi.dhcpBootServer**
- 0 (default)
- 1
- 2
- V4
- V6
- **Static**

**device.wifi.dhcpEnabled**
Enable or disable DHCP for Wi-Fi.
- 0 (default)
- 1

**device.wifi.enabled**
Enable or disable Wi-Fi.
- 0 (default)
**device.wifi.ipAddress**
Enter the IP address of the wireless device if you are not using DHCP.
0.0.0.0 (default)
String

**device.wifi.ipGateway**
Enter the IP gateway address for the wireless interface if not using DHCP.
0.0.0.0 (default)
String

**device.wifi.psk.key**
Enter the hexadecimal key or ASCII passphrase.
0xFF (default)
String

**device.wifi.radio.band2_4GHz.enable**
Enable or disable 2.4 GHz band for Wi-Fi.
0 (default)
1

**device.wifi.radio.band5GHz.enable**
Enable or disable the 5 GHz band for Wi-Fi.
0 (default)
1

**device.wifi.securityMode**
Specify the wireless security mode.
NULL (default)
None
WEP
WPA-PSK
WPA2-PSK
WPA2-Enterprise
device.wifi.ssid
  Set the Service Set Identifier (SSID) of the wireless network.
  SSID1 (default)
  SSID

device.wifi.subnetMask
  Set the network mask address of the wireless device if not using DHCP.
  255.0.0.0 (default)
  String

device.wifi.wep.key
  Set the length of the hexadecimal WEP key.
  0 = 40-bits (default)
  1 = 104-bits

device.wifi.wpa2Ent.caCert.name
  For use with the Poly Trio 8800 system. Specify the CA certificate for Wireless WPA2 Enterprise security. To use the default certificate, set the value to Poly 802.1X Device Certificate.
  NULL (default)
  String (0 - 128 characters)

device.wifi.wpa2Ent.clientCert.name
  For use with the Poly Trio 8800 system. Specify the Client certificate for Wireless WPA2 Enterprise security. To use the default certificate, set the value to Poly 802.1X Device Credential.
  NULL (default)
  String (0 - 128 characters)

device.wifi.wpa2Ent.method
  Set the Extensible Authentication Protocol (EAP) to use for 802.1X authentication.
  NULL (default)
  EAP-PEAPv0/MSCHAPv2
  EAP-FAST
  EAP-TLS
  EAP-PEAPv0-GTC
  EAP-TTLS-MSCHAPv2
  EAP-TTLS-GTC
  EAP-PEAPv0-NONE
EAP-TTLS-NONE
EAP-PWD

device.wifi.wpa2Ent.password
For use with the Poly Trio 8800 system. Enter the WPA2-Enterprise password.

device.wifi.wpa2Ent.user
For use with the Poly Trio 8800 system. Enter the WPA2-Enterprise user name.
Configuration Parameters

Topics:

- Quick Setup Soft Key Parameter
- Per-Registration Call Parameters
- Remote Packet Capture Parameters
- Per-Registration Dial Plan Parameters
- Local Contact Directory File Size Parameters
- Feature Activation/Deactivation Parameters
- HTTPD Web Server Parameters
- Feature License Parameter
- Chord Parameters
- Message Waiting Parameters
- Ethernet Interface MTU Parameters
- Presence Parameters
- Provisioning Parameters
- Configuration Request Parameter
- General Security Parameters
- User Preferences Parameters
- Upgrade Parameters
- Voice Parameters
- Session Description Protocol (SDP) Parameters
- Web Configuration Utility Language File Download Parameter
- XML Streaming Protocol Parameters
- Session Headers

This section is a reference for configuration parameters available for UC Software features.

Quick Setup Soft Key Parameter

Use the following parameter to configure Quick Setup soft key.

prov.quickSetup.enabled

0 (default) - Disables the quick setup feature.
1 - Enables the quick setup feature.
Per-Registration Call Parameters

Poly phones support an optional per-registration feature that enables automatic call placement when the phone is off-hook.

The phones also support a per-registration configuration that determines which events cause the missed-calls counter to increment. You can enable/disable missed call tracking on a per-line basis.

In the following parameters, x is the registration number.

**call.advancedMissedCalls.addToReceivedList**

- Applies to calls on that are answered remotely.
- 0 (default) - Calls answered from the remote phone are not added to the local receive call list.
- 1 - Calls answered from the remote phone are added to the local receive call list.

**call.advancedMissedCalls.enabled**

- Use this parameter to improve call handling.
- 1 (default) - Shared lines can correctly count missed calls.
- 0 - Shared lines may not correctly count missed calls.

**call.advancedMissedCalls.reasonCodes**

- Enter a comma-separated list of reason code indexes interpreted to mean that a call should not be considered as a missed call.
- 200 (default)

**call.autoAnswer.micMute**

- 1 (default) - The microphone is initially muted after a call is auto-answered.
- 0 - The microphone is active immediately after a call is auto-answered.

**call.autoAnswer.ringClass**

- The ring class to use when a call is to be automatically answered using the auto-answer feature. If set to a ring class with a type other than answer or ring-answer, the setting are overridden such that a ringtone of visual (no ringer) applies.
- ringAutoAnswer (default)

**call.autoAnswer.ringTone**
Intercom (default) – Auto answer plays the intercom tone.

doubleBeep – Auto answer plays the double-beep tone.

call.autoAnswer.SIP

0 (default) - Disable auto-answer for SIP calls.
1 - Enable auto-answer for SIP calls.

call.autoAnswer.ringTone

intercom (default) – While auto answering a call, phone plays an intercom tone.
doubleBeep – Phone plays the double beep tone.

call.autoAnswerMenu.enable

1 (default) - The Autoanswer menu displays and is available to the user.
0 - The Autoanswer menu is disabled and is not available to the user.

call.BlindTransferSpecialInterop

0 (default) - Do not wait for an acknowledgment from the transferee before ending the call.
1 - Wait for an acknowledgment from the transferee before ending the call.

call.dialtoneTimeOut

The time is seconds that a dial tone plays before a call is dropped.

60 (default)
0 - The call is not dropped.
Change causes system to restart or reboot.

call.internationalDialing.enabled

Use this parameter to enable or disable the key tap timer that converts a double tap of the asterisk (*) symbol to the plus (+) symbol used to indicate an international call.

1 (default) - A quick double tap of * converts immediately to +. To enter a double asterisk (**), tap the asterisk (*) once and wait for the key tap timer to expire to enter a second asterisk (*).
0 - You cannot dial plus (+) symbol and you must enter the international exit code of the country you are calling from to make international calls.
This parameter applies to all numeric dial pads on the phone including for example, the contact directory.
Change causes system to restart or reboot.

call.internationalPrefix.key

0 (default)
**call.localConferenceEnabled**

1 (default) - The feature to join a conference during an active call is enabled and the Conference soft key displays.

0 - The feature to join a conference during an active call is disabled and the Conference soft key does not display. When you try to join the Conference, an "Unavailable" message displays.

Change causes system to restart or reboot.

**call.offeringTimeOut**

Specify a time in seconds that an incoming call rings before the call is dropped.

60 (default)

0 - No limit.

Note that the call diversion, no answer feature takes precedence over this feature when enabled.

Change causes system to restart or reboot.

**call.playLocalRingBackBeforeEarlyMediaArrival**

Determines whether the phone plays a local ring-back after receiving a first provisional response from the far end.

1 (default) - The phone plays a local ringback after receiving the first provisional response from the far end. If early media is received later, the phone stops the local ringback and plays the early media.

0 - No local ringback plays, and the phone plays only the early media received.

**call.playLocalRingBackBeforeEarlyMediaArrival**

0 (default) - URL mode is used for URL calls.

1 - Number mode is used for URL calls.

**call.ringBackTimeOut**

Specify a time in seconds to allow an outgoing call to remain in the ringback state before dropping the call.

60 (default)

0 - No limit.

Change causes system to restart or reboot.

**call.showDialpadOnProceeding**

0 (default) – The phone does not show the dialpad button while a placed call is outgoing.

1 – The phone displays the dialpad button while a placed call is outgoing.
**call.stickyAutoLineSeize**

0 (default) - Dialing through the call list uses the line index for the previous call. Dialing through the contact directory uses a random line index.

1 - The phone uses sticky line seize behavior. This helps with features that need a second call object to work with. The phone attempts to initiate a new outgoing call on the same SIP line that is currently in focus on the LCD. Dialing through the call list when there is no active call uses the line index for the previous call. Dialing through the call list when there is an active call uses the current active call line index. Dialing through the contact directory uses the current active call line index.

Change causes system to restart or reboot.

**call.stickyAutoLineSeize.onHookDialing**

0 (default)

If `call.stickyAutoLineSeize` is set to 1, this parameter has no effect. The regular `stickyAutoLineSeize` behavior is followed.

If `call.stickyAutoLineSeize` is set to 0 and this parameter is set to 1, this overrides the `stickyAutoLineSeize` behavior for hot dial only. (Any new call scenario seizes the next available line.)

If `call.stickyAutoLineSeize` is set to 0 and this parameter is set to 0, there is no difference between hot dial and new call scenarios.

A hot dial occurs on the line which is currently in the call appearance. Any new call scenario seizes the next available line.

Change causes system to restart or reboot.

**call.switchToLocalRingbackWithoutRTP**

Determines whether local ringback plays in the event that early media stops.

0 (default) – No ringback plays when early media stops.

1 – The local ringback plays if no early media is received.

**call.teluri.showPrompt**

1 (default) - Phone displays a pop-up box to either call or cancel the number when tel URI is executed.

0 - Phone does not display the pop-up box.

**call.urlModeDialing**

0 (default) - Disable URL dialing.

1 - Enable URL dialing.

Change causes system to restart or reboot.
Remote Packet Capture Parameters

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

**diags.dumpcore.enabled**

- Determine whether the phone generates a core file if it crashes.
  - 1 (default)
  - 0
  - Change causes system to restart or reboot.

**diags.pcap.enabled**

- Enable or disable all on-board packet capture features.
  - 0 (default)
  - 1

**diags.pcap.remote.enabled**

- Enable or disable the remote packet capture server.
  - 0 (default)
  - 1

**diags.pcap.remote.password**

- Enter the remote packet capture password.
  - `<MAC Address>` (default)
  - alphanumeric value

**diags.pcap.remote.port**

- Specify the TLS profile to use for each application.
  - 2002 (default)
  - Valid TCP Port

Per-Registration Dial Plan Parameters

All the following parameters are per-registration parameters that you can configure instead of the general equivalent dial plan parameters.

Note that the per-registration parameters override the general parameters where x is the registration number; for example, `dialplan.x.applyToTelUriDial` overrides `dialplan.applyToTelUriDial` for registration x.
**dialplan.userDial.timeOut**

Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook.

- Generic Base Profile (default) – 0
- Lync Base Profile (default) – 4
- 0-99 seconds

You can apply `dialplan.userDial.timeOut` only when its value is lower than `up.IdleTimeOut`.

**dialplan.x.applyToCallListDial**

- Generic Base Profile (default) – 1
- Lync Base Profile (default) – 0
- 0 - The dial plan does not apply to numbers dialed from the received call list or missed call list, including sub-menus for this line.
- 1 - The dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus for this line.

Change causes system to restart or reboot.

**dialplan.x.applyToDirectoryDial**

- Generic Base Profile (default) – 1
- Lync Base Profile (default) – 0
- Poly Trio (default) - 0
- 0 - The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers for this line.
- 1 - The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers for this line.

Change causes system to restart or reboot.

**dialplan.x.applyToForward**

- Generic Base Profile (default) – 1
- Lync Base Profile (default) – 0
- Poly Trio system (default) - 0
- 0 - The dial plan applies to forwarded calls for this line.
- 1 - The dial plan applies to forwarded calls for this line.

**dialplan.x.applyToFtelUriDial**

0
1 (default)
Change causes system to restart or reboot.

dialplan.x.applyToUserDial
0
1 (default)
Change causes system to restart or reboot.

dialplan.x.applyToUserSend
0
1 (default)
Change causes system to restart or reboot.

dialplan.x.conflictMatchHandling
Selects the dialplan based on more than one match with the least timeout.
0 (default for Generic Profile)
1 (default for Skype Profile)

dialplan.x.digitmap.timeOut
Generic Base Profile (default) – 0
Lync Base Profile (default) – 4
Change causes system to restart or reboot.

dialplan.x.digitmap
Generic Base Profile (default) - Null
Lync Base Profile (default) - 4
string - max number of characters 100
Change causes system to restart or reboot.

dialplan.x.e911dialmask
Null (default)
string - max number of characters 256

dialplan.x.e911dialstring
Null (default)
string - max number of characters 256
dialplan.x.impossibleMatchHandling

0 (default) - Digits are sent to the call server immediately.
1 - A reorder tone is played and the call is canceled.
2 - No digits are sent to the call server until the Send or Dial key is pressed.
3 - No digits are sent to the call server until the timeout is configured by dialplan.X.impossibleMatchHandling.timeOut parameter.
Change causes system to restart or reboot.

null (default)
string - max number of characters 2560

-dialplan.x.removeEndOfDial

0
1 (default)
Change causes system to restart or reboot.

-dialplan.x.routing.emergency.y.server.z

0 (default)
1
2
3
x, y, and z = 1 to 3
Change causes system to restart or reboot.

-dialplan.x.routing.emergency.y.value

Null (default)
string - max number of characters 64
Change causes system to restart or reboot.

-dialplan.x.routing.server.y.address

Null (default)
string - max number of characters 256
Change causes system to restart or reboot.

-dialplan.x.routing.server.y.port

5060 (default)
1 to 65535
Change causes system to restart or reboot.

`dialplan.x.routing.server.y.transport`

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

Change causes system to restart or reboot.

**Local Contact Directory File Size Parameters**

Use the following parameters to set the size of the local contact directory.

The maximum local directory size is limited based on the amount of flash memory in the phone and varies by phone model. Poly recommends that you configure a provisioning server that allows uploads to ensure a back-up copy of the directory when the phone reboots or loses power.

`dir.local.nonVolatile.maxSize`

Set the maximum file size of the local contact directory stored on the phone's non-volatile memory.

- 1 - 100KB

`dir.local.volatile`

- 0 (default) - The phone uses non-volatile memory for the local contact directory.
- 1 - Enables the use of volatile memory for the local contact directory.

`dir.local.volatile.maxSize`

Sets the maximum file size of the local contact directory stored on the phone's volatile memory.

- 1 - 200KB
Parameter Elements for the Local Contact Directory

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

Local Contact Directory Parameter Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
<th>Permitted Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>fn</td>
<td>The contact’s first name.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>ln</td>
<td>The contact’s last name.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>ct</td>
<td>Contact. Used by the phone to address a remote party in the same way that a string of digits or a SIP URL are dialed manually by the user. This element is also used to associate incoming callers with a particular directory entry. The maximum field length is 128 characters. Note: This field cannot be null or duplicated.</td>
<td>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</td>
</tr>
<tr>
<td>sd</td>
<td>Speed Dial Index, Associates a particular entry with a speed dial key for one-touch dialing or dialing.</td>
<td>20</td>
</tr>
<tr>
<td>lb</td>
<td>The label for the contact. The label of a contact directory item is by default the label attribute of the item. If the label attribute does not exist or is Null, then the first and last names form the label. A space is added between first and last names.</td>
<td>UTF-8 encoded string of up to 40 bytes1</td>
</tr>
<tr>
<td>Element</td>
<td>Definition</td>
<td>Permitted Values</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>pt</strong></td>
<td>Protocol,</td>
<td>SIP, H323, or Unspecified</td>
</tr>
<tr>
<td></td>
<td>The protocol to use when placing a call to this contact.</td>
<td></td>
</tr>
<tr>
<td><strong>rt</strong></td>
<td>Ring Tone,</td>
<td>Null, 1 to 21</td>
</tr>
<tr>
<td></td>
<td>When incoming calls match a directory entry, this field specifies the ringtone to be used.</td>
<td></td>
</tr>
<tr>
<td><strong>dc</strong></td>
<td>Divert Contact,</td>
<td>UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL</td>
</tr>
<tr>
<td></td>
<td>The address to forward calls to if the Auto Divert feature is enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>ad</strong></td>
<td>Auto Divert,</td>
<td>0 or 1</td>
</tr>
<tr>
<td></td>
<td>If set to 1, callers that match the directory entry are diverted to the address specified for the divert contact element.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If auto-divert is enabled, it has precedence over auto-reject.</td>
<td></td>
</tr>
<tr>
<td><strong>ar</strong></td>
<td>Auto Reject,</td>
<td>0 or 1</td>
</tr>
<tr>
<td></td>
<td>If set to 1, callers that match the directory entry specified for the auto reject element are rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If auto divert is also enabled, it has precedence over auto reject.</td>
<td></td>
</tr>
<tr>
<td><strong>bw</strong></td>
<td>Buddy Watching,</td>
<td>0 or 1</td>
</tr>
<tr>
<td></td>
<td>If set to 1, this contact is added to the list of watched phones.</td>
<td></td>
</tr>
</tbody>
</table>
### Element | Definition | Permitted Values
--- | --- | ---
bb | Buddy Block, If set to 1, this contact is blocked from watching this phone. | 0 or 1
up | User Photo The contact's photo icon. | 1-24

**Related Links**

[Example: Set Icons for Speed Dial Contacts](#) on page 225

## Feature Activation/Deactivation Parameters

Use the feature parameters to control the activation or deactivation of a feature at run time.

**feature.callCenterCallInformation.enable**

1 (default) - The phone displays a full-screen popup showing call information details. The popup closes after 40 seconds or you can press the **Exit** button to close it and return to the active call screen. You can set how long the popup displays using the parameter `up.idleTimeout`.

0 - The phone uses the active call screen and ACD call information is not available.

**feature.callCenterStatus.enabled**

0 (default) - Disable the status event threshold capability.

1 - Enable the status event threshold capability to display at the top of the phone screen.

**feature.enhancedCallDisplay.enabled**

0 (default) - The phone displays the protocol at the end of the called party identification (for example, 1234567 [SIP]).

1 - The phone displays the number only (for example, 1234567).

**feature.flexibleLineKey.enable**

0 (default) - Disables the Flexible Line Key feature.

1 - Enables the Flexible Line Key feature.

**feature.ringDownload.enabled**

1 (default) - The phone downloads ringtones when starting up.

0 - The phone does not download ringtones when starting up.
Change causes system to restart or reboot.

**feature.uniqueCallLabeling.enabled**

0 (default) - Disable Unique Call Labeling.
1 - Enable Unique Call Labeling. Use `reg.x.line.y.label` to define unique labels.

Change causes system to restart or reboot.

**feature.urlDialing.enabled**

1 (default) - URL/name dialing is available from private lines, and unknown callers are identified on the display by their phone’s IP address.
0 - URL/name dialing is not available.

**feature.usb.device.enabled**

The USB device port enables you to use a Poly Trio system as an audio device for your laptop.
1 (default) - Enable the USB device port.
0 - Disable the USB device port.

When you disable the Poly Trio system’s USB device port using the parameter `feature.usb.device.enabled`, the USB Connections settings do not display on the phone menu at Settings > Advanced > Administration Settings > USB Computer Connections.

**feature.usb.host.enabled**

1 (default) Enable the USB host port on the Poly Trio system.
0 - Disable the USB host port on the Poly Trio system.

Use the host port for memory sticks, mouse, keyboards, and charging your devices.

**reg.x.urlDialing.enabled**

1 (default) - Enable dialing by URL for SIP registrations.
0 - Disable dialing by URL for SIP registrations.

---

**HTTPD Web Server Parameters**

The phone contains a local Web Configuration Utility server for user and administrator features.

Note that several of these parameters can be used with Microsoft Skype for Business Server and the parameter values have two default states: a generic default value and a different value when the phone is registered with Skype for Business Server. The default values are listed for both states where applicable.

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

Base Profile = Generic
1 (default) - The web server is enabled.
0 - The web server is disabled.

Base Profile = Skype
0 (default) - The web server is disabled.
1 - The web server is enabled.

Change causes system to restart or reboot.

**httpd.cfg.enabled**

Base Profile = Generic
1 (default) - The Web Configuration Utility is enabled.
0 - The Web Configuration Utility is disabled.

Base Profile = Skype
0 (default) - The Web Configuration Utility is disabled.
1 - The Web Configuration Utility is enabled.

Change causes system to restart or reboot.

**httpd.cfg.port**

Port is 80 for HTTP servers. Take care when choosing an alternate port.

80 (default)
1 to 65535

Change causes system to restart or reboot.

**httpd.cfg.secureTunnelPort**

The port to use for communications when the secure tunnel is used.

443 (default)
1 to 65535

Change causes system to restart or reboot.

**httpd.cfg.secureTunnelRequired**

1 (default) - Access to the Web Configuration Utility is allowed only over a secure tunnel (HTTPS) and non-secure (HTTP) is not allowed.

0 - Access to the Web Configuration Utility is allowed over both a secure tunnel (HTTPS) and non-secure (HTTP).

Change causes system to restart or reboot.
Feature License Parameter

Use the following parameter to configure the feature licensing system.
Once the license is installed on a phone, it cannot be removed.

**license.polling.time**

Specifies the time (using the 24-hour clock) to check if the license has expired.

02:00 (default)
00:00 - 23:59

Change causes system to restart or reboot.

Chord Parameters

Chord-sets are the sound effect building blocks that use synthesized audio instead of sampled audio.

Most call progress and ringer sound effects are synthesized. A chord-set is a multi-frequency note with an optional on/off cadence, and can contain up to four frequency components generated simultaneously, each with its own level.

Three chord sets are supported: **callProg**, **misc**, and **ringer**. Each chord set has different chord names, represented by x in the following parameters.

For **callProg**, x can be one of the following chords:
- dialTone
- busyTone
- ringback
- reorder
- stutter_3
- callWaiting
- callWaitingLong
- howler
- recWarning
- stutterLong
- intercom
- callWaitingLong
- precedenceCallWaiting
- preemption
- precedenceRingback
- spare1 to spare6

For **misc**, x can be one of the following chords:
- spare1 to spare9
- cs1 to cs12.

For **ringer**, x can be one of the following chords:
- ringback
- originalLow
- originalHigh
- spare1 to spare19

**tone.chord.callProg.x.freq.y**  **tone.chord.misc.x.freq.y**  **tone.chord.ringer.x.freq.y**

Frequency (in Hertz) for component y. Up to six chord-set components can be specified (y=1 to 6).

0-1600

**tone.chord.callProg.x.level.y**  **tone.chord.misc.x.level.y**  **tone.chord.ringer.x.level.y**

Level of component y in dBm0. Up to six chord-set components can be specified (y=1 to 6).
-57 to 3

tone.chord.callProg.x.onDur  tone.chord.misc.x.onDur  tone.chord.ringer.x.onDur
   On duration (length of time to play each component) in milliseconds.
   0=infinite
   positive integer

tone.chord.callProg.x.offDur  tone.chord.misc.x.offDur  tone.chord.ringer.x.offDur
   Off duration (the length of silence between each chord component) in milliseconds
   0=infinite
   positive integer

tone.chord.callProg.x.repeat  tone.chord.misc.x.repeat  tone.chord.ringer.x.repeat
   Number of times each ON/OFF cadence is repeated.
   0=infinite
   positive integer

**Message Waiting Parameters**

Use the following parameters to configure the message-waiting feature, supported on a per-registration basis.

The maximum number of registrations (x) for each phone model is listed in the topic Flexible Call Appearances under the column Registrations.

**msg.bypassInstantMessage**

0 (default) - Displays the menus Message Center and Instant Messages on pressing Messages or MSG key.

1 - Bypasses the menus and goes to voicemail.

**msg.mwi.x.led**

1 (default) - The LED flashes as long as new unread voicemail messages is there for any line.

0 - Red MWI LED doesn't flash when there's new unread messages for the selected line.

Also, x is an integer referring to the registration indexed by reg.x.
Ethernet Interface MTU Parameters

Use the following parameters to control the Ethernet interface maximum transmission unit (MTU).

```
net.interface.mtu
  Configures the Ethernet or Wi-Fi interface maximum transmission unit (MTU).
  1496 (default)
  800 - 1500
  This parameter affects the LAN port and the PC port.
```

```
net.interface.mtu6
  Specifies the MTU range for IPv6.
  1500 (default)
  1280 - 1500
```

```
net.lldp.extenedDiscovery
  Specifies the duration of time that LLDP discovery continues after sending the number of packets defined by the parameter lldpFastStartCount.
  0 (default)
  0 - 3600
  The LLDP packets are sent every 5 seconds during this extended discovery period.
```

Presence Parameters

Use the following parameters to configure for the presence feature.

Note that the parameter `pres.reg` is the line number used to send SUBSCRIBE. If this parameter is missing, the phone uses the primary line to send SUBSCRIBE.

```
pres.idleTimeoutoffHours.enabled
  1 (default) - Enables the off hours idle timeout feature.
  0 - Disables the off hours idle timeout feature.
```

```
pres.idleTimeoutoffHours.period
  The number of minutes to wait while the phone is idle during off hours before showing the Away presence status.
  15 (default)
  1 - 600
```
**pres.idleTimeout.officeHours.enabled**

1 (default) - Enables the office hours idle timeout feature
0 - Disables the office hours idle timeout feature

**pres.idleTimeout.officeHours.periods**

The number of minutes to wait while the phone is idle during office hours before showing the Away presence status
15 (default)
1 - 600

---

**Provisioning Parameters**

Use the following parameters to control the provisioning server system for your phones.

**prov.autoConfigUpload.enabled**

1 (default) - Enables the automatic upload of configuration files from the phone or Web configuration utility to the provisioning server.
0 - Disabled the automatic upload of configuration files from the phone or Web configuration utility to the provisioning server.

**prov.configUploadPath**

Specifies the directory path where the phone uploads the current configuration file.
Null (default)
String

**prov.login.lcCache.domain**

The user's domain name to sign-in.
Null (default)
String

**prov.login.lcCache.user**

The user's sign-in name to login.
Null (default)
String

**prov.login.password.encodingMode**

The default encoding mode for the text in the Password field on the User Login screen.
**prov.login.userId.encodingMode**

The default encoding mode for the text in the User ID field on User Login screen.

- 123 (default)
- Alphanumeric

**prov.loginCredPwdFlushed.enabled**

- 1 (default) - Resets the password field when the user logs in or logs out.
- 0 - Does not reset the password field when the user logs in or logs out.

**prov.startupCheck.enabled**

- 1 (default) - The phone is provisioned on startup.
- 0 - The phone is not provisioned on startup.

**prov.quickSetup.limitServerDetails**

- 0 (default) - Provide all the necessary details for the given fields.
- 1 - Enter only the user name and password fields. Other details are taken from `ztp/dhcp` (option66).

### Configuration Request Parameter

Use the following parameter to configure the phone's behavior when a request for restart or reconfiguration is received.

**request.delay.type**

- Specifies whether the phone should restart or reconfigure.
- `call` (default) - The request will be executed when there are no calls.
- `audio` - The request will be executed when there is no active audio.
- Change causes system to restart or reboot.

### General Security Parameters

Use the following parameters to configure security features of the phone.

**sec.tagSerialNo**
0 (default) - The phone does not display the serial number.
1 - The phone displays the serial number through protocol signaling.
Change causes system to restart or reboot.

**sec.uploadDevice.privateKey**
0 (default) - While generating the Certificate Signing Request from the phone, the device private key is not uploaded to provisioning server.
1 - The device private key is uploaded to provisioning server along with the CSR.

**DHCP Parameter**
Use the following parameter to configure how the phone reacts to DHCP changes.

**tcpIpApp.dhcp.releaseOnLinkRecovery**
Specifies whether or not a DHCP release occurs.
1 (default) - Performs a DHCP release after the loss and recovery of the network.
0 - No DHCP release occurs.

**Domain Name System (DNS) Parameters**
Use the following parameters to set the Domain Name System (DNS).
However, values set using DHCP have a higher priority, and values set using the `<device/>` parameter in a configuration file have a lower priority.

**tcpIpApp.dns.server**
Phone directs DNS queries to this primary server.
NULL (default)
IP address
Change causes system to restart or reboot.

**tcpIpApp.dns.altServer**
Phone directs DNS queries to this secondary server.
NULL (default)
IP address
Change causes system to restart or reboot.

**tcpIpApp.dns.domain**
Specifies the DNS domain for the phone.
NULL (default)
TCP Keep-Alive Parameters
Use the following parameters to configure TCP keep-alive on SIP TLS connections; the phone can detect a failure quickly (in minutes) and attempt to re-register with the SIP call server (or its redundant pair).

**tcpIpApp.keepalive.tcp.idleTransmitInterval**
Specifies the amount of time to wait (in seconds) before sending the keep-alive message to the call server. Range is 10 to 7200.
30 (Default)
If this parameter is set to a value that is out of range, the default value is used.
Specifies the number of seconds TCP waits between transmission of the last data packet and the first keep-alive message.

**tcpIpApp.keepalive.tcp.noResponseTransmitInterval**
Specifies the amount of idle time between the transmission of the keep-alive packets the TCP stack waits on. This applies whether or not the last keep-alive was acknowledged.
If no response is received to a keep-alive message, subsequent keep-alive messages are sent to the call server at this interval (every x seconds). Range is 5 to 120.

**tcpIpApp.keepalive.tcp.sip.persistentConnection.enable**
Specifies whether the TCP socket connection remains open or closes.
0 (Default) - The TCP socket opens a new connection when the phone tries to send any new SIP message and closes after one minute.
1 - The TCP socket connection remains open.
Change causes system to restart or reboot.

**tcpIpApp.keepalive.tcp.sip.tls.enable**
Specifies whether to disable or enable TCP keep-alive for SIP signaling connections.
0 (Default) - Disables TCP keep-alive for SIP signaling connections that use TLS transport.
1 - Enables TCP keep-alive for SIP signaling connections that use TLS transport.

File Transfer Parameter
Use the following parameter to configure file transfers from the phone to the provisioning server.

**tcpIpApp.fileTransfer.waitForLinkIfDown**
Specifies whether a file transfer from the FTP server is delayed or not attempted.
1 (Default) - File transfer from the FTP server is delayed until Ethernet comes back up.
0 - File transfer from the FTP server is not attempted.

User Preferences Parameters
Sets phone user preferences.

up.25mm
Specifies whether to use a mobile phone or a PC to connect to the 2.5mm audio port on a conference phone.
1 (Default) - Mobile phone
2 - PC

up.backlight.idleIntensity
Brightness of the LCD backlight when the phone is idle. Range is 0 to 3.
1 (Default) - Low
0
2 - Medium
3 - High
If this setting is higher than active backlight brightness (onIntensity), the active backlight brightness is used.

up.backlight.onIntensity
Brightness of the LCD backlight when the phone is active (in use). Range is 0 to 3.
3 (Default) - High
1 - Low
2 - Medium

up.backlight.timeout
Number of seconds to wait before the backlight dims from the active intensity to the idle intensity. Range is 5 to 60.
40 (default)

up.basicSettings.networkConfigEnabled
Specifies whether Network Configuration is shown or not shown under the Basic Settings menu.
0 (default) - Network Configuration is not shown under Basic Settings.
Basic Settings menu shows Network Configuration with configurable network options for the user without administrator rights.

**up.DIDFormat**

NumberAndExtension (default) – Display the DID number and extension.

NumberOnly – Display the DID number on the phone screen.

**up.cfgWarningsEnabled**

Specifies whether a warning displays on a phone or not.

0 (Default) - Warning does not display.

1 - Warning is displayed on the phone if it is configured with pre-UC Software 3.3.0 parameters.

**up.formatPhoneNumbers**

Enable or disable automatic number formatting.

1 (Default)

0

**up.hearingAidCompatibility.enabled**

Specifies whether audio Rx equalization is enabled or disabled.

0 (Default) - Audio Rx equalization is enabled.

1 - Phone audio Rx (receive) equalization is disabled for hearing aid compatibility.

**up.idleBrowser.enabled**

Specifies if the idle browser is enabled or disabled.

0 (Default) - Idle browser is disabled.

1 - Idle browser is enabled.

If the parameter `up.prioritizeBackgroundMenuItem.enabled` is set to 1, displays the background or the idle browser on the phone menu.

**up.idleRestingState**

menu (default) – The idle screen will display the Home screen menu.

calendar – The idle screen will display a top-level calendar.

dialpad – The idle screen will display a dial pad

**up.idleStateView**

Sets the phone default view.

0 (Default) - Call/line view is the default view.
1 - Home screen is the default view.
Change causes system to restart or reboot.

**up.idleTimeout**
Set the number of seconds that the phone is idle for before automatically leaving a menu and showing the idle display.
During a call, the phone returns to the Call screen after the idle timeout.
40 seconds (default)
0 to 65535 seconds
Change causes system to restart or reboot.

**up.IdleViewPreferenceRemoteCalls**
Determines when the phone displays the idle browser.
0 (Default) - Phone with only remote calls active, such as on a BLF monitored line, is treated as in the idle state and the idle browser displays.
1 - Phone with only remote calls active, such as on a BLF monitored line, is treated as in the active state and the idle browser does not display.
Change causes system to restart or reboot.

**up.lineKeyCallTerminate**
Specifies whether or not you can press the line key to end an active call.
0 (Default) - User cannot end an active call by pressing the line key.
1 - User can press a line key to end an active call.

**up.numberFirstCID**
Specifies what is displayed first on the **Caller ID** display.
0 (Default) - **Caller ID** display shows the caller's name first.
1 - Caller's phone number is shown first.
Change causes system to restart or reboot.

**up.numOfDisplayColumns**
Sets the maximum number of columns on the display. Set the maximum number of columns that phones display. Range is 0 to 4.
3 (Default)
0 - Phones display one column.
Change causes system to restart or reboot.

**up.osdIncomingCall.Enabled**
Specifies whether or not to display full screen popup or OSD for incoming calls.

1 (Default) - Full screen popup or OSD for incoming calls displays.
0 - Full screen popup or OSD for incoming calls does not display.

**up.prioritizeBackgroundMenuItem.enabled**

User can choose whether or not the phone background should take priority over the idle browser.

1 (Default) - If `up.idleBrowser.enabled` is set to 1, this parameter can be set to 1 to display a Prioritize Background menu to the user.

Change causes system to restart or reboot.

**up.rebootSoundEnabled**

1 (default) – Enable a sound effect alert when the phone reboots.
0 – Disable a sound effect alert when the phone reboots.

**up.ringer.minimumVolume**

Configure the minimum ringer volume. This parameter defines how many volume steps are accessible below the maximum level by the user.

16 (Default) - Full 16 steps of volume range are accessible.
0 - Ring volume is not adjustable by the user and the phone uses maximum ring volume.

Example: Upon bootup, the volume is set to ½ the number of configured steps below the maximum (16). If the parameter is set to 8 on bootup, the ringer volume is set to 4 steps below maximum.

**up.screenSaver.enabled**

0 (Default) - Screen saver feature is disabled.

1 - Screen saver feature is enabled. If a USB flash drive containing images is connected to the phone, and the idle browser is not configured, a slide show cycles through the images from the USB flash drive when the screen saver feature is enabled.

The images must be stored in the directory on the flash drive specified by `up.pictureFrame.folder`. The screen saver displays when the phone has been in the idle state for the amount of time specified by `up.screenSaver.waitTime`.

**up.screenSaver.type**

Choose the type of screen saver to display.

0 (Default) - Phone screen saver displays default images.
2 - Phone screen saver displays the idle browser.

**up.screenSaver.waitTime**
Number of minutes that the phone waits in the idle state before the screen saver starts. Range is 1 to 9999 minutes.
15 (Default)

**up.simplifiedSipCallInfo**
1 (Default) - This displayed host name is trimmed for both incoming and outgoing calls and the protocol tag/information is not displayed for incoming and outgoing calls.
0 - The full host name displays and the protocol tag/information displays for incoming and outgoing calls.

**up.softkey.transferTypeOption.enabled**
1 - The user can change the transfer type from consultative to blind and vice versa using a soft key after the user has initiated a transfer, but before completing the call to the far end.
0 (default) - There is no option to change from consultative to blind and blind to consultative when the user is in dial prompt after pressing the Transfer soft key.

**up.status.message.flash.rate**
Controls the scroll rate of the status bar. Range is 2 to 8 seconds.
2 seconds (Default)

**up.showDID**
AllScreens (default) – Display the DID number on all the screens.
None – Disable DID number on phone.
LockedScreen – Display the DID number on the lock screen.
StatusScreen – Display the DID number on the Status screen/Idle screen.
IncomingOSD – Display the DID number on the incoming On Screen Display (OSD) screen.
LockedScreenIncomingOSD – Display the DID number on the lock and incoming OSD screen.
LockedAndStatusScreen – Display the DID number on the lock and Status/Idle screen.
StatusScreenIncomingOSD – Display the DID number on the incoming OSD and Status/Idle screen.

**up.volumeChangeTone.enabled**
1 (default) – The phone plays a tone when the user adjusts the ringer or call volume.
0 – The phone does not play a tone.
Zoom Rooms Base Profile: 0 (default)

**up.warningLevel**
Line keys block display of the background image. All warnings are listed in the **Warnings** menu.
0 (Default) - The phone’s warning icon and a pop-up message display on the phone for all warnings.

1 - Warning icon and pop-up messages are only shown for critical warnings.

2 - Phone displays a warning icon and no warning messages. For all the values, all warnings are listed in the **Warnings** menu.

Access to the **Warnings** menu varies by phone model.

Change causes system to restart or reboot.

**up.welcomeSoundEnabled**

1 (Default) - Welcome sound is enabled and played each time the phone reboots.

0 - Welcome sound is disabled.

To use a welcome sound you must enable the parameter **up.welcomeSoundEnabled** and specify a file in *saf.x*. The default UC Software welcome sound file is Welcome.wav.

Change causes system to restart or reboot.

**up.welcomeSoundOnWarmBootEnabled**

0 (Default) - Welcome sound is played when the phone powers on (cold boot), but not after it restarts or reboots (warm boot).

1 - Welcome sound plays each time the phone powers on, reboots, or restarts.

Change causes system to restart or reboot.

**up.display.showFullCallerID**

Phone displays the caller ID.

0 (default) – Phone displays the caller ID on the first line.

1 – Phone displays the caller ID on the second line.

**up.answerCall.listOrder**

Defines the order to answer a call upon pressing speaker button on the phone.

LIFO (default) - Last-In, First-Out.

FIFO - First-In, First-Out.

**Upgrade Parameters**

Specify the URL of a custom download server and the Polycom UC Software download server when you want the phone to check when to search for software upgrades.

**upgrade.custom.server.url**

The URL of a custom download server.
upgrade.plcm.server.url
The URL of the Polycom UC Software software download.

URL - http://downloads.polycom.com/voice/software/

Voice Parameters
Use the following parameters to configure phone audio.

voice.rxPacketFilter
Define a high-pass filter to improve sound intelligibility when the phone receives narrow band signals. Narrow band signals occur when a narrow band codec is in use, such as G.711mu, G.711A, G.729AB, iLBC, and some Opus and SILK variants.

0 (default) - Pass through.
1 - 300 Hz high-pass.
2 - 300 Hz high-pass with pre-emphasis. Use this value with G.729.

voice.txPacketDelay
Null (default)

normal, Null - Audio parameters are not changed.
low - If there are no precedence conflicts, the following changes are made:
voice.codecPref.G722="1" voice.codecPref.G711Mu="2"
voice.codecPref.G711A="3" voice.codecPref.<OtherCodecs>=""
voice.audioProfile.G722.payloadSize="10"
voice.audioProfile.G711Mu.payloadSize= "10"
voice.audioProfile.G711A.payloadSize= "10" voice.aec.hs.enable="0"
voice.ns.hs.enable="0"

Change causes system to restart or reboot.

voice.txPacketFilter
Null (default)

0 - Tx filtering is not performed.
1 - Enables Narrowband Tx high pass filter.

Change causes system to restart or reboot.
Acoustic Echo Suppression (AES) Parameter

Use this parameter to enable speakerphone acoustic echo suppression (AES).
This feature removes residual echo after AEC processing. Because AES depends on AEC, enable AES only when you also enable AEC using voice.aec.hd.enable.

voice.aes.hs.enable
1 (default) - Enables the handset AES function.
0 - Disables the handset AES function.

Comfort Noise Parameters

Use these parameters to configure the addition and volume of comfort noise during conferences.

voice.cn.hf.enable
0 (default) - Comfort noise not added.
1 - Adds comfort noise added into the Tx path for hands-free operation.
Far end users should use this feature when they find the phone to be 'dead', as the near end user stops talking.

voice.cn.hf.attn
35 (default) - quite loud
0 - 90
Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when voice.cn.hf.enabled is 1.

voice.cn.hd.attn
30 (default) - quite loud
0 - 90
Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when voice.cn.hd.enabled is 1.

voice.cn.hs.enable
0 (default) - Comfort noise is not added into the Tx path for the handset.
1 - Adds comfort noise is added into the Tx path for the headset.
Far end users should use this feature when they find the phone to be 'dead', as the near end user stops talking.

voice.cn.hs.attn
35 (default) - quite loud
0 - 90
Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when `voice.cn.hs.enabled` is 1.

**voice.vadRxGain**

Tunes VAD or CNG interoperability in a multi-vendor environment.

0 (default)

-20 to +20 dB

The specified gain value in dB is added to the noise level of an incoming VAD or CNG packet, when in a narrow band call.

When tuning in multi-vendor environments, the existing Poly to Poly phone behavior can be retained by setting `voice.vadTxGain = -voice.vadRxGain`.

This parameter is ignored for HD calls.

**voice.vadTxGain**

Tunes VAD or CNG interoperability in a multi-vendor environment.

0 (default)

-20 to +20 dB

The specified gain value in dB is added to the noise level of an incoming VAD or CNG packet, when in a narrow band call.

This causes the noise level to synthesize at the local phone to change by the specified amount.

When tuning in multi-vendor environments, the existing Poly to Poly phone behavior can be retained by setting `voice.vadTxGain = -voice.vadRxGain`.

This parameter is ignored for HD calls.

### Voice Jitter Buffer Parameters

Use the following parameters to configure wired network interface voice traffic and push-to-talk interface voice traffic.

**voice.rxQoS.avgJitter**

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

20 (default)

0 to 80

`avgJitter` The wired interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.

Change causes system to restart or reboot.

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

240 (default)

0 to 320

maxJitter The wired interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss.

Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss. If legacy voice.audioProfile.x.jitterBuffer.* parameters are explicitly specified, they will be used to configure the jitter buffer and these voice.rxQoS parameters will be ignored.

Change causes system to restart or reboot.

**voice.rxQoS.ptt.avgJitter**

The average jitter in milliseconds for IP multicast voice traffic.

150 (default)

0 - 200

avgJitter The PTT/Paging interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.

Change causes system to restart or reboot.

**voice.rxQoS.ptt.maxJitter**

The maximum jitter in milliseconds for IP multicast voice traffic.

480 (default)

20 - 500

maxJitter The PTT/Paging interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss.

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

If legacy voice.audioProfile.x.jitterBuffer.* parameters are explicitly specified, they will be used to configure the jitter buffer and these voice.rxQoS parameters will be ignored for PTT/Paging interface interfaces.

Change causes system to restart or reboot.

**voice.handsfreePtt.rxdg.offset**

This parameter allows a digital Rx boost for Push To Talk.

0 (default)

9 to -12 - Offsets the RxDg range of the hands-free and hands-free Push-to-Talk (PTT) by the specified number of decibels.
**voice.ringerPage.rxdg.offset**

This parameter allows a digital Rx boost for Push To Talk. Use this parameter for handsfree paging in high noise environments.

0 (default)

9 to -12 - Raise or lower the volume of the ringer and hands-free page by the specified number of decibels.

**Digital Gain Parameters**

The following parameters affect the gain applied to microphones.

**voice.handset.txdg**

Digital gain applied to the wired handset mic.

0 (Default)

-90 to 90

**voice.handsfree.txdg**

Digital gain applied to the built-in hands free mic.

0 (Default)

-90 to 90

**voice.headset.txdg**

Digital gain applied to the wired headset mic.

0 (Default)

-90 to 90

**voice.usb.headset.txdg**

Digital gain applied to the USB headset mic.

0 (Default)

-90 to 90

**voice.bt.headset.txdg**

Digital gain applied to the Bluetooth headset mic.

0 (Default)

-90 to 90
Session Description Protocol (SDP) Parameters

Use the following parameters to configure Session Description Protocol.

voIpProt.SDP.answer.useLocalPreferences

0 (default) - Attempt to match the negotiated voice and video codecs using the order in the SDP offer from the far end.

1- Answer SDP offers using the phone's local preferences for codec ordering instead of the preference order from the offer.

voIpProt.SDP.answer.useLocalPreferences.video

Allows you to reset the parameter voIpProt.SDP.answer.useLocalPreferences to the default 0 for audio only.

1 (default) - The phone uses its own preference list instead of the preference list in the offer when deciding which video codec to use.

0 - The phone’s use of its own preference list is disabled.

voIpProt.SDP.early.answerOrOffer

0 (default) - SDP offer or answer is not generated.

1 - SDP offer or answer is generated in a provisional reliable response and PRACK request and response.

Note: An SDP offer or answer is not generated if reg.x.musicOnHold.uri is set.

voIpProt.SDP.offer.iLBC.13_33kbps.includeMode

1 (default) - The phone should include the mode=30 FMTP parameter in SDP offers:
If voice.codecPref.iLBC.13_33kbps is set and voice.codecPref.iLBC.15_2kbps is Null.
If voice.codecPref.iLBC.13_33kbps and voice.codecPref.iLBC.15_2kbps are both set, the iLBC 13.33 kbps codec is set to a higher preference.
0 - the phone should not include the mode=30 FTMP parameter in SDP offers even if iLBC 13.33 kbps codec is being advertised.

voIpProt.SDP.useLegacyPayloadTypeNegotiation

0 (default) - RFC 3264 is followed for transmit and receive RTP payload type values.

1 - The phone transmits and receives RTP using the payload type identified by the first codec listed in the SDP of the codec negotiation answer.

voIpProt.SDP.offer.rtcpVideoCodecControl

This parameter determines whether or not RTCP-FB-based controls are offered in Session Description Protocol (SDP) when the phone negotiates video i-frame request methods. Even
when RTCP-FB-based controls are not offered in SDP, the phone may still send and receive RTCP-FB I-frame requests during calls depending on other parameter settings. For more information about video I-frame request behavior, refer to video.forceRtcpVideoCodecControl. For an account of all parameter dependencies refer to the I-Frames section.

0 - The phone does not include the SDP attribute "a=rtcp-fb".
1 (default) - The phone includes SDP attribute "a=rtcp-fb" into offers during outbound SIP calls.

### Web Configuration Utility Language File Download Parameter

The following parameter specifies the download location of the translated language files for the Web Configuration Utility.

**webutility.language.plcmServerUrl**

Specifies the download location of the translated language files for the Web Configuration Utility.

http://downloads.polycom.com/voice/software/languages/

(default) URL

### XML Streaming Protocol Parameters

Use the following parameters to set the XML streaming protocols for instant messaging, presence, and contact list for BroadSoft features.

**xmpp.1.auth.domain**

Specify the domain name of the XMPP server.

Null (Default)

Other values - UTF-8 encoded string

**xmpp.1.auth.useLoginCredentials**

Specifies whether or not to use the login credentials provided in the phone's Login Credentials Menu for XMPP authentication.

0 (Default)

1

**xmpp.1.enable**

Specifies to enable or disable the XMPP presence.
Session Headers

You can enable session header parameters to convey information between phones about the SIP message.

Session Header Parameters

Use the following parameters to configure session header components.

voIpProt.SIP.supportFor100rel

Poly recommends setting this parameter to 1 when using Poly Trio systems with Polycom RealPresence DMA systems.

1 (default) - The phone advertises support for reliable provisional responses in its offers and responses.

0 - The phone does not offer 100rel and rejects offers requiring 100rel.

voIpProt.SIP.keepalive.sessionTimers

0 (default) – The phone does not declare “timer” in “Support” header in an INVITE. The call does not get disconnected when the phone does not receive UPDATE packet. The phone still responds to a re-INVITE or UPDATE and follows session timer to send re-INVITE or UPDATE if the remote endpoint asks for it.

1 – The session timer is enabled and the call gets disconnected when the phone does not receive UPDATE packet within the specified session timer.

reg.x.keepalive.sessionTimers

1 (default) – The session timer is enabled and the call received on the registered line gets disconnected when the phone does not receive UPDATE packet within the specified timer.

0 – The session timer is disabled and the call received on the registered line does not get disconnected when the phone does not receive UPDATE packet.