



PVOS 8.0.1 | October 2022 | 3725-13771-002A

Poly Voice Software

Trio C60 Administrator Guide

Contents

Before You Begin	10
Audience, Purpose, and Required Skills	10
Related Poly and Partner Resources	10
Getting Started with Poly Trio C Series	11
PVOS Overview	11
Supported Phones and Accessories	11
Working with PVOS	11
PVOS Provisioning Methods	11
Certificates	13
Using the Factory-Installed Certificate	13
Check for a Device Certificate	13
Customizing Certificate Use	14
Determining TLS Platform Profiles or TLS Application Profiles	14
TLS Protocol Configuration for Supported Applications	17
TLS Parameters	19
Configurable TLS Cipher Suites	21
Create a Certificate Signing Request	22
Download Certificates	23
Custom URL Location for LDAP Server CA Certificate	23
Custom URL Location for LDAP Server Certificates Parameter	24
Confirm the Installed LDAP Server Certificates on the Phone	24
Online Certificate Status Protocol	24
Online Certificate Status Protocol Parameter	24
Supported Inbound and Outbound Ports	25
Inbound Ports for Poly Trio Systems	25
Outbound Ports for Poly Trio Systems	26
Audio Features	28
Automatic Gain Control	28
Background Noise Suppression	28
Comfort Noise	28
Voice Activity Detection	28
Voice Activity Detection Parameters	28
Comfort Noise Payload Packets	29
Comfort Noise Payload Packets Parameters	29
Synthesized Call Progress Tones	29
Jitter Buffer and Packet Error Concealment	29
DTMF Tones	29
DTMF Tone Parameters	30
Acoustic Echo Cancellation	31
Acoustic Echo Cancellation Parameters	31
Poly NoiseBlock	32
Poly NoiseBlock Parameter	32
Audio Input Options	32
USB Audio Calls	32
USB Audio Call Parameters	32
Location of Audio Alerts	33
Audio Alert Parameters	33
Ringtones	33
Supported Ring Classes	34
Ringtone Parameters	34
Sound Effects	35
Sampled Audio Files	35
Sampled Audio File Parameter	36
Sound Effect Patterns	36
Sound Effect Pattern Parameters	37

Supported Audio Codecs	39
Supported Audio Codec Specifications	39
Audio Codec Parameters	41
SILK Audio Codec Parameters	44
Opus Audio Codec Parameters	45
IEEE 802.1p/Q	47
IEEE 802.1p/Q Parameters	47
Voice Quality Monitoring (VQMon)	48
VQMon Reports	48
VQMon Parameters	48
Call Controls	52
Microphone Mute	52
Microphone Mute Parameters	52
Persistent Microphone Mute	52
Persistent Microphone Mute Parameter	52
Answer Incoming Calls with Mute Button	53
Answer Incoming Calls with Mute Button Parameter	53
Call Timers	53
Called Party Identification	53
Connected Party Identification	53
Calling Party Identification	53
Calling Party Identification Parameters	53
Remote Party Caller ID from SIP Messages	54
Remote Party Caller ID from SIP Messages Parameters	54
Calling Line Identification	54
Calling Line Identification Parameters	55
Enable and Configure STIR/SHAKEN Caller ID Validation	55
STIR/SHAKEN Caller ID Validation Parameters	56
SIP Header Warnings	57
SIP Header Warning Parameters	57
Distinctive Call Waiting	57
Distinctive Call Waiting Parameters	57
Do Not Disturb	58
Server-Based Do Not Disturb	58
Do Not Disturb Parameters	58
Remote Party Disconnect Alert Tone	59
Remote Party Disconnect Alert Tone Parameter	59
Call Waiting Alerts	59
Call Waiting Alert Parameters	59
Missed Call Notifications	60
Missed Call Notification Parameters	60
Call Hold	61
Call Hold Parameters	61
Hold Implementation	62
Call Transfer	62
Call Transfer Parameters	62
Call Forwarding	62
Call Forward on Shared Lines	63
Call Forwarding Parameters	63
Automatic Off-Hook Call Placement	66
Automatic Off-Hook Call Placement Parameters	66
Multiple Line Keys Per Registration	67
Multiple Line Keys Per Registration Parameter	67
Multiple Call Appearances	67
Multiple Call Appearance Parameters	67
Bridged Line Appearance	68
Bridged Line Appearance Signaling	68
Bridged Line Appearance Parameters	68
Voicemail	69

Voicemail Parameters	69
Local Call Recording	70
Local Call Recording Parameter	70
Local and Centralized Conference Calls on Poly Trio C60	70
Conference Management Parameter	71
Conference Meeting Dial-In Options	71
Conference Meeting Dial-In Options Parameters	71
Hybrid Line Registration	72
Hybrid Line Registration Limitations	73
Hybrid Line Registration Parameters	73
Configure Hybrid Line Registration Using the System Web Interface	74
Local Digit Map	74
Local Digit Maps Parameters	74
OpenSIP Digit Map	78
Generating Secondary Dial Tone with Digit Maps	79
Configure Poly Trio to Use Regular Expressions in Dial Plans	80
Enhanced 911 (E.911)	80
Enhanced 911 (E.911) Parameters	80
MLPP for AS-SIP	85
Preemption Behavior for Low Priority Calls	85
MLPP with AS-SIP Parameters	86
International Dialing Prefix	87
International Dialing Prefix Parameters	87
Switching Call Applications	88
Call Application Switching Parameters	88
Shared Lines	90
Shared Call Appearances	90
Shared Call Appearances Parameters	90
Private Hold on Shared Lines	102
Private Hold on Shared Lines Parameters	102
Intercom Calls	103
Creating a Custom Intercom Soft Key	103
Intercom Calls Parameters	103
Group Paging	104
Group Paging Parameters	104
Daisy-Chaining Poly Trio C60 Systems	107
Daisy-Chaining Requirements	107
Daisy-Chain Poly Trio Systems	107
Daisy-Chaining Parameters	107
Hardware and Power for Poly Trio C60 Systems	108
Powering the Poly Trio C60	108
Power the Poly Trio C60 System with the Optional Power Adapter	108
Poly Trio System Power Management	108
USB Port Power Management	109
Poly Trio System Power Management Parameters	109
Power-Saving on Poly Trio Systems	109
Power-Saving Parameters	109
Phone Display Features	111
Administrator Menu on Poly Trio Systems	111
Administrator Menu Parameters	111
Poly Trio System Display Name	112
Display Name Parameters	112
LED Indicators on Poly Trio System	113
LED Pattern Parameters	113
LED Indicator Pattern Types	113
Example: Turn Off the Message Waiting Indicator in Power Saving Mode	114
Poly Trio System Status Messages	114
Poly Trio System Status Message Parameters	114

Olson Time Zone Configuration	115
Olson Time Zone Parameters	115
Set an Olson Time Zone with the Web Configuration Utility	115
Set an Olson Time Zone from the Device Menu	116
Olson Time Zone IDs	116
Time Zone Location Description	119
Time Zone Location Parameters	119
Time and Date	122
Time and Date Display Parameters	123
Phone Languages	127
Change the Keyboard Layout	127
Phone Language Parameters	127
Multilingual Parameters	128
Access the Country of Operation Menu in Set Language	129
Add a Language for the Phone Display and Menu	129
Hide the MAC Address	130
Hide MAC Address Parameters	130
Unique Line Labels for Registration Lines	130
Unique Line Labels for Registration Lines Parameters	130
Poly Trio System Number Formatting	131
Poly Trio System Number Formatting Parameters	131
Number or Custom Label	131
Configure the Number or Label from the System	131
Number and Label Parameters	131
Custom Icons for Contacts and Line Registrations	132
Custom Icon Parameters	133
Example: Configure an Icon for a Line Registration	133
Example: Set Icons for Speed Dial Contacts	133
Capture Your Phone's Screen	134
Capture Current Phone Screen Parameters	134
Default In-Call Screen	134
Default In-Call Screen Parameters	135
Custom Call Control Options	135
Custom Call Control Options Parameters	135
Poly Trio Home Screen Parameters	136
LED Indicators	138
LED Indicator Pattern Types	138
Set an LED Pattern for Active Calls	138
Set an LED Pattern on BLF for Held Calls	139
Set an LED Pattern for Incoming Calls	139
Set an LED Pattern for Self-Parked Calls	139
Set an LED Pattern for Remote-Parked Calls	140
Configure LED Behavior for Held Calls on Shared Lines	140
Enable the LED Indicator for Incoming Calls	140
Enable the LED Indicator for Missed Calls on a Call Server	141
Disable in Power Saving Mode	141
Directories and Contacts	142
Local Contact Directory	142
Local Contact Directory Parameters	142
Maximum Capacity of the Local Contact Directory on Poly Trio	143
Creating Per-Phone Directory Files	143
Local Contact Directory File Size Parameters	144
Speed Dials on Poly Trio Systems	146
Speed Dial Contacts Parameters	146
Corporate Directory	147
Corporate Directory Parameters	147
Call Lists	152
Call List Parameters	153

Call Log Elements and Attributes	154
Resetting Contacts and Recent Calls Lists on Your Phone	155
Configuring Security Options	156
Administrator and User Passwords	156
Change the Administrator Password on the Phone Menu	156
Change the User Password on the System	156
Change the Administrator Password in the System Web Interface	157
Change the User Password in the System Web Interface	157
Administrator and User Password Parameters	157
California SB-327 Password Requirement Compliance	158
Disabling External Ports and Features	158
Disable Unused Ports and Features Parameters	158
Visual Security Classification	160
Visual Security Classification Parameters	160
Encryption	160
Encrypting Configuration Files	160
Configuration File Encryption Parameters	161
Voice over Secure IP	162
VoSIP Parameter	162
Securing Phone Calls with SRTP	162
SRTP Parameters	163
Enabling Users to Lock Phones	166
Phone Lock Parameters	166
Locking the Basic Settings Menu	167
Basic Settings Menu Lock Parameter	167
Secondary Port Link Status Report	168
Secondary Port Link Status Report Parameters	168
802.1X Authentication	169
802.1X Authentication Parameters	169
Simple Certificate Enrollment Protocol	170
Simple Certificate Enrollment Protocol Parameters	170
Session Management on the System Web Interface	173
Session Management Parameters	173
General Security Parameters	173
DHCP Parameter	174
DNS Parameters	174
TCP Keep-Alive Parameters	175
File Transfer Parameter	176
Network	177
System and Model Names	177
Two-Way Active Measurement Protocol	177
TWAMP Limitations	177
Two-Way Active Measurement Protocol Configuration Parameters	177
Incoming Network Signaling Validation	178
Network Signaling Validation Parameters	178
SIP Subscription Timers	178
SIP Subscription Timers Parameters	179
Enhanced IPv4 ICMP Management	179
IPv4 Parameters	179
Provisional Polling of Phones	180
Provisional Polling Parameters	180
SIP Instance Support	181
SIP Instance Parameter	181
IP Type-of-Service	182
IP Type-of-Service Parameters	182
Static DNS Cache	185
Configuring Static DNS	185
Example Static DNS Cache Configuration	192

DNS SIP Server Name Resolution	194
Customer Phone Configuration	195
For Outgoing Calls (INVITE Fallback)	195
Phone Operation for Registration	196
Recommended Practices for Fallback Deployments	197
Server Redundancy	197
Server Redundancy Parameters	197
Network Address Translation (NAT)	200
Network Address Translation Parameters	200
Real-Time Transport Protocol (RTP) Ports	201
RTP Ports Parameters	201
Wireless Network Connectivity (Wi-Fi)	202
Wi-Fi Parameters	203
Enable Wi-Fi	205
Configure Wireless Network Settings with EAP	205
Wi-Fi Settings in Basic Menu Parameter	206
Bluetooth for Poly Trio Systems	206
Bluetooth Parameters	206
Web Proxy	208
PAC File Search Priority	208
Supported HTTP/HTTPS Web Proxy Services	208
Configure Web Proxy Settings in the Local Interface	209
Configure Web Proxy Access Manually	209
Configure Proxy-Specific Credentials for Users	209
View Web Proxy Diagnostics on the System Web Interface	209
Web Proxy Configuration Parameters	209
User Profiles	211
User Profile Parameters	211
Remotely Logging Out Users	212
User Profile Authentication	213
User Profile Server Authentication	213
User Profile Phone Authentication	214
Third-Party Servers	216
Cisco BroadWorks Server	216
Authentication with Cisco BroadWorks XSP Service Interface	216
UC-One Integration	217
BroadSoft UC-One Directory Parameters	219
Anonymous Call Rejection	219
Simultaneous Ring	220
Line ID Blocking	220
BroadWorks Anywhere	221
Remote Office	221
BroadSoft UC-One Credentials	222
BroadSoft Server-Based Call Forwarding	223
Microsoft Exchange Integration	223
Integrating with Microsoft Exchange	223
Poly Trio Solution with Skype for Business	225
Private Meetings in Microsoft Exchange	225
Configuring the Microsoft Exchange Server	226
Join a Meeting with a SIP URI	231
Microsoft Exchange Advanced Login	232
Exchange Impersonation for Calendaring	233
Basic Authentication for One Touch Dial Exchange Services	234
Cisco Webex	234
Configure Direct Dial to Cisco Webex Meetings	234
Configuration Parameters	236
Quick Setup Soft Key Parameter	236
Per-Registration Call Parameters	236

Remote Packet Capture Parameters	239
Per-Registration Dial Plan Parameters	240
Local Contact Directory File Size Parameters	243
Parameter Elements for the Local Contact Directory	244
Feature Activation and Deactivation Parameters	245
HTTPD Web Server Parameters	247
Feature License Parameter	248
Chord Parameters	248
Message Waiting Parameters	249
Ethernet Interface MTU Parameters	250
Presence Parameters	250
Provisioning Parameters	251
Configuration Request Parameter	252
User Preferences Parameters	252
Upgrade Parameters	257
Voice Parameters	257
Acoustic Echo Suppression (AES) Parameter	258
Comfort Noise Parameters	258
Voice Jitter Buffer Parameters	259
Digital Gain Parameters	260
SDP Parameters	261
Download Location Parameter for Language Files	262
XML Streaming Protocol Parameters	262
Session Header Parameters	263
Device Parameters	264
Changing Device Parameters	264
Types of Device Parameters	264
Parameter List Conventions	265
Device Parameters	266
Device Parameters for Wi-Fi	276
Diagnostics and Status	280
View the Phone's Status	280
Upload a Phone's Configuration Files to Provisioning Server	281
Perform Network Diagnostics	281
Rebooting the Phone at a Scheduled Time	281
Scheduled Reboot Parameters	281
Resetting a Phone to Factory Defaults	282
Reset the Phone and Configuration	282
Factory Reset the Poly Trio System at Power-Up	282
Factory Reset the Poly Trio System from the Local Interface	283
Reset to Factory Configuration Parameters	283
Status Indicators on Poly Trio C60 Systems	283
Monitoring the Phone's Memory Usage	284
Check Memory Usage from the Phone	284
Viewing Memory Usage Errors in the Application Log	284
Phone Memory Resources	284
Poly Lens	285
Poly Lens Parameter	285
System Logs	287
Configuring Log Files	287
Severity of Logging Event Parameter	287
Log File Collection and Storage Parameters	287
Logging Levels	289
Logging Level, Change, and Render Parameters for Poly Trio	289
Logging Parameters	293
Upload Poly Trio System Logs	293
Uploading Logs to a USB Flash Drive	294
USB Logging Parameter	294

Upgrading the Software	295
Upgrade UC Software Using a USB Flash Drive	295
Upgrading the Software on a Single Phone	295
User-Controlled Software Update	295
User-Controlled Software Update Parameters	296
Updating UC Software with Windows Device Manager	296
Configure Windows to Update UC Software via Device Manager	296
Update UC Software Using a Windows Computer	297
Disable UC Software Updates through Windows	297
Troubleshooting	298
Updater Error Messages and Possible Solutions	298
UC Software Error Messages	298
Network Authentication Failure Error Codes	299
Power and Start-Up Issues	300
Screen and System Access Issues	301
Calling Issues	301
Display Issues	302
Software Upgrade Issues	303

Before You Begin

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

- Poly Trio C60

Audience, Purpose, and Required Skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

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

Related Poly and Partner Resources

See the following sites for information related to this product.

- [Poly Support](#) is the entry point to online product, service, and solution support information. Find product-specific information such as Knowledge Base articles, Support Videos, Guide & Manuals, and Software Releases on the Products page, download software for desktop and mobile platforms from Downloads & Apps, and access additional services.
- The [Poly Documentation Library](#) provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The [Poly Community](#) provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The [Poly Partner Network](#) is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- [Poly Services](#) help your business succeed and get the most out of your investment through the benefits of collaboration. Enhance collaboration for your employees by accessing Poly service solutions, including Support Services, Managed Services, Professional Services, and Training Services.
- With [Poly+](#) you get exclusive premium features, insights and management tools necessary to keep employee devices up, running, and ready for action.
- [Poly Lens](#) enables better collaboration for every user in every workspace. It is designed to spotlight the health and efficiency of your spaces and devices by providing actionable insights and simplifying device management.

Getting Started with Poly Trio C Series

Understand Poly UC software features and review methods to configure your phones..

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

PVOS Overview

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

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

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

Supported Phones and Accessories

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

Product Name, Model Name, and Part Number

Product Name	Model Name	Part Number
Poly Trio C60	Poly TrioC60	3111-86240-001

Working with PVOS

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.

PVOS Provisioning Methods

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

You can use multiple methods simultaneously to provision and configure features. There is a priority among the methods that impacts your phone deployment when you use multiple methods simultaneously. If there is a discrepancy among multiple provisioning methods or configuration settings, the Poly phone uses the setting set with the higher-priority method based on the following hierarchy:

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

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

For more information on provisioning phones, see the Poly Trio Solution Provisioning Guide.

Certificates

Use security certificates when deploying a solution to ensure the integrity and privacy of communications involving Poly devices.

Poly phones come with an authenticated, built-in device certificate. 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 the type of device certificate used for each secure communication option. By default, all operations use the factory-installed device certificate unless you specify otherwise.

Note: You can install custom device certificates on your phones in the same way you install custom CA certificates. For more information, see *Technical Bulletin 17877: Using Custom Certificates With Polycom Phones* at [Poly Support](#).

Your phone uses certificates in the following situations:

- Mutual TLS authentication - The server can verify that a device is truly a Poly device and not a malicious endpoint or software masquerading as a Poly device.
Use this option for provisioning or SIP signaling using TLS signaling. For example, certain partner provisioning systems and Polycom Zero Touch Provisioning (ZTP) use mutual TLS.
- Secure HTTP (HTTPS) - Access to the web server on the phone at `https://<IP ADDRESS OF PHONE>`.
The phone uses the web server for certain configuration and troubleshooting activities.
- Polycom applications API - Provides secure communications.

You can configure the following options for two platform device certificates and six application device certificates on the phone:

- 802.1X authentication
- Provisioning
- Syslog
- SIP signaling
- Browser communications
- Presence
- LDAP

Note: You must apply platform device certificates for syslog, 802.1X, and provisioning using TLS platform profiles, but you can't use TLS application profiles to applied certificates for those options.

Using the Factory-Installed Certificate

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

You can use the factory-installed certificate for all your security needs. The certificate is signed by the Poly Certificate Authority (CA), so to configure your web servers and/or clients to trust the factory-installed certificates, you must download the Poly Root CA certificate 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 Poly Root CA—is part of the Poly 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.

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

You can check if your phone has a factory-installed certificate. The certificate and associated private key are stored on the phone in its non-volatile memory as part of the manufacturing process.

Task

1 Go to **Settings > Advanced > Administration Settings > TLS Security > Custom Device Credentials**.

2 Choose a credential and select **Info** to view the certificate.

One of the following messages displays:

- **Installed** or **Factory Installed** - The certificate is available in flash memory, all the certificate fields are valid, and the certificate isn't expired.
- **Not Installed** - The certificate isn't available in flash memory or the flash memory location that stores the device certificate is blank.
- **Invalid** - The certificate isn't 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, or 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*.

TLS Platform Profile and Application Profile Parameters

By default, all preinstalled 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.

TLSv1_0 (default)

SSLv2v3

TLSv1_1

TLSv1_2

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 for the phone's web server.

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
TLSv1_2

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/>.

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/>

NoCipher (default)

String

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.

PlatformProfile1 (default)

PlatformProfile1 or PlatformProfile2

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.

TLS Cipher Suites

Cipher	Cipher Suite
ADH	ADH-RC4-MD5, ADH-DES-CBC-SHA, ADH-DES-CBC3-SHA, ADH-AES128-SHA, ADH-AES256-SHA
AES128	AES128-SHA
AES256	AES256-SHA
DES	DES-CBC-SHA, DES-CBC3-SHA
DHE	DHE-DSS-AES128-SHA, DHE-DSS-AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA
EXP	EXP-RC4-MD5, EXP-DES-CBC-SH, EXP-EDH-DSS-DES-CBC-SHA, EXP-DES-CBC-SHA, EXP-ADH-RC4-MD5, EXP-ADH-DES-CBC-SHA, EXP-EDH-RSA-DES-CBC-SHA
EDH	EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC3-SHA, EDH-DSS-CBC-SHA
NULL	NULL-MD5, NULL-SHA
RC4	RC4-MD5, RC4-SHA

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:!DH:!AECDH:!PSK:!SRP:!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

Generate a certificate signing request directly from your device.

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

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

Task

- 1 Go to **Settings > Advanced > Admin Settings > Generate CSR**.
- 2 When prompted, enter the administrative password and press **Enter**.
- 3 Enter the following information:
 - Common Name
 - Organization (optional)
 - Email Address (optional)
 - Country (optional)
 - State (optional)
- 4 Select **Generate**.
A CSR generation completed message displays. The `MAC.csr` (certificate request) and `MAC-private.pem` (private key) files upload 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 must forward the CSR to a security 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 local interface
- Through the system web interface

Task

- 1 Go 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. Note that the system can't accept chevrons (<, >) in the URL field.
For example, `http://bootserver1.polycom.com/ca.crt`.

The certificate downloads, and the certificate's MD5 fingerprint displays to verify that you are installing the correct certificate.
- 4 Select **Accept**.
The certificate installs successfully.

Custom URL Location for LDAP Server CA Certificate

You can set the URL from where Polycom phones can 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 Polycom phone. The certificates are installed in descending order starting with the Application CA 7 slot and continues to Application CA 1 slot depending on how many certificates are in the chain.

Note: If the custom application CA certificate slots already have CA certificates installed on your Polycom phones, downloading LDAP server CA certificates will overwrite any existing certificates on the phone in descending order starting with the seventh certificate.

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 parameters `dir.corp.address` and `feature.corporateDirectory.enabled` as well, the certificates are automatically updated on the phones. You can confirm that the correct certificates were downloaded and installed on the phone.

Task

- 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 retrieves 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

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

0 (default) OCSP is disabled.

1 - OCSP is enabled

Change causes system to restart or reboot.

Supported Inbound and Outbound Ports

You can configure the inbound and outbound ports on Poly Trio C60 systems.

Inbound Ports for Poly Trio Systems

The following table lists the inbound IP ports currently used on all Poly Trio C60 systems, except where noted.

Inbound IP Port Connections to Poly Trio C60 Systems

Inbound Port	Type	Protocol	Function	Default	Configurable Port Number?
80	Static	TCP	HTTP Pull web interface, HTTP Push	Off	Yes
443	Static	TCP	HTTP Pull web interface, HTTP Push	On	Yes
10010	Static	TLS 1.2	Synchronize daisy-chained Poly Trio systems	On	No
1024 to 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 to 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes
1719	Static	UDP	H.225.0 RAS	Off	No
1720	Static	TCP	H.225.0 Call Signaling	On	No
2000	static	UDP	Multicast pairing		
2222	Dynamic (2222 to 2269)	TCP/UDP	RTP media packets	On	Yes tcplpApp.port.rtp.mediaPort RangeStart
2223	Dynamic (2222 to 2269)	TCP/UDP	RTCP media packets statistics	On	Yes tcplpApp.port.rtp.mediaPort RangeStart
5001	Static	TCP	People+Content IP	On	No
5060	Static	TCP/UDP	SIP signaling	On	No
5061	Static	TLS	SIP over TLS signaling	On	No
8001	Static	TCP	HTTPS for modular room provisioning	On	Yes mr.deviceMgmt.port
8150 to 8153	Static	TCP	Airplay audio control	On	No
8150 to 8153	Static	UDP	Airplay audio data	On	No

Outbound Ports for Poly Trio Systems

The following table lists the outbound IP ports currently used by UC Software running on Poly Trio C60 systems.

Outbound IP Port Connections to Poly Trio C60 Systems

Outbound Port	Type	Protocol	Function	Default	Configurable Port Number
21	Static	TCP	FTP provisioning Logs	On	No
22	Static	TCP	SSH	On	No
53	Static	UDP	DNS	On	No
67	Static	UDP	DHCP server	On	No
68	Static	UDP	DHCP client		No
69	Static	UDP	TFTP provisioning Logs		No
80	Static	TCP	HTTP Provisioning Logs System web interface		No
123	Static	UDP	NTP time server		No
389	Static	TCP/UDP	LDAP directory query		No
443	Static	TCP	HTTPS provisioning Logs System web interface		No
514	Static	UDP	SYSLOG		No
636	Static	TCP/UDP	LDAP directory query		No
10010	Static	TLS 1.2	Synchronize daisy-chained Poly Trio systems	On	No
1024 to 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 to 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes
1719	Static	UDP	H.225.0 RAS	Off	No

Outbound Port	Type	Protocol	Function	Default	Configurable Port Number
1720	Static	TCP	H.225.0 Call Signaling	On	No
2222	Dynamic (2222 to 2269)	TCP/UDP	RTP media packets	On	Yes tcpIpApp.port.rtp.mediaPort RangeStart
2223	Dynamic (2222 to 2269)	TCP/UDP	RTCP media packets statistics	On	Yes tcpIpApp.port.rtp.mediaPort RangeStart
5060		TCP/UDP	SIP signaling	On	
5061		TCP	SIP over TLS signaling	On	
5222	Static	TCP	RealPresence Resource Manager: XMPP	Off	No
8001	Static	TCP	HTTPS for modular room provisioning	On	Yes mr.deviceMgmt.port
8150 to 8153	Static	TCP	Airplay audio control	On	No

Audio Features

After you set up your phones on the network, users can send and receive calls using the default configuration. You can configure modifications that optimize the audio quality of your network.

Poly phones support audio sound quality features and options you can configure to optimize the conditions of your organization's phone network system.

Automatic Gain Control

Automatic Gain Control (AGC) boosts the gain of the near-end conference participants and helps conference participants hear your voice.

Note: This feature is enabled by default and you can't disable it.

Background Noise Suppression

Background noise suppression reduces the background noise caused by items such as fans, projectors, and air conditioners.

Note: This feature is enabled by default and you can't disable it.

Comfort Noise

Comfort Noise ensures a consistent background noise level to provide a natural call experience.

Note: Comfort Noise fill isn't related to Comfort Noise packets the phone generates when you enable Voice Activity Detection.

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

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).

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).

voice.vadEnable

0 (Default) - 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.

15 (default)

Integer from 0 - 30

Comfort Noise Payload Packets

Comfort noise is enabled by default on Poly phones, and the payload type is negotiated in Session Description Protocol (SDP) with a default of 13 for 8 KHz codecs or 122 for 16 KHz codecs or higher.

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 – 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 (default) – 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

Poly 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 your phone's call progress tones to match the standard tones in your region, contact [Technical Support](#).

Jitter Buffer and Packet Error Concealment

Poly phones employ 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.

DTMF Tones

Poly phones generate dual-tone multi-frequency (DTMF) tones, also called touch tones, in response to user dialing on the dialpad. Your phone transmits these tones in the real-time transport protocol (RTP) streams of connected calls.

Your 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.

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.

50 (default)

1 - 65535

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

Acoustic Echo Cancellation (AEC) enables the phones to significantly reduce echo while permitting natural communication. Configure your phones to use advanced AEC for hands-free operation using the speakerphone.

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 hands-free options.
 - 0 - Disables the AEC function for hands-free options.
- Poly doesn't 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.

Poly NoiseBlock

Poly NoiseBlock technology works to suppress and eliminate unwanted background noise that can reduce call quality.

NoiseBlock automatically mutes the microphone when a user stops speaking. NoiseBlockAI can suppress background noise while a call participant actively speaks. Both systems work to reduce interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter. Call recipients hear only the intended speaker's voice.

Poly NoiseBlock Parameter

Use the following parameter to configure NoiseBlock:

voice.ns.hf.block

- 1 - Enables NoiseBlock. The system automatically mutes the microphones when it detects that the user has stopped speaking. When it detects that the user starts speaking again, the microphones unmute.
- 2 (default) - Enables NoiseBlockAI. The system works to mute unwanted background noise while users speak.
- 0 - Disables both NoiseBlock and NoiseBlock AI.

Audio Input Options

Poly Trio C60 systems can use the following microphones in addition to internal microphones:

- Expansion Microphones
The expansion microphones include a 2.1 m | 7 ft cable that you can attach directly to the system to broaden its audio range to a total of 70 ft.
- Polycom Microphone Array

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 latest software versions when connected by USB and used as an audio speakerphone.

USB Audio Call Parameters

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

device.baseProfile

- NULL (default)

Generic - Disables the Skype for Business graphic interface.

Lync - Use this Base Profile for Skype for Business deployments.

Location of Audio Alerts

You can choose where all audio alerts, including incoming call alerts, are played on the 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.

se.touchFeedback.enabled

Play sound effect when certain buttons are pressed, like microphone mute.

0 (default) - Does not play an alert tone when the mute status is changed.

1 - An alert tone is played when the mute status is changed.

call.mute.reminder.period

The time interval in seconds to play an alert tone periodically when the phone is in the mute state. The parameter `se.touchFeedback.enabled` must be set to 1 in order for this behavior to be applied.

Null (default) - No reminder tone is played.

5-3600

Ringtones

Use ringtones to define a simple ring class that the phone applies based on credentials carried within the network protocol.

The ring class includes parameters such as call-waiting and ringer index (if appropriate), and it can use one of the following ring types:

- Ring - Plays a specified ring pattern or call waiting indication.
- Visual - Provides a visual indication (no audio) of an incoming call. You don't need to specify a ringer.
- 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 are no other calls in progress on the phone, including 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

Ring classes help you define which ringtone to play for certain function notifications.

The phones support 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

Use the following parameters to 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 Supported Ring Classes.

callWaiting (default)

callWaitingLong

precedenceCallWaiting

se.rt.<ringClass>.name

The answer mode for a ringtone, which is used to identify the ringtone in the user interface.

UTF-8 encoded string

0-127 characters

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

Set the answer mode for a ringtone.

ring

visual

answer

ring-answer

Sound Effects

The phone uses built-in sampled audio files (SAF) in .wav format for some sound effects.

You can customize the audio sound effects that play for incoming calls and other alerts. Use synthesized tones or sampled audio files with .wav files that you download from the provisioning server or internet.

Ringtone files are stored in volatile memory which allows a maximum size of 600 KB (614400 B) for all ringtones.

Sampled Audio Files

The phones use built-in sampled audio files (SAF) in .wav file format for some sound effects.

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 sampled audio files.

Default Sample Audio File Usage

Sampled Audio File Number	Default Use (Pattern Reference)
1	Ringer 12 (se.pat.misc.welcome) Ringer 15 (se.pat.ringer.ringer15)
2	Ringer 16 (se.pat.ringer.ringer16)
3	Ringer 17 (se.pat.ringer.ringer17)
4	Ringer 18 (se.pat.ringer.ringer18)
5	Ringer 19 (se.pat.ringer.ringer19)
6	Ringer 20 (se.pat.ringer.ringer20)
7	Ringer 21 (se.pat.ringer.ringer21)
8	Ringer 22 (se.pat.ringer.ringer22)
9	Ringer 23 (se.pat.ringer.ringer23)
10	Ringer 24 (se.pat.ringer.ringer24)
11 to 24	Not Used

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 Welcome sound file is `Welcome.wav`.

Null (default) – The phone uses a built-in file.

Path Name – During start-up, the phone attempts to download the file at the specified path in the provisioning server.

URL – During start-up, 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 Instruction Types

Instruction	Meaning	Example
sampled (n)	Play sampled audio file n	<pre>se.pat.misc.SAMPLED_1.inst.1.type = "sampled" (sampled audio file instruction type) se.pat.misc.SAMPLED_1.inst.1.value = "2" (specifies sampled audio file 2)</pre>
chord (n, d)	Play chord set n (d is optional and allows the chord set ON duration to be overridden to d milliseconds)	<pre>se.pat.callProg.busyTone.inst.2.type = "chord" (chord set instruction type) se.pat.callProg.busyTone.inst.2.value = "busyTone" (specifies sampled audio file busyTone) se.pat.callProg.busyTone.inst.2.param = "2000" (override ON duration of chord set to 2000 milliseconds)</pre>
silence (d)	Play silence for d milliseconds (Rx audio is not muted)	<pre>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)</pre>
branch (n)	Advance n instructions and execute that instruction (n must be negative and must not branch beyond the first instruction)	<pre>se.pat.callProg.alerting.inst.4.type = "branch" (branch instruction type) se.pat.callProg.alerting.inst.4.value = "-2" (step back 2 instructions and execute that instruction)</pre>

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.<cat>.x.inst.y.type

Sound effects name, where `<cat>` is `callProg`, `ringer`, or `misc`.

sample

chord

silence

branch

se.pat.<cat>.x.inst.y.value

sampled – Sampled audio file number

chord – Type of sound effect

silence – Silence duration in milliseconds

branch – Number of instructions to advance

String

Call Progress Tones

The following table lists the call progress pattern names and their descriptions.

Call Progress Tone Pattern Names

Call Progress Pattern	Description
alerting	Alerting
bargeln	Barge-in tone
busyTone	Busy tone
callWaiting	Call waiting tone
callWaitingLong	Call waiting tone long (distinctive)
confirmation	Confirmation tone
dialTone	Dial tone
howler	Howler tone (off-hook warning)
intercom	Intercom announcement tone
msgWaiting	Message waiting tone
precedenceCallWaiting	Precedence call waiting tone
precedenceRingback	Precedence ringback tone
preemption	Preemption tone
precedence	Precedence tone
recWarning	Record warning
reorder	Reorder tone
ringback	Ringback tone
secondaryDialTone	Secondary dial tone
stutter	Stuttered dial tone

Miscellaneous Patterns

The following table lists the miscellaneous patterns and their descriptions.

Miscellaneous Pattern Names

Parameter Name	Miscellaneous Pattern Name	Description
instantmessage	instant message	New instant message
localHoldNotification	local hold notification	Local hold notification
messageWaiting	message waiting	New message waiting indication
negativeConfirm	negative confirmation	Negative confirmation
positiveConfirm	positive confirmation	Positive confirmation
remoteHoldNotification	remote hold notification	Remote hold notification
welcome	welcome	Welcome (boot up)
callParkBLFReminderTone	call Park BLF Reminder Tone	Cadence of call park reminder tone
callParkBLFAudioNotification	call Park BLF Audio Notification	Cadence of call park audio notification

Supported Audio Codecs

The following table includes the supported audio codecs and priorities for Poly Trio C60 systems.

Note: The Opus codec isn't compatible with G.729 and iLBC. If you set Opus to the highest priority, G.729 and iLBC don't publish; if you set G.729 and iLBC to the highest priority, Opus doesn't not publish.

Audio Codec Priority

Supported Audio Codecs	Priority
G.711 μ -law	6
G.711 a-law	7
G.722	4
G.719 (64 Kbps)	0
G.722.1 (32 Kbps)	5
G.722.1C (48 Kbps)	2
G.729AB	8
Opus	0
iLBC (13.33 Kbps, 15.2 Kbps)	0,0
Siren 7	0
SILK	0

Supported Audio Codec Specifications

The following table summarizes the specifications for audio codecs supported on Poly Trio C60 systems.

Note: The network bandwidth necessary to send encoded voice is typically 5% to 10% higher than the encoded bit rate due to packetization overhead. For example, a G.722.1C call at 48 Kbps consumes about 100 Kbps of network bandwidth for both the receive and transmit signals (two-way audio).

Audio Codec Specifications

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
All systems	G.711 μ -law	RFC 1890	64 Kbps	80 Kbps	8 ksps	20 ms	3.5 kHz
All systems	G.711 a-law	RFC 1890	64 Kbps	80 Kbps	8 ksps	20 ms	3.5 kHz
All systems	G.719	RFC 5404	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 ksps	20 ms	20 kHz
All systems	G.711	RFC 1890	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722 Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16 ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.	RFC 3551	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1	RFC 3047	24 Kbps 32 Kbps	40 Kbps 48 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 ksps	20 ms	14 kHz
All systems	G.729AB	RFC 1890	8 Kbps	24 Kbps	8 ksps	20 ms	3.5 kHz

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
All systems	Opus	RFC 6716	8 to 24 Kbps	24 to 40 Kbps	8 ksps 16 ksps	20 ms	3.5 kHz 7 kHz
All systems	Lin16	RFC 1890	128 Kbps 256 Kbps 512 Kbps 705.6 Kbps 768 Kbps	132 Kbps 260 Kbps 516 Kbps 709.6 Kbps 772 Kbps	8 ksps 16 ksps 32 ksps 44.1 ksps 48 ksps	10 ms	3.5 kHz 7 kHz 14 kHz 20 kHz 22 kHz
All systems	Siren 7	SIREN7	16 Kbps 24 Kbps 32 Kbps	32 Kbps 40 Kbps 48 Kbps	16 ksps	20 ms	7 kHz
All systems	Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 ksps	20 ms	14 kHz
All systems	Siren22	SIREN22	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 ksps	20 ms	22 kHz
All systems	iLBC	RFC 3951	13.33 Kbps 15.2 Kbps	31.2 Kbps 24 Kbps	8 ksps	30 ms 20 ms	3.5 kHz
All systems	SILK	SILK	6 to 20 Kbps 7 to 25 Kbps 8 to 30 Kbps 12 to 40 Kbps	36 Kbps 41 Kbps 46 Kbps 56 Kbps	8 ksps 12 ksps 16 ksps 24 ksps	20 ms	3.5 kHz 5.2 kHz 7 kHz 11 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 - 35
- A value of 1 is the highest priority, 35 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.

voice.codecPref.G711_A

7 (default)

voice.codecPref.G711_Mu

6 (default)

voice.codecPref.G719.32kbps

0 (default)

voice.codecPref.G719.48kbps

0 (default)

voice.codecPref.G719.64kbps

0 (default)

voice.codecPref.G722

4 (default)

voice.codecPref.G7221.16kbps

0 (default)

voice.codecPref.G7221.24kbps

0 (default)

voice.codecPref.G7221_C.24kbps

0 (default)

voice.codecPref.G7221.32kbps

5 (default)

voice.codecPref.G7221_C.32kbps

0 (default)

voice.codecPref.G7221_C.48kbps

2 (default)

voice.codecPref.G729_AB

8 (default)

voice.codecPref.iLBC.13_33kbps

0 (default)

voice.codecPref.iLBC.15_2kbps

0 (default)

voice.codecPref.Lin16.8ksps

0 (default)

voice.codecPref.Lin16.16ksps

0 (default)

voice.codecPref.Lin16.32ksps

0 (default)

voice.codecPref.Lin16.44_1ksps

0 (default)

voice.codecPref.Lin16.48ksps

0 (default)

voice.codecPref.Siren7.16kbps

0 (default)

voice.codecPref.Siren7.24kbps

0 (default)

voice.codecPref.Siren7.32kbps

0 (default)

voice.codecPref.Siren14.24kbps

0 (default)

voice.codecPref.Siren14.32kbps

0 (default)

voice.codecPref.Siren14.48kbps

3 (default)

voice.codecPref.Siren22.32kbps

0 (default)

voice.codecPref.Siren22.48kbps

0 (default)

voice.codecPref.Siren22.64kbps

1 (default)

voice.codecPref.SILK.8ksps

0 (default)

voice.codecPref.SILK.12ksps

0 (default)

voice.codecPref.SILK.16ksps

0 (default)

voice.codecPref.SILK.24ksps

0 (default)

SILK Audio Codec Parameters

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) 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) 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) for the supported SILK sample rate.

30 kbps (default)

8 – 30 kbps

voice.audioProfile.SILK.24ksps.encMaxAvgBitrateKbps

Set the maximum average encoder output bitrate in kilobits per second (kbps) for the supported SILK sample rate.

40 kbps (default)

12 to 40 kbps

voice.audioProfile.SILK.encComplexity

Specify the SILK encoder complexity. The higher the number the more complex the encoding allowed.

2 (default)

0 to 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 to 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)

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.

2 (Default)

0 - 7

qos.ethernet.rtp.video.user_priority

Set user-priority used for Video RTP packets.

5 (Default)

0 - 7

qos.ethernet.rtp.user_priority

Choose the priority of voice Real-Time Protocol (RTP) packets.

5 (Default)

0 - 7

qos.ethernet.callControl.user_priority

Set the user-priority used for call control packets.

5 (Default)

0 - 7

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.

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 seconds

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)

TCPpreferred

UDPOnly

TLS

TCPOnly

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 or identifier for the phone, for the purposes of aggregation for the local endpoint.. If you do not configure a location value, you must use the default string 'Unknown'.

The phone sends this information in the SIP PUBLISH message, in the "LocalGroup" attribute of the voice quality session report. This parameter is only used when `voice.qualityMonitoring.rfc6035.enable="1"`

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.

Call Controls

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 (default) - 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.

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 Timers

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 can't configure the call timer display.

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.

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.

call.callsPerLineKey

Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines.

Note: The per-registration parameter `reg.x.callsPerLineKey` overrides this parameter.

12 (default)

1 - 12

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

Enable and Configure STIR/SHAKEN Caller ID Validation

Configure STIR/SHAKEN standard protocol values for caller ID validation on a registered line.

Note: By default, if the incoming call signaling has both P-Asserted-Identity and From headers, the phone will check the P-Asserted-Identity header. If the P-Asserted-Identity header does not include the caller validation parameter, the phone will not display the caller verification icon, even if the caller validation parameter is included in the From header.

Task

- 1 Open the configuration file.
- 2 Enable STIR/SHAKEN caller ID validation on a registered line. Replace x with the registered line number.

```
reg.x.SIP.stirshakenCallerVerification.enabled="1"
```

- 3 Configure the header parameter that the phone parses for caller ID validation. The default is verstat. Replace x with the registered line number. The maximum string length is 64 characters.

```
reg.x.SIP.stirshaken.attestationName="<string>"
```

- 4 Enter every possible attestation value the phone can receive from your service provider as a comma-separated list with no spaces. Replace x with the registered line number.

The default value is TN-VALIDATION-PASSED, TN-VALIDATION-PASSED-A, TN-VALIDATION-PASSED-B, TN-VALIDATION-PASSED-C, NO-TN-VALIDATION, TN-VALIDATION-FAILED.

```
reg.x.SIP.stirshaken.attestationValue="<attestation value(s)>"
```

- 5 Enter a subset of the attestation values in reg.x.SIP.stirshaken.attestationValue that pass validation as a comma-separated list with no spaces. Replace x with the registered line number.

The default value is TN-VALIDATION-PASSED, TN-VALIDATION-PASSED-A, TN-VALIDATION-PASSED-B.

```
reg.x.SIP.stirshaken.verstatPassed="<attestation value(s)>"
```

- 6 Enter a subset of the values in reg.x.SIP.stirshaken.attestationValue that fail validation as a comma-separated list with no spaces. Replace x with the registered line number.

The default value is TN-VALIDATION-PASSED-C, TN-VALIDATION-FAILED.

```
reg.x.SIP.stirshaken.verstatFailed="<attestation value(s)>"
```

- 7 Enter a subset of the values in reg.x.SIP.stirshaken.attestationValue that the phone doesn't validate as a comma-separated list with no spaces. Replace x with the registered line number.

The default value is NO-TN-VALIDATION.

```
reg.x.SIP.stirshaken.verstatNotAvailable="<attestation value(s)>"
```

- 8 Save the configuration file.

STIR/SHAKEN Caller ID Validation Parameters

Use the following parameters to configure the STIR/SHAKEN caller ID validation.

reg.x.SIP.stirshakenCallerVerification.enabled

0 (default) - Disabled.

1 - Enables caller ID validation based on STIR/SHAKEN.

reg.x.SIP.stirshaken.attestationName

String - PAI header parameter name that's parsed for caller ID validation.

verstat (default)

0-64 characters

reg.x.SIP.stirshaken.attestationValue

A list of all the possible caller ID attestation values. Values are comma separated with no spaces.

TN-VALIDATION-PASSED, TN-VALIDATION-PASSED-A, TN-VALIDATION-PASSED-B, TN-VALIDATION-PASSED-C, NO-TN-VALIDATION, TN-VALIDATION-FAILED (default)

0-256 characters

reg.x.SIP.stirshaken.verstatPassed

A subset of the values listed in reg.x.SIP.stirshaken.attestationValue that pass validation.

TN-VALIDATION-PASSED, TN-VALIDATION-PASSED-A, TN-VALIDATION-PASSED-B (default)

0-256 characters

reg.x.SIP.stirshaken.verstatNotAvailable

A subset of the values listed in `reg.x.SIP.stirshaken.attestationValue` that don't need validation.

NO-TN-VALIDATION (default)

0-256 characters

reg.x.SIP.stirshaken.verstatFailed

A subset of the values listed in `reg.x.SIP.stirshaken.attestationValue` that fail validation.

TN-VALIDATION-PASSED-C,TN-VALIDATION-FAILED (default)

0-256 characters

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.

voIpProt.SIP.header.warning.enable

0 (default) - The warning header is not displayed.

1 - The warning header is displayed if received.

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:

`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. 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 when the phone is already on a call.

voIpProt.SIP.alertInfo.x.class

Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE.

NULL (default)

voIpProt.SIP.alertInfo.x.value

Alert-Info fields from INVITE requests are compared as many of these parameters as are specified (x=1, 2, ...,22) and if a match is found, the behavior described in the corresponding ring class is applied.

default (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.

Change causes system to restart or reboot.

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.

call.shared.displayAlertWhenDnd

When the phone is set to Do Not Disturb (DND) mode, users can disable visual call notifications for incoming intercom calls using this parameter.

0 - Disable call notifications.

1 (default) - Enable call notifications.

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. 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.

In the following parameters, replace x with the line registration index.

call.missedCallTracking.x.enabled

1 (default) - Missed call tracking for a specific registration is enabled.

0 - The missed call counter doesn't update regardless of how you configure `call.serverMissedCalls.x.enabled` or the server. The missed call list doesn't display in the phone menu.

If `call.missedCallTracking.x.enabled="1"` and `call.serverMissedCalls.x.enabled="0"`, then the number of missed calls increments regardless of how you configure the server.

If `call.missedCallTracking.x.enabled="1"` and `call.serverMissedCalls.x.enabled="1"`, then the handling of missed calls depends on how you configure the server.

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 increment the counter.

Note: This feature is supported only with the BroadSoft Synergy call server (previously known as Sylanro).

Change causes system to restart or reboot.

call.serverMissedCall.led

0 (default) - The LED doesn't flash if there is a missed call on the call server.

1 - The LED flashes when there is a missed call on the call server.

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

Poly phones support two currently accepted means of signaling hold, and you can configure phones to use either hold signaling method.

Poly phones support both methods when signaled by a remote endpoint.

Supported Hold Methods

Method	Notes
Signal the media directions with the "a" SDP media attributes <code>sendonly</code> , <code>recvonly</code> , <code>inactive</code> , or <code>sendrecv</code> .	Preferred method.
Set the "c" destination addresses for the zmedia streams in the SDP to zero. For example, <code>c=0.0.0.0</code>	No longer recommended due to RTCP problems associated with this method. Receiving <code>sendrecv</code> , <code>sendonly</code> , or <code>inactive</code> from the server causes the phone to revert to the other hold method.

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.

`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.

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

Call Forward on Shared Lines

You can enable server-based call forwarding for shared lines.

You can use the **Forward** softkey on the phone screen to forward incoming, shared line calls.

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.

feature.forward.enable

1 (default) - Enables call forwarding.

0 - Disables call forwarding. Users cannot use Call Forward and the option is removed from the phone's Features menu.

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.

Change causes system to restart or reboot.

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.

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 - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior.

1 (default) - 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.

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.

In the following parameters, replace x with the line registration index.

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

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.

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.

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: The per-registration parameter `reg.x.callsPerLineKey` overrides this parameter.

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 the `call.callsPerLineKey` parameter.

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.

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).

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

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 using an audio application on the computer. To use this feature, you must enable USB port.

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 C60

You can configure local and centralized multipoint audio conference calls on Poly Trio C60 systems.

When in a conference call, the Poly Trio C60 displays a list of call participants, and you can enable conference management features that users can perform from the Participants screen.

Poly Trio C60 doesn't support local or bridged video conference calls or sharing content during conference calls.

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 - 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) - A meeting reminder does not show a list of numbers to dial.

1 - Tapping Join on a meeting reminder should show a list of numbers to dial rather than immediately dialing the first one.

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

Select a meeting invite field to fetch a VMR or meeting number from.

All (default)

Location

LocationAndSubject

Description

Change causes a reboot.

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

Use Cases	Presence State on Skype for Business Line	Presence String	Presence State on Open SIP Line
Non-Skype line in a call	Busy	In a call	Not Supported
Skype line in a call	Busy	In a call	Not Supported
Content shared over PPCIP	Busy	In a call	Not Supported
Non-Skype line in conference	Busy	In a conference	Not Supported
Skype line in conference	Busy	In a conference	Not Supported
DND on Skype line	DND	Do Not Disturb	Not Supported
DND on Open SIP line	Available	Available	Not Supported

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 System Web Interface

You can configure the phone to support hybrid line registration (Skype for Business and OpenSIP) from the system web interface.

You must set the Base Profile as Skype for Business on the Poly Trio system.

Task

- 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.
- 2 On the Web Configuration Utility page, go to **Settings > Line**.
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.

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

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) - Enabled

0 - Disabled

Change causes system to restart or reboot.

dialplan.applyToDirectoryDial

0 (default) - 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

0 (default) - 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) - Enabled

0 - Disabled

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) - Enabled

0 - Disabled

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) - Enabled

0 - Disabled

Change causes system to restart or reboot.

dialplan.conflictMatchHandling

Selects the dialplan based on more than one match with the least timeout.

0 (default) - Disabled

1 - Enabled

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.

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 system to restart or reboot.

dialplan.filterNonDigitUriUsers

Determine whether to filter out (+) from the dial plan.

0 (default) - Disabled

1 - Enabled

Change causes system to restart or reboot.

dialplan.impossibleMatchHandling

0 – 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 – 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 system to restart or reboot.

dialplan.removeEndOfDial

Sets if the trailing # is stripped from the digits sent out.

1 (default) - Enabled

0 - Disabled

Change causes system to restart or reboot.

dialplan.routing.emergency.outboundIdentity

Choose how your phone is identified when you place an emergency call. The outbound identity is only used when dialing emergency numbers through one of the servers configured in `dialplan.routing.server.x.address`.

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=1: 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

Set the time, in seconds, the phone waits for digit input before placing a call when the phone is onhook.

0-99 seconds

You can apply `dialplan.userDial.timeOut` only when its value is lower than `up.IdleTimeOut`.

OpenSIP 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.

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.
- xR60xR600Rxxxxxxx-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.comR - appends @registrar.polycomcsn.com to any URI calls matching with "764xxxx".
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 custom secondary 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|011xxx.T|[0-1][2-9]xxxxxxxx|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 a secondary 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:

```
[2-9]11|0T|011xxx.T|[0-1][2-9]xxxxxxxx|R8RR,[2-9]xxxxxxT|[2-9]xx.T
```

The following example illustrates how to create a secondary dial tone that sounds like the dial tone used in Ireland. An explanation of the code follows the example.

```
<secondaryDialTone
se.pat.callProg.secondaryDialTone.name="Irish secondary dial"
se.pat.callProg.secondaryDialTone.inst.1.type="chord"
se.pat.callProg.secondaryDialTone.inst.1.value="spare1"
>
<tone.chord.callProg.spare1
tone.chord.callProg.spare1.offDur="0"
```

```
tone.chord.callProg.spare1.onDur="0"
tone.chord.callProg.spare1.repeat="0"
/>
<tone.chord.callProg.spare1.freq
tone.chord.callProg.spare1.freq.1="425"
tone.chord.callProg.spare1.freq.2="450"
/>
<tone.chord.callProg.spare1.level
tone.chord.callProg.spare1.level.1="-12"
tone.chord.callProg.spare1.level.2="-12"
/>
</secondaryDialTone>
```

First, secondaryDialTone call progress pattern calls the spare1 chord. Poly provides spare1 through spare6 for the creation of customized chords.

Then, the tone.chord.callProg.spare1.freq and tone.chord.callProg.spare1.level parameters define the spare1 custom chord consisting of the frequencies and volume levels needed to reproduce the sound of the Irish secondary dialtone.

With these settings in place, the appearance of a comma (",") in a digit map rule triggers the phone to play the secondary dial tone you configured instead of the phone's default dial tone.

Configure Poly Trio to Use Regular Expressions in Dial Plans

Poly Trio systems support regular expressions (regex) on a per-registration basis for matching.

Note: Global dial plans don't support regular expressions.

Task

- 1 Set the following parameter:

```
dialplan.x.digitmap.mode = regex
```

- 2 Set the regex notation in the dialplan.x.digitmap parameter. For example:

```
dialplan.1.digitmap = "^.*bjn\\.vc$"
```

Enhanced 911 (E.911)

This E.911 feature allows you to configure one of three methods the phone uses to provide location information for emergency services.

The phone supports the following methods:

- 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.

Note: In E.911 configurations which use HELD to determine a phone's location, note that the phone defaults to a 24-hour HELD refresh interval if it can't calculate an expiration interval due to an error, if it doesn't have an SNTP connection, or if the calculated expiration interval is greater than 48 hours.

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 xxx.xxx.xxx.xxx.

0 - 255 characters

feature.E911.HELD.username

NULL (default)

Set the user name used to authenticate to the LIS.

0 - 255 characters

feature.E911.HELD.password

NULL (default)

Set the password used to authenticate to the Location Information Server.

0 - 255 characters

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.

CONFIG - Use location information defined in the configuration.

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

locInfo.x.label

Enter a label for the location.

Null (default)

0-255

locInfo.x.country

Enter the country where the phone is located.

Null (default)

0-255

locInfo.x.A1

Enter the national subdivision where the phone is located. For example, a state or province.

Null (default)

0-255

locInfo.x.A3

Enter the city where the phone is located.

Null (default)

0-255

locInfo.x.PRD

Enter the leading direction of the street location.

Null (default)

0-255

locInfo.x.RD

Enter the name of road or street where the phone is located.

Null (default)

0-255

locInfo.x.STS

Enter the suffix of the name used in locInfo.x.RD. For example, street or avenue.

Null (default)

0-255

locInfo.x.POD

Enter the trailing street direction. For example, southwest.

Null (default)

0-255

locInfo.x.HNO

Enter the street address number of the phone's location.

Null (default)

0-255

locInfo.x.HNS

Enter a suffix for the street address used in `locInfo.x.HNS`. For example, A or ½.

Null (default)

0-255

locInfo.x.LOC

Enter any additional information that identifies the location.

Null (default)

0-255

locInfo.x.NAM

Enter a proper name to associate with the location.

Null (default)

0-255

locInfo.x.PC

Enter the ZIP or postal code of the phone's location.

Null (default)

0-255

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.

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.

voIpProt.SIP.header.switchInfo.enable

The phone gathers the MAC address and port information from LLDP and sends that data to the server, which determines phone location based on "Location" configurations.

0 (default) - The register message does not include the custom header `X-switch-info`.

1 - Register messages include the custom header `X-switch-info` that contains the MAC address and port information.

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 `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.

MLPP for 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

Current Call State	New call—same precedence: one active call One call per line	New call—same precedence: multiple active calls Multiple calls per line
Active Call	Rejected	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.
Ringing State	Rejected	The new call displays in the top center corner and the current call is in the main screen.
Call on Hold	Rejected	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.

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:

Preemption Behavior for Low Priority Calls

The phone sends a 180 ringing response to the far end only when a call appearance is allocated for the incoming precedence call.

The following table illustrates the preemption behavior of low priority calls.

Preemption Behavior on Low Priority Calls

Preemption Status	Behavior
Connected	The phone terminates the call with a BYE request containing a preemption Reason header. A preemption tone plays for a configured duration or until the user hangs up, whichever comes first.
Locally Held	The phone may terminate the call with a BYE request containing a preemption Reason header.
Alerting	The phone sends a 486 Busy Here response to the far end containing a preemption Reason header.
Dial Tone or Setup	When the phone is off-hook and receives an incoming precedence call, The phone ignores the precedence call until the user finishes placing an outgoing call and the phone determines if the call has a higher priority. If the call has a lower priority, then the phone doesn't place the call, and a preemption tone plays for the configured time or until the user hangs up. If the call is of the same or higher priority, then the phone terminates the incoming call by sending a 486 Busy Here response to the far end containing a preemption Reason header.
Preceding	When the phone is off-hook and receives an incoming precedence call, The phone ignores the precedence call until the user finishes placing an outgoing call and the phone determines if the call has a higher priority. If the call has a lower priority, then the phone doesn't place the call, and a preemption tone plays for the configured time or until the user hangs up. If the call is of the same or higher priority, then the phone terminates the incoming call by sending a 486 Busy Here response to the far end containing a preemption Reason header.

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)

String

voIpProt.SIP.assuredService.namespace.custom.priority.x

The namespace precedence values, lowest to highest.

Null (default)

String

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 number to identify to the switch that you are dialing an international phone number.

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.

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".

Switching Call Applications

Users can switch between the Generic OpenSIP base profile and the Microsoft Teams call application, giving the Trio C60 system additional flexibility in Modular Room Hub Mode.

The Trio C60 supports up to three (3) OpenSIP voice line registrations.

Note: Poly Trio systems don't support call application switching while in USB mode.

Call Application Switching Parameters

Use the following parameters to configure call application switching.

apps.android.appSwitcher.enabled

0 (default) - Call application switching is disabled.

1 - App Switcher icon appears on the on the Nav bar, allowing users to switch call applications.

: The `device.baseProfile` must be set to `Generic` to enable this parameter.

Change causes the system to restart or reboot.

apps.android.appSwitcher.MSTeams.enabled

0 (default) - Microsoft Teams is not accessible via app switching.

1 - Microsoft Teams is accessible via app switching.

apps.android.appSwitcher.RingCentral.enabled

0 (default) - Ring Central is not accessible via app switching.

1 - Ring Central is accessible via app switching.

apps.android.appSwitcher.ZoomRooms.enabled

0 (default) - Zoom Rooms is not accessible via app switching.

1 - Zoom Rooms is accessible via app switching.

apps.android.statusBar.enabled

1 (default) - Enables the Poly Control Panel.

0 - Disables the Poly Control Panel.

apps.android.statusBar.Bluetooth.enabled

With the `feature.bluetooth.enabled` parameter set to 1, enable this parameter to allow users to toggle Bluetooth functionality on and off from the Poly Control Panel.

0 (default) - Bluetooth doesn't appear in the Poly Control Panel.

1 - Users can toggle Bluetooth on and off from the Poly Control Panel while the system is in Hub mode.

apps.android.statusBar.UCS.enabled

1 (default) - Enables the Poly App icon in the Poly Control Panel.

0 - Disables the Poly App icon in the Poly Control Panel.

Shared Lines

This section shows you how to configure shared line features.

Shared Call Appearances

Shared call appearance enables calls 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 to enter a conversation on one of the group phones. This is referred to as a barge in.

A phone with shared lines can send caller ID (CID) information on an outbound call. When other shared lines join in the outbound shared call, the CID displays the information if the SIP messages have CID information.

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@poly.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.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.

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.

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.

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.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 `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` .

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.pearlymedia.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

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 `voIpProt.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

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 and/or the H.323 alias used 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.filterReflectedBlDialogs

- 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 parameters 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.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 parameters 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't 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 [Poly 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.

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 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.

call.shared.distinctiveLedOnHold

0 (default) - The LED blinks red for both remotely held calls and locally held calls.

1 - The LED blinks as red and green for local hold calls, and blinks only red for remotely held calls.

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.

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.

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.

Daisy-Chaining Poly Trio C60 Systems

You can pair (daisy-chain) a Poly Trio C60 system with up to two other Poly Trio C60 systems for enhanced audio performance in large or acoustically challenging rooms.

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 can't pair or daisy-chain a Poly Trio C60 system with Poly Trio 8500 or 8800 systems or with a Poly Trio C60 system connected to your network using Wi-Fi.

Daisy-Chaining Requirements

When daisy-chaining Poly Trio C60 systems, you must adhere to some requirements for optimal performance.

You can daisy-chain up to three Poly Trio C60 systems for audio-only calls when you meet the following requirements:

Daisy-Chain Poly Trio Systems

You can daisy-chain up to three Trio C60 systems for audio-only calls. You must configure one Trio C60 system as the hub and the other systems as devices.

Task

- 1 On the Poly Trio system you want to set as the hub, go to **Settings > Advanced > Networked Devices** and set **Networked Device Role** to **Hub**.
- 2 On the systems you want to set as a device, go to **Settings > Advanced > Networked Devices** and set **Networked Device Role** to **Device**.
The systems you set as a device reboot.
- 3 After the device systems reboot, on the hub system, go to **Settings > Advanced > Networked Devices** and under **Available Devices**, select a device system.
- 4 Select **Pair** and wait for the devices to connect.
- 5 Optional: If you want to daisy-chain another system, repeat the pairing process on the second device system.

When you daisy-chain two or more Poly Trio systems, all the systems display the user interface on the hub system.

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.

mr.pair.maxDevices

Set the maximum number of paired devices to **2** for daisy-chaining Trio systems.

5 (default)

0 - 15

Hardware and Power for Poly Trio C60 Systems

This section provides information on hardware and power for Poly Trio systems and accessories, as well as information on power management.

Powering the Poly Trio C60

You can power your Poly Trio C60 system with Power over Ethernet (PoE) or PoE+ (IEEE 802.3 at Type 2). When the Poly Trio system is booting up, an on-screen message indicates the available power supply type.

Poly Trio C60 systems support the following power options, which provide full functionality:

- PoE+
- PoE Class 0

The following features aren't available on Poly Trio C60 systems when using PoE:

- The system LAN OUT port doesn't provide PoE+ power.
- You can't charge USB devices (mobile phones or tablets) connected to the system USB port.
- Maximum peak power to the loudspeaker is limited.

Power the Poly Trio C60 System with the Optional Power Adapter

If your building isn't equipped with PoE+, you can use the optional power adapter to provide PoE+ power and full functionality to your Poly Trio C60 system.

Place the power 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 power injector. Keep the power injector away from heat and humidity and free from vibration and dust.

Important: When using the power adapter to power your Poly Trio system, you must connect the cables in the following sequence.

Task

- 1 Plug the AC power cord of the power adapter into the wall and use a network cable to connect the power adapter to the system.
- 2 Connect the power adapter to the network with a CAT-5E or CAT-6 Ethernet cable.
The power adapter LED glows green when the system is correctly powered.
If the power adapter LED glows yellow, the adapter is bypassed, and the Poly Trio C60 system is drawing PoE power from the outlet.
- 3 Optional: Turn off the PoE network port or connect the Poly Trio system in the following sequence:
 - A Power up Poly Trio C60 system using the power adapter, but don't plug the device into the network wall port.
 - B Wait for the system to boot up.
 - C Plug the system into the network wall port.
 - D Ensure the LED indicator on the power adapter is green.

Poly Trio System Power Management

Power available to Poly Trio systems is limited. 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 power requirements and options carefully to understand power for your Poly Trio system.

The Poly Trio C60 system supports powering the following types of devices:

- USB devices consuming < 2.5 W power

- USB port over current detection

USB Port Power Management

Device charging with the USB port on the Poly Trio C60 system is disabled by default. When disabled, the USB host port provides 100 mA of power for peripheral devices.

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

Poly Trio System Power Management Parameters

You can use the parameters listed to manage the Poly Trio system's power usage.

poe.pse.class

Specify the LAN OUT PoE class.

0 (default)

0 - 3

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.

usb.charging.enabled

0 (default) - You can't charge USB-connected devices from the USB charging port.

1 - Enable fast charging of devices connected by USB port up to 7.5 W power / 1.5 A current.

Power-Saving on Poly Trio Systems

Power-saving automatically puts the phone into a low-power state to conserve energy when not in use.

When the phone is in power-saving mode, a steady yellow LED indicator displays. The phone returns to a full-power state after detecting user movement (based on changes in lighting), a button press, screen touch, or incoming call.

You can configure the following power-saving options for Poly Trio systems:

- Power-saving during workdays
- Power-saving during nonworking days
- Idle or inactivity time after which the phone enters power-saving mode

Note: Poly Trio systems can't enter power-saving mode while idle in the **Bluetooth** menu. To ensure the phone can enter power-saving mode, don't leave the phone idle in the **Bluetooth** menu.

You can configure the behavior of the LED indicator (see LED Behavior Patterns).

Power-Saving Parameters

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

powerSaving.Enable

0 (default) - The paired device does not into power-saving mode.

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.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 weekday.

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 (see `powerSaving.officeHours.duration` for an example).

Phone Display Features

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.

device.auth.localAdvancedPassword.set

Set a password for the **Advanced** menu.

0 (default) - You cannot set a password for the **Advanced** menu.

1 - You can set a password for the **Administrator** menu.

device.auth.localAdvancedPassword

Enter a password for the **Administrator** menu.

Null (default)

String (0 to 64 characters)

feature.advancedUser.enabled

0 (default) - The password-protected **Advanced** menu displays.

1 - Renames the **Advanced** menu item to **Admin** and adds a menu item **Advanced** that contains a subset of administrator features.

feature.advancedUser.web.enabled

Display the **Advanced** menu in the system web interface.

0 (default) - The system web interface provides login options for **Admin** or **User** only.

1 - Enable the **Advanced** user login option on the system web interface.

ui.menu.advancedUser.networkConfiguration.

Set whether to display the **Network** option under **Settings** for advanced users.

1 - (default) Displays the **Network** option.

0 - The **Network** option doesn't display.

ui.menu.advancedUser.networkConfiguration.tls

Set whether to display the TLS option under **Settings > Network** for advanced users.

1 – (default) Displays the TLS option.

0 – The TLS option doesn't display.

This parameter requires **ui.menu.advancedUser.networkConfiguration** to be set to 1.

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 accessory.

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 Trio<model number>_xxxx where xxxx is the last four digits of the phone's MAC address.

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:

- system.name
- reg.x.displayname
- reg.x.label
- reg.x.address
- Default system name

If you set the system name using the system.name parameter, the value you set displays for the system unless you configure a name to display for a specific feature.

Display Name Parameters

Set the phone name using one or more of following parameters.

bluetooth.device.name

Enter the name of the system that broadcasts over Bluetooth to other devices.

NULL (default)

UTF-8 encoded string

reg.x.address

The user part (for example, 1002) or the user and the host part (for example, 1002@poly.com) of the registration SIP URI or the H.323 ID/extension for registration x.

Null (default)

string address

reg.x.displayname

The display name used in SIP signaling and/or the H.323 alias used as the default caller ID for registration x.

Null (default)

UTF-8 encoded string

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.cfgLabelEliide` 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 phone.

Enter a string, maximum 96 characters.

LED Indicators on Poly Trio System

The LED indicators on Poly Trio systems alert users to the different states of the phone. You can turn LED indicators on or off, and set the pattern, color, and duration of a pattern for the LED indicators.

LED Pattern Parameters

The LED pattern parameters listed in the following list configure the pattern state, color, and duration of the LED indicators and the pattern types on Poly devices.

For each parameter, specify x, y, and a permitted value:

- Specify an LED pattern using the LED pattern parameters.
- For x, specify an LED pattern type.
- For y, specify the step in the LED pattern with a number between 1-20.

Use the parameters in the following list to set the pattern state, color, and duration of the LED indicators.

ind.pattern.x.step.y.state

0 (default) - Turn off the LED indicator.

1 - Turn on the LED indicator.

ind.pattern.x.step.y.color

Specify the color of the LED indicator.

Red (default)

Green

Yellow

ind.pattern.x.step.y.duration

Specify the duration of the pattern in milliseconds.

0 (default)

0 - 32767

LED Indicator Pattern Types

Enter one of the values in the following table to indicate the LED indicator pattern type.

LED Indicator Pattern Type

Pattern Type	Function
powerSaving	Sets the behavior for Message Waiting Indicator when the phone is in Power Saving mode.
active	Sets the pattern for line keys during active calls.
on	Turns on the LED indicator pattern.
off	Turns off the LED indicator pattern.
offering	Sets the pattern for line keys during incoming calls.
flash	Sets the pattern for line keys during held calls and the Message Waiting Indicator when there are unread voicemail messages.
lockedOut	Sets the pattern for line keys when a remote party is busy on a shared line.
held	Sets the pattern for line keys during a held call.
remoteBusyOffering	Sets the pattern for line keys for monitored BLF contacts when the BLF is in an active call and receives a new incoming call.
blfHold	Sets the pattern for BLF line keys when a call is on the hold. The default pattern is slow flashing red color LED.
parkedCallSelf	Sets the LED pattern for a self-parked call.
parkedCallRemote	Sets the LED pattern for remote-parked call.

Example: Turn Off the Message Waiting Indicator in Power Saving Mode

When Power Saving mode is enabled, the screen darkens, and the MWI flashes red.

By default, the powerSaving pattern has two steps before the pattern is repeated: a quick on period and then a long off period.

You can turn off the MWI or change the duration of the pattern steps.

Task

» Set the parameter `ind.pattern.powerSaving.step.1.state` to 0.

Poly Trio System Status Messages

You can choose to display a maximum of five multiline messages in the 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

<message line one>

<message line two>

<message line three>

<message line four>

<message 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 accessories.

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.

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.snntp.olsonTimezoneID`. 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.snntp.olsonTimezoneID

Enter an Olson time zone ID. If set to an invalid or unrecognized value, the time zone is 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.

Task

- 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.

Task

- 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.

Olson Time Zone IDs

Olson Time Zone ID	Poly Trio Time Zone ID
Pacific/Midway	(GMT -11:00) Midway Island
Pacific/Honolulu	(GMT -10:00) Hawaii
America/Anchorage	(GMT -9:00) Alaska
Mexico/BajaNorte	(GMT -8:00) Baja California
America/Phoenix	(GMT -7:00) Arizona
America/Chihuahua	(GMT -7:00) Chihuahua,La Paz
America/Denver	(GMT -7:00) Mountain Time (US & Canada)
America/Costa_Rica	(GMT -6:00) Central America
America/Chicago	(GMT -6:00) Central Time (US & Canada)
America/Mexico_City	(GMT -6:00) Mexico City
America/Regina	(GMT -6:00) Saskatchewan
America/Bogota	(GMT -5:00) Bogota,Lima
America/New_York	(GMT -5:00) Eastern Time (US & Canada)
America/Caracas	(GMT -4:30) Caracas
America/Barbados	Atlantic Time (Barbados)
America/Halifax	(GMT -4:00) Atlantic Time (Canada)

Olson Time Zone ID	Poly Trio Time Zone ID
America/Manaus	(GMT -4:00) Manaus,La Paz
America/Santiago	(GMT -3:00) Santiago
America/St_Johns	(GMT -3:30) Newfoundland
America/Sao_Paulo	(GMT -3:00) Brasilia
America/Argentina/Buenos_Aires	(GMT -3:00) Buenos Aires
America/Godthab	(GMT -3:00) Greenland
America/Montevideo	(GMT -3:00) Montevideo
Atlantic/South_Georgia	(GMT -2:00) Mid-Atlantic
Atlantic/Azores	(GMT -1:00) Azores
Atlantic/Cape_Verde	(GMT -1:00) Cape Verde Islands
Africa/Casablanca	(GMT 0:00) Casablanca
Europe/London	(GMT 0:00) London,Lisbon
Europe/Amsterdam	(GMT +1:00) Amsterdam,Berlin
Europe/Belgrade	(GMT +1:00) Bratislava
Europe/Brussels	(GMT +1:00) Brussels
Europe/Sarajevo	(GMT +1:00) Sarajevo,Skopje
Africa/Brazzaville	(GMT +1:00) West Central Africa
Africa/Windhoek	(GMT +1:00) Windhoek
Asia/Amman	Amman
Europe/Athens	(GMT +2:00) Athens
Asia/Beirut	Beirut
Africa/Cairo	(GMT +2:00) Bucharest,Cairo
Europe/Helsinki	(GMT +2:00) Helsinki,Kyiv
Asia/Jerusalem	(GMT +2:00) Jerusalem
Africa/Harare	(GMT +2:00) Harare,Pretoria
Europe/Minsk	(GMT +3:00) Minsk
Asia/Istanbul	(GMT +3:00) Istanbul
Europe/Moscow	(GMT +3:00) Moscow
Asia/Kuwait	(GMT +3:00) Kuwait,Riyadh

Olson Time Zone ID	Poly Trio Time Zone ID
Africa/Nairobi	(GMT +3:00) Nairobi
Asia/Tehran	(GMT +3:30) Tehran
Asia/Baku	(GMT +4:00) Baku,Tbilisi
Asia/Yerevan	(GMT +4:00) Yerevan
Asia/Dubai	Dubai
Asia/Kabul	(GMT +4:30) Kabul
Asia/Karachi	(GMT +5:00) Karachi
Asia/Tashkent	(GMT +5:00) Tashkent
Asia/Yekaterinburg	(GMT +5:00) Yekaterinburg (RTZ 4)
Asia/Calcutta	(GMT +5:30) Kolkata,New Delhi
Asia/Colombo	(GMT +5:30) Sri Jayawardenepura
Asia/Katmandu	(GMT +5:45) Kathmandu
Asia/Dhaka	(GMT +6:00) Astana,Dhaka
Asia/Rangoon	(GMT +6:30) Yangon (Rangoon)
Asia/Krasnoyarsk	(GMT +7:00) Krasnoyarsk (RTZ 6)
Asia/Bangkok	(GMT +7:00) Bangkok,Hanoi
Asia/Jakarta	(GMT +7:00) Jakarta
Asia/Shanghai	(GMT +8:00) Beijing,Chongqing
Asia/Hong_Kong	(GMT +8:00) Hong Kong,Urumqi
Asia/Irkutsk	(GMT +8:00) Irkutsk (RTZ 7)
Asia/Kuala_Lumpur	(GMT +8:00) Kuala Lumpur
Asia/Taipei	(GMT +8:00) Taipei,Perth
Asia/Tokyo	(GMT +9:00) Tokyo,Seoul,Osaka
Asia/Yakutsk	(GMT +9:00) Sapporo,Yakutsk (RTZ 8)
Australia/Adelaide	Adelaide
Australia/Darwin	Darwin
Australia/Brisbane	Brisbane
Australia/Hobart	(GMT +10:00) Hobart
Australia/Sydney	Sydney,Canberra

Olson Time Zone ID	Poly Trio Time Zone ID
Asia/Vladivostok	(GMT +10:00) Vladivostok
Pacific/Guam	(GMT +10:00) Guam,Port Moresby
Asia/Magadan	(GMT +10:00) Magadan (RTZ 9)
Pacific/Auckland	(GMT +12:00) Auckland,Anadyr
Pacific/Fiji	(GMT +12:00) Fiji Islands
Pacific/Majuro	(GMT +12:00) Marshall Islands
Pacific/Tongatapu	(GMT +13:00) Nuku'alofa

Time Zone Location Description

There are two parameters that configure a time zone location description for their associated GMT offset.

- `device.snntp.gmtOffsetcityID` If you are not provisioning phones manually from the phone menu or Web Configuration Utility and you are setting the `device.snntp.gmtOffset` parameter, then you must configure `device.snntp.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.snntp.gmtOffset` parameter manually using the phone menu or Web Configuration Utility.
- `tcplpApp.snntp.gmtOffsetcityID` If you are not provisioning phones manually from the Web Configuration Utility and you are setting the `tcplpApp.snntp.gmtOffset` parameter, then you must configure `tcplpApp.snntp.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 `tcplpApp.snntp.gmtOffset` parameter manually using the Web Configuration Utility.

Time Zone Location Parameters

The following parameters configure time zone location.

Time Zone Location Parameter Values

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

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

Permitted Value	Time Zone Description
51	GMT +1:00) Brussels
52	(GMT +1:00) Copenhagen
53	(GMT +1:00) Madrid,Paris
54	(GMT +1:00) Amsterdam,Berlin
55	(GMT +1:00) Bern,Rome
56	(GMT +1:00) Stockholm,Vienna
57	(GMT +1:00) West Central Africa
58	(GMT +1:00) Windhoek
59	(GMT +2:00) Bucharest,Cairo
60	(GMT +2:00) Amman,Beirut
61	(GMT +2:00) Helsinki,Kyiv
62	(GMT +2:00) Riga,Sofia
63	(GMT +2:00) Tallinn,Vilnius
64	(GMT +2:00) Athens
65	(GMT +2:00) Damascus
66	(GMT +2:00) E.Europe
67	(GMT +2:00) Harare,Pretoria
68	(GMT +2:00) Jerusalem
69	(GMT +2:00) Kaliningrad (RTZ 1)
70	(GMT +2:00) Tripoli
71	(GMT +3:00) Moscow
72	(GMT +3:00) St.Petersburg
73	(GMT +3:00) Volgograd (RTZ 2)
74	(GMT +3:00) Kuwait,Riyadh
75	(GMT +3:00) Nairobi
76	(GMT +3:00) Baghdad
77	(GMT +3:00) Minsk, Istanbul
78	(GMT +3:30) Tehran
79	(GMT +4:00) Abu Dhabi,Muscat
80	(GMT +4:00) Baku,Tbilisi
81	(GMT +4:00) Izhevsk,Samara (RTZ 3)
82	(GMT +4:00) Port Louis
83	(GMT +4:00) Yerevan
84	(GMT +4:30) Kabul
85	(GMT +5:00) Yekaterinburg (RTZ 4)
86	(GMT +5:00) Islamabad
87	(GMT +5:00) Karachi
88	(GMT +5:00) Tashkent
89	(GMT +5:30) Mumbai,Chennai
90	(GMT +5:30) Kolkata,New Delhi

Permitted Value	Time Zone Description
91	(GMT +5:30) Sri Jayawardenepura
92	(GMT +5:45) Kathmandu
93	(GMT +6:00) Astana,Dhaka
94	(GMT +6:00) Almaty
95	(GMT +6:00) Novosibirsk (RTZ 5)
96	(GMT +6:30) Yangon (Rangoon)
97	(GMT +7:00) Bangkok,Hanoi
98	(GMT +7:00) Jakarta
99	(GMT +7:00) Krasnoyarsk (RTZ 6)
100	(GMT +8:00) Beijing,Chongqing
101	(GMT +8:00) Hong Kong,Urumqi
102	(GMT +8:00) Kuala Lumpur
103	(GMT +8:00) Singapore
104	(GMT +8:00) Taipei,Perth
105	(GMT +8:00) Irkutsk (RTZ 7)
106	(GMT +8:00) Ulaanbaatar
107	(GMT +9:00) Tokyo,Seoul,Osaka
108	(GMT +9:00) Sapporo,Yakutsk (RTZ 8)
109	(GMT +9:30) Adelaide,Darwin
110	(GMT +10:00) Canberra
111	(GMT +10:00) Magadan (RTZ 9)
112	(GMT +10:00) Melbourne
113	(GMT +10:00) Sydney,Brisbane
114	(GMT +10:00) Hobart
115	(GMT +10:00) Vladivostok
116	(GMT +10:00) Guam,Port Moresby
117	(GMT +11:00) Solomon Islands
118	(GMT +11:00) New Caledonia
119	(GMT +11:00) Chokurdakh (RTZ 10)
120	(GMT +12:00) Fiji Islands
121	(GMT +12:00) Auckland,Anadyr
122	(GMT +12:00) Petropavlovsk-Kamchatsky (RTZ 11)
123	(GMT +12:00) Wellington
124	(GMT +12:00) Marshall Islands
125	(GMT +13:00) Nuku'alofa
126	(GMT +13:00) Samoa

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.

Poly phones can try alternate sources for SNTP addresses and offsets if attempts to contact the time server don't work due to one of the following issues:

- The attempt fails.
- The phone receives invalid or no responses.

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 - Displays the date above time.

0 (default) - 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.snntp.address

Specifies the SNTP server address.

NULL (default)

Valid hostname or IP address.

tcpIpApp.snntp.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.snmp.address.overrideDHCP

0 (Default) - DHCP values for the SNMP server address are used.

1 - SNMP parameters override the DHCP values.

tcpIpApp.snmp.daylightSavings.enable

Enable or disable Daylight Savings Time rules to the displayed time.

1 (Default) - Enabled

0 - Disabled

tcpIpApp.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.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.snmp.gmtOffsetcityID

You must disable `tcpIpApp.snmp.daylightSavings.enable` for the phone to display daylight savings time according to `gmtOffsetcityID`.

NULL (Default)

For descriptions of all values, refer to Time Zone Location Description.

0 to 127

tcpIpApp.snmp.gmtOffset.overrideDHCP

0 (Default) - The DHCP values for the GMT offset are used.

1 - The SNTP values for the GMT offset are used.

tcpIpApp.snmp.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.snmp.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

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.

Date Formats

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

lcl.datetime.date.format	lcl.datetime.date.longformat	Date Displayed on Phone
D,dM	0	Fri, 19 Aug
D,dM	1	Friday, August 19
DD/MM/YY	n/a	19/08/11
DD/MM/YYYY	n/a	19/08/2011
MM/DD/YY	n/a	08/19/11
MM/DD/YYYY	n/a	08/19/2011
YY/MM/DD	n/a	11/08/19
YYYY/MM/DD	n/a	2011/08/11

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 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 Keyboard Layout

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.

Task

- 1 On the phone's keyboard, long-press and release the comma key and choose .
- 2 Select one or more available languages and press the back arrow.
The phone enables each language you select, along with its default keyboard layout. When you enable more than one language, a globe key displays on the phone keyboard.
- 3 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.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.

Unicode Ranges for Basic Character Support

Name	Range
C0 Controls and Basic Latin	U+0000 - U+007F
C1 Controls and Latin-1 Supplement	U+0080 - U+00FF
Cyrillic (partial)	U+0400 - U+045F

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.

Task

- » On the Poly Trio system Home screen, go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu > Country of origin**.

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.

Task

- 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 Poly, the line keys are labeled as 1_Poly, 2_Poly, 3_Poly, and 4_Poly. 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: 12223334444 displays as 1-222-333-4444.

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

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.

Task

» Go to **Settings > Advanced > Administration Settings > Home Screen Label**.

Number and Label Parameters

You can configure display of the phone number or label on the Home screen using centralized provisioning parameters.

homeScreen.placeACall.enable

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.

Custom - Enter an alphanumeric string between 0 and 255 characters into the `homeScreen.customLabel` parameter.

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 your phone 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 × 106 pixels with a size of 100 KB or smaller. You can upload images as large as 200 × 200 pixels, however, the phone automatically scales the icons to 106 × 106 pixels. The phone only supports .png image files. Other image filetypes, such as .jpg, .tiff, .bmp, .webp and .gif aren't supported.

You can configure up to 24 icons for registered lines and contacts.

Note: Custom PNG icons larger than 100 KB won't display on daisy-chained Poly Trio systems.

You can add the icons to the root directory or a subdirectory on the provisioning server or specify the URL location for the icons. If you place icons in a subdirectory, specify the subdirectory in the `ICONS_DIRECTORY` attribute in the `<APPLICATION>` tag in the `MAC.cfg` file.

Note: Make sure that the icons configured and distributed through UC Software 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 `reg.y.icon` or favorite contacts set for `<up></up>` in the `Mac-directory.xml` file.

Null (default)

icon file name or URL location

For example `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 `icons.x` to this registered line (y), where y equals 1-24.

Null

iconX, where x is 1-24

For example, if `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.

Task

- 1 Copy icons to your provisioning or FTP server.
- 2 Configure the following parameters:
 - `reg.1.address="7756638509"`
 - `reg.2.address="7756638708"`
 - `icons.1="blue.png"`
 - `icons.2="green.png"`
 - `reg.1.icon="icon1"`
 - `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.

Task

- 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>

```

Capture Your Phone's Screen

You can capture your phone's current screen.

Before you can take a screen capture, make sure the phone's web server is enabled.

Task

- 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 this step 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 from the phone.
- 7 Enter the username **Polycom** and the phone's current password.
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.

`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.

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.

up.callStateView

Set the default screen while in a call.

Drawer (default) – Displays the in-call controls.

Dialpad – Displays the dial pad.

Note that `reg.X.callStateView` can override this setting.

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 `reg.X.callStateView.conference` can override this setting.

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 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 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

0 (default) - Enable display of the Applications icon on the phone Home screen.

1 - 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

0 (default) - Disable display of the call forward icon on the phone Home screen.

1 - Enable 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.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.

LED Indicators

LED indicators alert users to the different states of the phone and remote contacts.

Important: Configuring these options can impact the accessibility of your phones for people who have low vision or are colorblind. It can also impact accessibility for people with seizure disorders.

You can turn LED indicators on or off and set the pattern, color, and duration of a pattern for all physical keys on the phones and the following LED indicators:

- Line keys
- Headset key

Use the following example configuration tasks to configure custom LED patterns.

LED Indicator Pattern Types

Use the values from the following table to indicate the LED indicator pattern type.

LED Indicator Pattern Type

Pattern Type	Function
powerSaving	Sets the behavior for the message waiting indicator when the phone is in power saving mode.
active	Sets the pattern for line keys during active calls.
on	Turns on the LED indicator pattern.
off	Turns off the LED indicator pattern.
offering	Sets the pattern for line keys during incoming calls.
flash	Sets the pattern for line keys during held calls and the message waiting indicator when there are unread voicemail messages.
lockedOut	Sets the pattern for line keys when a remote party is busy on a shared line.
held	Sets the pattern for line keys during a held call.
remoteBusyOffering	Sets the pattern for line keys for monitored BLF contacts when the BLF is in an active call and receives a new incoming call.
blfHold	Sets the pattern for BLF line keys when a call is on the hold. The default pattern is a slow flashing red LED.
parkedCallSelf	Sets the LED pattern for a self-parked call.
parkedCallRemote	Sets the LED pattern for remote-parked call.

Set an LED Pattern for Active Calls

Configure the phone's LED to alternate colors during an active call.

Task

- 1 Open the configuration file.
- 2 Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.

Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.active.step.1.state="1"  
ind.pattern.active.step.1.color="<LED color>"  
ind.pattern.active.step.1.duration="<duration>"
```

- 3 Enable the LED, configure the second LED color, and set how long the LED glows, in milliseconds, before turning off. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.active.step.2.state="1"  
ind.pattern.active.step.2.color="<LED color>"  
ind.pattern.active.step.2.duration="<duration>"
```

- 4 Save the configuration file.

Set an LED Pattern on BLF for Held Calls

Configure the LED indicator to flash when a monitored BLF line is on hold.

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

Task

- 1 Open the configuration file.
- 2 Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off. Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.blfHold.step.1.state="1"  
ind.pattern.blfHold.step.1.color="<LED color>"  
ind.pattern.blfHold.step.1.duration="<duration>"
```

- 3 Disable the LED and set how long the LED remains off, in milliseconds, before turning back on. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.blfHold.step.2.state="0"  
ind.pattern.blfHold.step.2.duration="<duration>"
```

- 4 Save the configuration file.

Set an LED Pattern for Incoming Calls

Configure the phone's LED to flash a different color for incoming calls.

Task

- 1 Open the configuration file.
- 2 Change the LED indicator color for incoming calls. Set the LED color as Red, Green, or Yellow. The default is Green.

```
ind.pattern.offering.step.1.color="<LED color>"
```

- 3 Save the configuration file.

Set an LED Pattern for Self-Parked Calls

Set how the LED indicator behaves for self-parked calls.

Task

- 1 Open the configuration file.
- 2 Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.
Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.parkedCallSelf.step.1.state="1"  
ind.pattern.parkedCallSelf.step.1.color="<LED color>"  
ind.pattern.parkedCallSelf.step.1.duration="<duration>"
```

- 3 Save the configuration file.

Set an LED Pattern for Remote-Parked Calls

Set how the LED indicator behaves for remote-parked calls.

Task

- 1 Open the configuration file.
- 2 Enable the LED, configure the LED color, and set how long the LED glows, in milliseconds, before turning off.
Set the LED color as Red, Green, or Yellow. The default is Red. Set the duration of the pattern from 0 to 32767 milliseconds. The default is 0.

```
ind.pattern.parkedCallRemote.step.1.state="1"  
ind.pattern.parkedCallRemote.step.1.color="<LED color>"  
ind.pattern.parkedCallRemote.step.1.duration="<duration>"
```

- 3 Save the configuration file.

Configure LED Behavior for Held Calls on Shared Lines

Configure the LED to blink red and green for locally held calls and to blink only red for remotely held calls.

By default, the phone blinks red for both remotely and locally held calls. You can also create a custom pattern.

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

Task

- 1 Open the configuration file.
- 2 Configure a distinctive LED behavior for held calls on shared lines.

```
call.shared.distinctiveLedOnHold="1"
```

- 3 Save the configuration file.

Enable the LED Indicator for Incoming Calls

In addition to displaying caller ID information onscreen and playing a ringtone, configure the phone to flash the LED indicator when it receives an incoming call.

Task

- 1 Open the configuration file.
- 2 Enable the phone's LED to flash for incoming calls.

```
call.offering.led="1"
```

- 3 Save the configuration file.

Enable the LED Indicator for Missed Calls on a Call Server

In addition to displaying new missed call information onscreen and in the **Missed Calls** directory, configure the phone to flash the LED indicator when the call server signals to the phone about a missed call.

After viewing the missed call, the LED indicator stops flashing.

Note: Some call servers can't signal phones about missed calls, so even with this feature enabled, the LED indicator may not illuminate. Check with your call server administrator to confirm support for this feature.

Task

- 1 Open the configuration file.
- 2 Enable the LED indicator to flash if there is a missed call on the call server.

```
call.serverMissedCall.led="1"
```

- 3 Save the configuration file.

Disable in Power Saving Mode

Disable the while the phone is in power saving mode to conserve power.

Task

- 1 Open the configuration file.
- 2 Disable the in power saving mode.

```
ind.pattern.powerSaving.step.1.state="0"
```

- 3 Save the configuration file.

Directories and Contacts

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.

1 (default) - The local contact directory is enabled.

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.

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, a ";" or "p" control character causes a one-second pause. A ";" or "w" control character causes 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.

Maximum File Size and Number of Contacts

Phone	Maximum File Size	Maximum Number of Contacts in File
Poly Trio systems	4MB	3000

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 restart. 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` 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. 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 - 100 KB

`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 - 200 KB

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

Element	Definition	Permitted Values
fn	The contact's first name	UTF-8 encoded string of up to 40 bytes1
ln	The contact's last name	UTF-8 encoded string of up to 40 bytes1
ct	<p>Contact</p> <p>Used by the phone to address a remote party in the same way that a user manually dials a string of digits or a SIP URL . Also used to associate incoming callers with a particular directory entry.</p> <p>The maximum field length is 128 characters.</p> <p>Note: You can't duplicate this field or leave it <code>Null</code>.</p>	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL
sd	<p>Speed Dial Index</p> <p>Associates a particular entry with a speed dial key for one-touch dialing or dialing.</p>	Null, 1 to 20
lb	<p>The label for the contact</p> <p>The label of a contact directory item is by default the label attribute of the item. If the label attribute does not exist or is <code>Null</code>, then the first and last names form the label. A space is added between first and last names.</p>	UTF-8 encoded string of up to 40 bytes1
pt	<p>Protocol</p> <p>The protocol to use when placing a call to this contact.</p>	SIP or Unspecified
rt	<p>Ring Tone</p> <p>When incoming calls match a directory entry, this field specifies the ringtone to use.</p>	Null, 1 to 21
dc	<p>Divert Contact</p> <p>The address to forward calls to if the Auto Divert feature is enabled.</p>	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL

Element	Definition	Permitted Values
ad	<p>Auto Divert</p> <p>If set to 1, callers that match the directory entry are diverted to the address specified for the divert contact element.</p> <p>Note: If auto-divert is enabled, it has precedence over auto-reject.</p>	0 or 1
ar	<p>Auto Reject</p> <p>If set to 1, callers that match the directory entry specified for the auto reject element are rejected.</p> <p>Note: If auto divert is also enabled, it has precedence over auto reject.</p>	0 or 1
bw	<p>Buddy Watching</p> <p>If set to 1, this contact is added to the list of watched phones.</p>	0 or 1
bb	<p>Buddy Block</p> <p>If set to 1, this contact is blocked from watching this phone.</p>	0 or 1
up	<p>User Photo</p> <p>The contact's photo icon set by the icons.x parameter.</p>	1-24

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

Phone Model	Range
Poly Trio systems	1 - 20

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 Home screen.

Enter a speed dial index number in the <sd>x</sd> element in the <MAC address>-directory.xml file to display a contact directory entry as a speed dial key on the 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: Use corporate directories that have server-side sorting for better performance. Consult your LDAP administrator when making any configuration changes for the corporate directory. For more information on LDAP attributes, see [RFC 4510 - Lightweight Directory Access Protocol \(LDAP\): Technical Specification Road Map](#)

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 Poly 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.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

other

Change causes system to restart or reboot.

dir.corp.auth.useLoginCredentials

0 (default) - Disabled

1 - Enabled

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.

64 (default)

8 to 64

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 the phone to 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 - 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 list to another server, use the `CALL_LISTS_DIRECTORY` field in the primary configuration file. All call lists are enabled by default.

The phone maintains all the calls in three separate user accessible call lists: 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`

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`

Generic Base Profile - 1 (default)

0 - Consultation calls not joined into a conference call aren't listed as separate calls in the calls list.

1 - Each consultation call 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 dialpad.

0 - Disables all call lists.

`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)

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 log feature.

0 - The Exchange call log feature is disabled, the user call log history can't be retrieved from the Exchange server, and the phone generates call logs 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.

Call Log Elements and Attributes

Element	Permitted Values
<code>direction</code> Call direction with respect to the user.	In, Out
<code>disposition</code> Indicates what happened to the call. When a call entry is first created, the disposition is set to Partial.	Busy, Forwarded, Normal, Partial, Preempted, Rejected, RemotelyHandled, Transferred
<code>line</code> The line (or registration) index.	Positive integer
<code>protocol</code> The line protocol.	SIP
<code>startTime</code> The start time of the call. For example: 2010-01-05T12:38:05 in local time.	String
<code>duration</code> The duration of the call, beginning when it is connected and ending when the call is terminated. For example: <code>PT1H10M59S</code> .	String
<code>count</code> The number of consecutive missed and abandoned calls from a call destination.	Positive Integer
<code>destination</code>	Address

Element	Permitted Values
<p>The original destination of the call.</p> <p>For outgoing calls, this parameter designates the outgoing call destination; the name is initially supplied by the local phone (from the name field of a local contact entry) but may later be updated via call signaling. This field should be used for basic redial scenarios.</p> <p>For incoming calls, the called destination identifies the requested party, which may be different than any of the parties that are eventually connected (the destination may indicate a SIP URI that is different from any SIP URI assigned to any lines on the phone).</p>	
source	Address
The source of the call (caller ID from the call recipient's perspective).	
Connection	Address
<p>An array of connected parties in chronological order.</p> <p>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.</p>	
finalDestination	Address
The final connected party of a call that has been forwarded or transferred to a third party.	

Resetting Contacts and Recent Calls Lists on Your Phone

You can reset the Contacts list and Recent call lists stored locally on your phone to their default settings.

Task

- 1 On the phone, go to **Settings > Advanced**.
- 2 Enter the administrative password.
- 3 Select **Reset to defaults > Reset User Data**.
- 4 When prompted "Are you sure?", select **Yes**.

Configuring Security Options

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

Administrator and user passwords control two levels of access to certain configuration menus in your Poly Trio system.

The administrator password grants full access to all configuration settings available on your system, and the user password grants limited access to configuration settings.

When you first power on a new Poly Trio system or following a factory reset, the system displays a message prompting you to change the default administrator password. You must change the default administrator password to a unique password to access the Poly Trio local interface and system web interface. You can't use the default administrator password again.

You must have a user or administrator password before you can access certain menu options on the phone and in the system web interface. The default passwords are:

- Administrator password: 456
- User password: 123

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

- The pop-up prompt when the phone first registers
- Phone menu
- System web interface (default user password only)
- Use the parameter `reg.1.auth.password`

You can use an administrator password where a user password is required to see all the user options. While you can use the user password where the administrator password is required, the phone displays a limited set of menu options. Note that the system web interface displays different features and options depending on which password you use.

When you set the **Base Profile** to `USBOptimized`, you can set the keyboard entry mode for the password in the **Advanced** menu on the phone.

Change the Administrator Password on the Phone Menu

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

Task

- 1 On the phone, go to **Settings > Advanced** and enter the current administrator password.
- 2 Select **Change Admin Password**.
- 3 Enter the current password, enter a new password, and confirm the new password.
Passwords can contain uppercase and lowercase letters, numerals, and special characters (!, #, %, \$, etc.).
Passwords cannot contain non-ASCII characters (ã, ç, ë, etc.) or chevrons (<, >).

Change the User Password on the System

You can change the user password at any time from the **Advanced** settings menu.

Task

- 1 On the phone, go to **Settings > Advanced**.
- 2 Enter your user password and select **Enter**.
- 3 Select **Change User Password**.
- 4 On the **Change User Password** screen, enter your old and new user password and select **Enter**.
Passwords can contain uppercase and lowercase letters, numerals, and special characters (!, #, %, \$, etc.).

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

Change the Administrator Password in the System Web Interface

You can change the administrator password on a per-phone basis using the system web interface.

If the default administrator password is in use, you can't use the system web interface.

Task

- 1 Enter your phone's IP address into a web browser.
- 2 Select **Admin** as the login type, enter the administrator password, and click **Submit**.
- 3 Select **Settings > Change Password**.
- 4 Select **Admin**.
- 5 Enter the current password into the **Old Password** field.

- 6 Enter the **New Password** and confirm it.

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

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

- 7 Select **Save**.

Change the User Password in the System Web Interface

You can change the user password on a per-phone basis using the system web interface.

Task

- 1 Enter your phone's IP address into a web browser.
- 2 Select **Admin** as the login type, enter the administrator password, and click **Submit**.
- 3 Select **Settings > Change Password**.
- 4 Select **User**.
- 5 Enter the **New Password** and confirm it.

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

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

- 6 Select **Save**.

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.

2 (default)

0 - 32

Change causes system to restart or reboot.

up.echoPasswordDigits

1 (default) - The phone briefly displays password characters before masking them with 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.

California SB-327 Password Requirement Compliance

Poly Trio C60 phones meet California SB-327 password mandates that require administrators to generate a new password before granting access to the system and the system web interface.

Note: You can't use the default password as the newly generated password. If your phone uses the default administrator password, the system requires you to change it.

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

-1 - Disabled

0 - Auto (default)

1 - 10HD

2 - 10FD

3 - 100HD

4 - 100FD

5 - 1000FD

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 a Top Secret classification level.

Note: Call classification is determined by the lowest classification 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

Polycom phones can download encrypted files from the provisioning server and encrypt files before uploading them to the provisioning server.

You can encrypt all configuration files except the master configuration file, contact directory files, and configuration override 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. You cannot encrypt the master configuration file.

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. Polycom 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.

You must update the files on the server to the new key or make the files available in unencrypted format. Updating to the new key requires that you decrypt the files with the old key, then re-encrypt it with the new key.

Task

- 1 Place all encrypted configuration files that you want to use with the new key on the provisioning server. The phone may reboot multiple times.
- 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.

Note: You may need to update configuration files, contact directory files, and configuration override files if they were already encrypted. You can delete configuration override files from the provisioning server so that the phone replaces them when it successfully boots.

The phone automatically reboots another time to use the new key.

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

VoSIP Parameter

The following table lists parameters to configure VoSIP.

reg.X.rfc3329MediaSec.enable

0 (default) - 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.

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) - Enabled

0 - Disabled

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) - Enabled

0 - Disabled

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 primary key lifetime is not set.

Positive integer minimum 1024 or power of 2 notation - The primary 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.

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.AES_ICM_256

0 (default) - The system doesn't accept or offer AES_256_CM_HMAC_SHA1_80 encryption.

1 - The system includes the AES_256_CM_HMAC_SHA1_80 crypto suite in SRTP offers, and accepts it when offered in SIP calls.

Change causes system to restart or reboot.

sec.srtp.offer.AES_GCM_256

0 (default) - The system doesn't accept or offer AEAD_AES_256_GCM encryption.

1 - The system includes the AEAD_AES_256_GCM crypto suite in SRTP offers, and accepts it when offered in SIP calls.

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.

reg.x.secureTransportRequired

0 (Default) - The phones register based on the transport priority received in the DNS response.

1 - The phones register only on the TLS transport in the DNS response if the transport is configured as DNSNaptr.

If the transport is configured as TLSOnly, then the phone registers to the configured SIP server. The phone doesn't register if the transport is either TCP or UDP.

Enabling Users to Lock Phones

This feature enables 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.

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.enabled

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. Poly 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 Poly phones.

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

Polycom 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 standard IEEE 802.

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

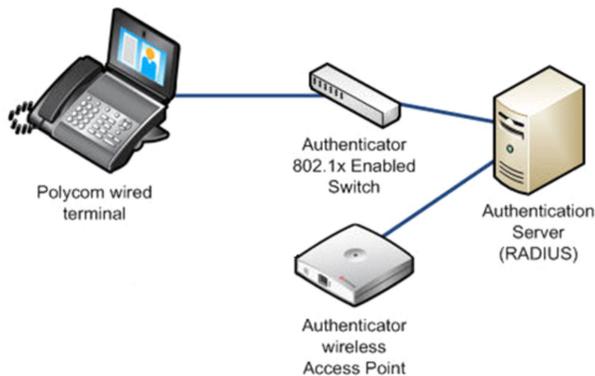


Figure 1: A typical 802.1X network configuration

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 - Disabled

1 - Enabled

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 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

Simple Certificate Enrollment Protocol

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

Simple Certificate Enrollment Protocol Parameters

Use the following parameters to configure Simple Certificate Enrollment Protocol (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 seconds (default)

28800 - 259200 seconds

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.

Note: If you use the default setting, the phone uses its own MAC address for the CN value in the generated CSR.

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.locality

Specify the phone's locality (L) to use for CSR generation.

null (default)

0-64 characters

SCEP.csr.organization

Specify the organization name to use for CSR generation.

null (default)

0 - 64

SCEP.csr.organizationUnit

Specify the phone's organizational unit (OU) to use for CSR generation.

null (default)

0-64 characters

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 enrollment process in case of enrollment failure.

12 (default)

1 - 24

SCEP.enrollment.retryInterval

Specify the time interval to retry the enrollment 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

SCEP.verifyWithScepCaCert

Connect to the SCEP server with TLS verified with a CA cert provided by the server.

1 (default)

0 - Use settings from TLS Provisioning Profile.

Session Management on the System Web Interface

You can use the Session Management on the system web interface to enhance phone security by setting the maximum number of sessions and determining session validity.

If you change the password, all the existing sessions expire and you must log in with the new password. If a session reaches the maximum limit, all existing sessions expire and the new session continues on the system web interface.

Note: If you aren't able to log in to the system web interface, clear your web browser cookies and try again.

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.

General Security Parameters

Use the following parameters to configure security features of the phone.

sec.tagSerialNo

Enable to include the phone's serial number (MAC address) in application layer HTTP GET request headers and SIP contact headers.

0 (default) - The phone doesn't provide the serial number (MAC address).

1 - The phone provides the serial number (MAC address).

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 isn't uploaded to the provisioning server.

1 - The device private key is uploaded to the 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.

DNS Parameters

Use the following parameters to set the DNS.

The values you set using DHCP have a higher priority, and the values you 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)

String

Change causes system to restart or reboot.

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.

Note: If the DHCP server doesn't send the DNS server addresses to the phone, then the values set for the `device.dns.serverAddress` and `device.dns.altSrvAddress` parameters are used. Alternatively, the phone uses the DNS server addresses set using the `tcpIpApp*` parameters, which override `device.dns.*` parameters.

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` parameter.

Change causes system to restart or reboot.

Note: If the DHCP server doesn't send the DNS domain to the phone, then the value set for `device.dns.domain` is used. Alternatively, the phone uses the DNS domain set using the `tcpIpApp*` parameter, which overrides `device.dns.*` parameter.

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.enable1

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.

Network

Polycom UC software enables you to make custom network configurations.

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.

Poly Trio C Series System and Model Names

Model	System Name	Model Name
Poly Trio C60	Poly Trio C60	Poly Trio-Trio_C60

Two-Way Active Measurement Protocol

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

0 (default) - Disable TWAMP protocol support.

1 - Enable TWAMP protocol support.

twamp.port.udp.PortRangeEnd

Set the TWAMP UDP session max port range value.

60000 (default)

1024 - 65486

twamp.port.udp.PortRangeStart

Set the TWAMP UDP session start port range value.

40000 (default)

1024 - 65485

twamp.udp.maxSession

Set the maximum UDP session supported by TWAMP.

1 (default)

1 - 10

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 expiration dates 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 the following parameters.

device.icmp.ipv4IcmpIgnoreRedirect.set

0 (default) - The phone doesn't allow you to use the `device.icmp.ipv4IcmpIgnoreRedirect` parameter to configure Enhanced IPv4 ICMP Management feature.

1 - The phone allows you to use the `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 `sipId` 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 phones 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.

- 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

Use the following parameter to enable a SIP instance on a registered line.

reg.x.gruu

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.

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@poly.com) of the registration SIP URI.

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, 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 doesn't accept 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 reregister 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 doesn't 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't 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 [Poly 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.

DNSnaptr (default) - If `reg.x.server.y.address` is a `<hostname>` and `reg.x.server.y.port` is 0 or Null, perform NAPTR then SRV lookups to try to discover the transport, ports, and servers, as per RFC 3263.

If `reg.x.server.y.address` is an IP address or if you provide a port, then the phone uses UDP.

TCPpreferred

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](https://www.rfc-editor.org/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](#).

0 (default)

0 to 65535

dns.cache.SRV.x.priority

The priority of this target host. For more information, see [RFC 2782](#).

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](#).

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 (2²⁹), 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.

Note: If the DHCP server doesn't send the DNS server addresses to the phone, then the values set for the `device.dns.serverAddress` and `device.dns.altSrvAddress` parameters are used.

Alternatively, the phone uses the DNS server addresses set using the `tcpIpApp*` parameters, which override `device.dns.*` parameters.

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` parameter.

Change causes system to restart or reboot.

Note: If the DHCP server doesn't send the DNS domain to the phone, then the value set for `device.dns.domain` is used. Alternatively, the phone uses the DNS domain set using the `tcpIpApp*` parameter, which overrides `device.dns.*` parameter.

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.queryRetryCount

Defines the number of retries the phone attempts before it restores the cache using the `dns.queryRetryCount` parameter.

0 to 48 - The number of retries that the phone attempts before the cache is restored.

0 - Disable.

4 (default)

Note: Requires `dns.cache.dynamicRestore.enable` to be enabled.

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.

voIpProt.SIP.naptrAllowDuplicateTransport.enable

0 (Default) - The system ignores NAPTR records with duplicate protocols.

1 - The system considers all NAPTR records, regardless of transport, up to a maximum of 16 records.

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 UC Software in the order listed.

When the static DNS cache is not used, the `site.cfg` configuration looks as follows:

reg	
reg.1.address	1001
reg.1.server.1.address	172.23.0.140
reg.1.server.1.port	5075
reg.1.server.1.transport	UDPOnly
reg.1.server.2.address	172.23.0.150
reg.1.server.2.port	5075
reg.1.server.2.transport	UDPOnly

When the static DNS cache is used, the `site.cfg` configuration looks as follows:

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

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](https://tools.ietf.org/html/rfc3263).

When the static DNS cache is not used, the `site.cfg` configuration looks as follows:

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

When the static DNS cache is used, the `site.cfg` configuration looks as follows:

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

Note: 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:

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

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

When the static DNS cache is used, the `site.cfg` configuration looks as follows:

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

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.

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 sub-domains 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

Configure phones at the customer site.

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)

To connect an outgoing call, the phone calls the working server. If the server does not respond to INVITE, the phone tries again with the next available server until the call connects or fails.

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

Note: The concurrent failover/fallback feature 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.

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.

reg.x.outboundProxy.failOver.failBack.mode

The mode for failover fallback (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 you configured for the server 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 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.

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`.

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 `device.wifi.country` parameter before enabling Wi-Fi.

You can configure Wi-Fi options to display in the phone's basic settings menu to enable 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 can't 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 don't 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 C60 systems 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. Poly Trio systems supports the following Wi-Fi security modes:

- WEP
- WPA PSK
- WPA2 PSK
- WPA2 Enterprise

`device.wifi.country`

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) - Disable

1 - Enable

device.wifi.enabled

Enable or disable Wi-Fi.

0 (default) - Disable

1 - Enable

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.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.

Task

- 1 Go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu**, and turn Wi-Fi to **On**.
The phone reboots.
- 2 After the phone restarts, go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu** to view available networks.
- 3 Select a network and press **Connect**.

Configure Wireless Network Settings with EAP

You can manually configure the phone to connect to a wireless network by selecting an enterprise- based network and EAP method for better security.

Task

- 1 Go to **Settings > Advanced > Administrator Settings > Network Configuration > Network Interfaces > Wi-Fi Menu**.
- 2 Turn Wi-Fi to **On**.
The phone reboots.
- 3 After the phone reboots, go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu** to view available networks.
- 4 Configure the following wireless network settings:

- A Select the SSID name of the wireless network.
- B Select the security type of the wireless network.
- C Optional: If you have an enterprise-based network, enter the **User ID** and **Password**.
- D 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

5 Select a network and press **Connect**.

Wi-Fi Settings in Basic Menu Parameter

Use the parameter below to allow access to Wi-Fi settings in the Basic menu.

feature.basicWifiMenu.enabled

Enable to allow access to Wi-fi Menu in Basic settings.

0 (default) - Disabled

1 - Enabled

Related Links

[Wi-Fi Settings in Basic Menu Parameter](#) on page 206

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.

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. When your device is connected over Bluetooth during an audio call, you can use the Poly Trio system microphones for audio instead of the microphone(s) of your connected device. The Poly Trio phones can remember up to 10 previously paired devices.

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 Parameters

Use the following parameters to configure Bluetooth on Poly Trio systems.

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.audio.enabled

Set to enable or disable audio playback through a Bluetooth connection.

0 - Bluetooth device audio is disabled.

1 (default) - Bluetooth device audio is enabled.

Note: This feature can also be controlled from the Poly Trio system user interface.

bluetooth.device.discoverable

1 (default) - This device is discoverable for Bluetooth pairing.

0 - This device is not discoverable for Bluetooth pairing.

bluetooth.device.maxPaired

Set the limit for the maximum number of Bluetooth devices that can be paired with a Poly Trio system.

10 (default)

0 - 10

bluetooth.device.name

NULL (default)

UTF-8 string

Enter the name of the device that broadcasts over Bluetooth to other devices.

bluetooth.device.pairedTimeout

Set the timeout limit for automatically unpairing Bluetooth devices when

`bluetooth.device.maxPaired` is set to 0.

30 (default)

30 - 1800 (in minutes)

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.

Web Proxy

A web proxy can help your Poly phone securely communicate outside your network with increased performance. For example, you can direct your phone's outbound requests through an enterprise proxy.

You can configure your system to use a proxy in one of the following ways:

- **Automatic:** You can specify only the proxy credentials (if needed). Using DHCP or DNS-A, your system obtains a URL to automatically download a proxy auto-configuration (PAC) file.
- **Manual:** You can specify the proxy address and port or the PAC URL.
- **Disabled:** You can't configure web proxy settings.

Note: Web proxy authentication is not supported for Microsoft Teams and Zoom base profiles.

PAC File Search Priority

When using automatic web proxy discovery, you can configure Poly phones to discover the Proxy Auto-Configuration (PAC) file location on your provisioning server (using DHCP Option 252) or using the DNS-A protocol mechanism.

Poly phones search for PAC files in the following priority order.:

- 1 **Provisioning server:** For example, `feature.wpad.url="http://server.domain.com/proxy.pac`
- 2 **DHCP Option 252:** For instructions, see *Creating an Option 252 entry in DHCP* at [Microsoft TechNet](#).
- 3 **DNS-A:** For instructions, see *Creating a WPAD entry in DNS* at [Microsoft TechNet](#).

When using a provisioning server or DHCP, the phone looks for the file name you specify. If using DNS-A, the phone looks only for the `wpad.dat` file.

If your configuration includes automatically downloading a PAC file, there must be an expiration associated with the file so the system knows when to download a new one. Make sure your PAC file server includes an `Expires` header in its HTTP response (for example, `Expires: Wed, 30 Oct 2016 09:30:00 GMT`).

Supported HTTP/HTTPS Web Proxy Services

When you successfully configure the web proxy server, Poly phones route specific HTTP and HTTPS services to the web proxy server.

The phones route the following services to the web proxy server:

Generic Services

- HTTP/HTTPS provisioning
- Core file upload

Skype for Business Services

- Registration services
- Address Book Service (ABS)
- Location Information Server (LIS)
- Device update (To ensure reliable software updates, device update is direct in case a proxy is not available.)
- Server log upload
- Exchange web services

Configure Web Proxy Settings in the Local Interface

You can enable web proxy from the Poly Trio C60 local interface and choose the configuration method. Poly recommends this method when configuring a single phone or a small set of phones.

You can choose to enable and configure web proxy using the following methods:

- **Auto:** Specify the proxy credentials. Using DHCP or DNS-A, the Poly Trio system obtains a URL to automatically download a proxy auto-configuration (PAC) file.
- **Manual:** Specify the proxy server address, port, and credentials or the proxy PAC URL.

Task

- 1 Go to **Settings > Administration Settings > Network Configuration > Network Interfaces**.
- 2 Select **Web Proxy** and choose a web proxy method.
- 3 Enter the web proxy information into the appropriate fields.

Configure Web Proxy Access Manually

Manually configure web proxy access for Poly phones that can't use automatic web proxy discovery.

Task

- 1 Set the parameter `feature.wpad.enabled` to 1.
- 2 Enter the web proxy server address for the parameter `feature.wpad.proxy`.

Configure Proxy-Specific Credentials for Users

Poly phones support digest and NTLM authentication mechanisms to authenticate with a proxy server. This enables you to manually configure proxy-specific credentials common to all users using basic authentication.

Task

- » Configure the following parameters on a provisioning server:
 - `feature.wpad.proxy.username`
 - `feature.wpad.proxy.password`

View Web Proxy Diagnostics on the System Web Interface

When you successfully configure the web proxy server, you can access important diagnostic information from the system web interface (Web Configuration Utility) to track HTTP and HTTPS traffic flowing via the configured web proxy.

From the system web interface, you can download the PAC file and view the following diagnostic information on a per-phone basis:

- PAC file fetch status
- Configured method used to fetch the PAC file and source URLs
- DNS domain, if configured
- PAC file expiry details
- Exchange and upload proxy

Task

- 1 Enter your phone's IP address into a web browser.
- 2 Select **Admin** as the login type, enter the administrator password, and select **Submit**.
- 3 Go to **Diagnostics > Web Proxy Auto Discovery (WPAD)**.

Web Proxy Configuration Parameters

The following parameters configure web proxy settings.

feature.wpad.enabled

Set to enable web proxy.

0 (default) - Disables web proxy.

1 - Enables web proxy. Default for the Skype Base Profile.

Change causes system to restart or reboot.

feature.wpad.curl

Enter the PAC file location.

Change causes system to restart or reboot.

feature.wpad.proxy

Configure the web proxy server address. If you configure this parameter with a proxy address, the phones don't discover DHCP or DNS-A or fetch the PAC file even if you configure a PAC file location using `feature.wpad.curl`.

0 to 255 characters

Change causes system to restart or reboot.

feature.wpad.proxy.username

Enter the user name to authenticate with the proxy server.

0 to 255 characters

Change causes system to restart or reboot.

feature.wpad.proxy.password

Enter the password to authenticate with the proxy server.

The credentials you can use depend on how authentication is enabled on the proxy server. You can use administrator or user credentials. If Skype for Business Active Directory is integrated with the proxy server, you don't need to configure user name or password credentials.

0 to 255 characters

Change causes system to restart or reboot.

User Profiles

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 useful for remote and mobile workers who don't 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, users can do the following:

- Log in to a phone to access their personal phone settings using their user ID and password.
- Place a call to an authorized number from a phone that is logged out.
- 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 corresponding user options are cleared from the device until the user profile related configuration is enabled on the phone again.

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 can't 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.hash

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 doesn't 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 isn't logged out and the phone returns to the user profile after reboot.

If a user isn't logged out from a phone and other users aren't 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`.

User Profile Authentication

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.

User Profile Server Authentication

Instead of phone-based authentication of user profiles, you can authenticate user profiles using a server.

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 isn't logged into the phone.

If you enable server authentication of user profiles, the following parameters don't apply and you don't need to configure them:

- `prov.login.defaultUser`
- `prov.login.defaultPassword`
- `prov.login.defaultOnly`
- `prov.login.localPassword`
- `prov.login.localPassword.hash`

Task

- 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: If you enable `prov.login.enabled=1` and don't 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 primary 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**.

The following override files upload to the generic profile directory:

- Log files
- Local interface settings
- System web interface settings
- Call logs
- Contact directory file

Create 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.

Task

- 1 On the server, create an account and a directory for each user (for example, `User1` and `User2`).
- 2 In each user directory, create a configuration file for each user (for example, `User1.cfg` and `User2.cfg`), that contains the user's registration details and feature settings.

The following override files upload to the generic profile account on the server:

- Log files
- System web interface settings

The following override files upload to the user profile account on the server:

- Local interface settings
- Contact directory file

User Profile Phone Authentication

You can create default credentials and authenticate user profiles without using a server.

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.

Task

- 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.

Some things to note about user configuration files:

- 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 list shows configuration parameter precedence (from first to last) for a phone with the user profile feature enabled:

- 1 `<user>-phone.cfg`
- 2 System web interface
- 3 Configuration files listed in the primary configuration file (including `<user>.cfg`)

4 Default values

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.

Task

1 On the provisioning server, create a user configuration file for each user. Specify the user's login ID in the name of the file.

For example, if the user's login ID is user100, name the user configuration file user100.cfg

2 In each <user>.cfg file, you must add and set values for the user's login password.

3 Optional: Add and set values for any user-specific parameters you want to add:

- Registration details, such as the number of lines the profile displays and line labels
- Feature settings, such as microbrowser settings

Caution: If you add optional user-specific parameters to <user>.cfg, only add parameters that don't cause the phone to restart or reboot when the parameter is updated.

Third-Party Servers

This section provides information on configuring phones and features with third-party servers.

Cisco BroadWorks Server

Poly devices support many Cisco BroadWorks Server feature options, including BroadWorks Anywhere, UC-One, flexible seating, and hoteling.

Refer to the *Cisco BroadWorks Partner Configuration Guide* for more information on configuring features on the Cisco BroadWorks server. Contact your Poly account team for information on where to access the guide.

Authentication with Cisco BroadWorks XSP Service Interface

Some Cisco BroadWorks server features require you to authenticate Poly phones with the Cisco BroadWorks Xtended Service Platform (XSP) service interface. The authentication method you use depends on which version of the BroadWorks server you are running.

Authentication for BroadWorks XSP Parameters

Use these parameters for authenticate Poly phones with BroadWorks server.

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.

UC-One Integration

Configure your phones to integrate with Cisco BroadWorks Enterprise Directory and BroadCloud services to enable users to access directories, share presence, and use call features on Poly phones.

UC-One integration on Poly phones enables users to:

- Access the BroadWorks Directory
- Search for contacts in BroadWorks Directory
- View UC-One contacts and groups
- View the presence status of UC-One contacts
- View and filter UC-One contacts
- Activate and control 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 the BroadSoft UC-One Application

Configure the Polycom BroadSoft UC-One Call Settings menu and feature options on the phone, in the Web Configuration Utility, and using configuration parameters.

Enable the BroadSoft UC-One Application from the Local Interface

Enable the BroadSoft UC-One menu directly from the phone's local interface.

Task

- 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

Enable the BroadSoft UC-One feature and feature options in the Web Configuration Utility.

Task

- 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.

Task

- 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

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 for their desk phone, mobile phone, or home office phone. Users can also move calls between phones and perform phone functions from any phone in their locations list.

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.

If you enable server-based call forwarding but it's inactive, the moving arrow icon doesn't display and the phone doesn't forward incoming calls when a user presses the **Forward** softkey.

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

Microsoft Exchange Integration

If you have a Skype for Business, Office 365, or Lync Server 2013 deployment, you can integrate with Microsoft Exchange Server.

After you connect phones with the Exchange Server, you can do the following:

- Verify the status of Exchange Server services on each phone
- View the status of each service in the system web interface

Integrating with Microsoft Exchange

The phone offers several methods to integrate with Microsoft Exchange.

Use one of the following methods:

- Exchange Server auto-discover
- Provision the phone with the Microsoft Exchange address
- System web interface

Provision the Microsoft Exchange Calendar

You can provision your systems with the Microsoft Exchange calendar.

When you connect a Poly Trio system to 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 that displays the day and meeting view for scheduled events. Users can't schedule calendar events or view email from the phone.

Task

- » 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 System Web Interface

You can use the system web interface to manually enable your phones with the Microsoft Exchange calendar. This option is useful for troubleshooting faulty auto-discovery.

You can enable the Microsoft Exchange calendar through the system web interface for only one phone at a time.

Task

- 1 Log in to the system web interface using admin credentials.
- 2 Go to **Settings > Applications > Exchange Applications**.
- 3 In the **Exchange Calendar** field, select **Enable**.
- 4 Enter the exchange web services URL using a Microsoft Exchange Server URL.
For example `https://<mail.com>/ews/exchange.asmx`.
- 5 Select **Save**.
- 6 Select **Yes**.

The Calendar icon displays on your phone screen.

Calendar Meeting Details

You can use the `exchange.meeting.show*` parameters to show or hide the following meeting details from the calendar display on the Poly Trio system screen:

- Subject
- Location
- Invitee(s)
- Agenda/Notes - When you hide Agenda/Notes, a message indicates the meeting is private.
- Meeting Organizer - The organizer doesn't display for meetings displayed on the monitor.
- Show More Actions - If users can dial multiple numbers to join a meeting, the **Show More Actions** option displays in **Meeting Details** to enable users to choose the dial-in number.

Meeting Reminder Messages

Poly Trio systems display several meeting reminder messages.

A meeting reminder displays on the system screen at 5 minutes and 1 minute before the start of a meeting. The five-minute reminder disappears after 30 seconds if you don't dismiss it. If you don't dismiss the one-minute reminder, 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 a time slot contains multiple meetings due to scheduling overlap, the meeting reminder message displays all available meetings. Users can select 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 monitors 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

Verify that all of the Exchange services work properly.

Task

- » Do one of the following:
 - On the phone's local interface, go to **Settings > Status > Diagnostics > Warnings**.

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 at [Poly Trio Support](#).

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 isn't currently available. Users can't schedule calendar events or view email from the phone.

Private Meetings in Microsoft Exchange

When you set a Skype for Business meeting 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 don't 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 don't 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 don't 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 don't 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 don't 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 don't display the name of the meeting organizer on the Poly Trio calendar.

exchange.meeting.private.enabled

- 1 (default) - The Poly Trio system 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 use Microsoft Exchange services on your phones.

Visual Voicemail

On the Exchange Server, enable unified messaging and enable messages to play on the phone for each user.

Synchronizing Call Logs

On the Exchange Server, you can enable the option to save calls logs to each user's conversation history in Outlook.

ABS Adaptive Search

You can enable the Address Book Service (ABS) 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.

Phones 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.

All (default)

Location

LocationAndSubject

Description

Change causes a reboot.

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 or an asterisk(*) 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

Set the interval at which phones display reminder messages.

300 seconds (default)

60 - 900 seconds

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 milliseconds, 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`.

1 (default) - Exchange autodiscovery is enabled and the phone automatically discovers the Exchange server using the email address information.

0 - Exchange autodiscovery is disabled on the phone and you must manually configure the Exchange server address.

feature.exchangeCalendar.enabled

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.

`exchange.multipleCalendarEvents.enabled`

1 (default) - Multiple calendar events display if at least two events begin within 15 minutes of each other.

0 - Only the next calendar event displays.

`feature.exchangeContacts.enabled`

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`

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`

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. Do not disable 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.oneTouchVoiceMail1

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.

The following list includes dial-in options that present a **Join** button in meeting reminders:

- SIP URI
- Tel URI
- PSTN number
- IP dial

Meeting 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

Select a meeting invite field to fetch a VMR or meeting number from.

All (default)

Location

LocationAndSubject

Description

Change causes a reboot.

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)

Exchange Impersonation for Calendaring

You can configure your phone to support Exchange Impersonation, which grants your Trio C60 access to other calendars through a single service account. Only the service account needs to log in on the system.

The system accesses and displays the calendar associated with the Exchange account you enter in the `exchange.targetMailbox` parameter.

Configure a Separate Calendar with a Service Account

To display a separate calendar on the Trio C60 without logging that account into the system, configure Exchange Impersonation for calendaring. Using the parameters listed below, enter the login credentials for the service account and the account sign-in address for the Exchange calendars you want to display.

Task

- » Set the following parameter values:
 - `exchange.showSeparateAuth = "1"`
 - `exchange.auth.email = "<service account sign-in address>"`
 - `device.loginAltCred.user = "<service account user ID>"`
 - `device.loginAltCred.password = "<service account password>"`
 - `device.loginAltCred.domain = "<domain name>"`
 - `exchange.targetMailbox = "<calendaring account sign-in address>"`
 - `device.loginAltCred.domain.set = "1"`
 - `device.loginAltCred.user.set = "1"`
 - `device.loginAltCred.password.set = "1"`

Exchange Impersonation for Calendaring Parameter

When you configure Exchange Impersonation for calendaring, enter the Exchange account whose calendar should display on the Trio C60 into the parameter below.

exchange.targetMailbox

This parameter configures the calendaring Exchange account sign-in address.

NULL (default) - The calendar for the account entered in `exchange.auth.email` displays on the Poly Trio system.

String (maximum of 255 characters) - The calendar for the entered Exchange account displays on the Poly Trio system.

Basic Authentication for One Touch Dial Exchange Services

You can require only basic authentication to allow the Poly Trio system to use One Touch Dialing (OTD) exchange services. When you use basic authentication for OTD services, the header contains the user name and password encoded in Base64 format.

Caution: When basic authentication is used with HTTP, user login information can be exposed to a middleman during the authentication process. When possible, Poly recommends using advanced authentication for OTD exchange services.

Basic Authentication for One Touch Dial Exchange Parameter

Use the following parameter to allow basic authentication for One Touch Dial exchange services.

feature.exchange.allowBasicAuth

Set to determine whether One Touch Dial (OTD) Exchange services use basic authentication.

0 (default) - OTD Exchange services do not use basic authentication.

1 - OTD Exchange services use basic authentication.

Change causes system to restart or reboot.

Cisco Webex

This section shows you how to connect Poly devices with Cisco Webex services.

Configure Direct Dial to Cisco Webex Meetings

You can enable users to join Cisco Webex meetings directly from the calendar events on the Poly Trio system.

This configuration allows direct dialing to Cisco Webex meetings. Once configured, users can join Cisco Webex meetings by selecting **Join** right on the Poly Trio system touchscreen.

Note: Poly Trio systems don't support Webex interactive voice responses (IVR) when direct dialing to Webex meetings.

Task

- 1 Configure the following parameters:

```
feature.fecc.enabled = "0"  
feature.nat.stun.enabled = "1"
```

- 2 Configure the STUN server using the following parameters:

```
nat.stun.server = <STUN Server Address>  
nat.stun.port = <STUN Port Number>
```

- 3 Enable the local directory feature, which is required in environments where Skype for Business is on a registered line:

```
feature.directory.enabled = "1"
```

- 4 Configure the Poly Trio system's Click-To-Join for Cisco Webex meetings with the following:

```
call.teluri.showPrompt = "0"  
feature.exchangeCalendar.enabled = "1"  
exchange.meeting.parseEmailsAsSipUris = "1"  
exchange.meeting.parseOption = "All"
```

- 5 Append "webex.com" to the exchange.meeting.parseAllowedSipUriDomains parameter:

```
exchange.meeting.parseAllowedSipUriDomains = webex.com
```

- 6 Configure video codec preferences for interoperability with Cisco Webex meetings:

```
video.codecPref.H264 = "2"  
video.codecPref.H264.packetizationMode0 = "3"  
video.codecPref.H264HP = "4"  
video.codecPref.H264HP.packetizationMode0 = "5"
```

- 7 Set the the NAT transversal mode to STUN. Replace x with the desired line key value.

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

- 8 Set the following for the specific Poly Trio system. Replace x in each parameter with the desired line key value as applicable.

```
reg.x.address = <SIP URI address>  
reg.x.label = <Line key registration label>  
reg.x.displayName = <System SIP signaling display name>
```

- 9 Configure Cisco Webex tenancy subdomain. Replace x with the desired line key value.

```
reg.x.server.1.address = <Domain address>
```

- 10 Set the following for interoperability. Replace x in each parameter with the desired line key value as applicable.

```
reg.x.keepalive.sessionTimers = "1"  
reg.x.server.1.register = "0"  
reg.x.server.1.transport = "TLS"  
reg.x.srtplib.offer = "1"  
tcpIpApp.keepalive.tcp.sip.tls.enable = "1"  
dialplan.applyToDirectoryDial = "1"  
dialplan.digitmap.lineSwitching.enable = "1"  
dialplan.x.applyToDirectoryDial = "1"  
dialplan.x.digitmap = "^.\.webex\.com$"  
dialplan.x.digitmap.mode = "regex"
```

Configuration Parameters

This section is a reference for configuration parameters available for PVOS features.

Quick Setup Soft Key Parameter

Use the following parameter to configure the **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.

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 you set to a ring class with a type other than `answer` or `ring-answer`, the settings 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)

1

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 doesn't 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 doesn't 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 you set `call.stickyAutoLineSeize` to 1, this parameter has no effect. The regular `stickyAutoLineSeize` behavior is followed.

If you set `call.stickyAutoLineSeize` to 0 and set this parameter to 1, this overrides the `stickyAutoLineSeize` behavior for hot dial only. (Any new call scenario seizes the next available line.)

If you set `call.stickyAutoLineSeize` to 0 and set this parameter 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 doesn't display the pop-up box.

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) - The phone generates a core file.

0 - The phone doesn't generate a core file.

Change causes system to restart or reboot.

diags.pcap.enabled

Enable or disable all on-board packet capture features.

0 (default) - Disable on-board packet capture features.

1 - Enable on-board packet capture features.

diags.pcap.remote.enabled

Enable or disable the remote packet capture server.

0 (default) - Disable the remote packet capture server.

1 - Enable the remote packet capture server.

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.

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

Set the time, in seconds, the phone waits for digit input before placing a call when the phone is onhook.

Note: The default value varies depending on the setting for the `device.baseProfile` setting.

Generic (default) - 0

Lync (default) - 4

0-99 seconds

You can apply `dialplan.userDial.timeOut` only when its value is lower than `up.IdleTimeOut`.

dialplan.x.applyToCallListDial

Note: The default value varies depending on the setting for the `device.baseProfile` setting.

Generic (default) - 0

Lync (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

0 (default) - 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

0 (default) - The dial plan applies to forwarded calls for this line.

1 - The dial plan applies to forwarded calls for this line.

dialplan.x.applyToTelUriDial

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

Note: The default value varies depending on the setting for the `device.baseProfile` setting.

Selects the dialplan based on more than one match with the least timeout.

Generic (default) - 0

Lync (default) - 1

0 - Conflict match handling is disabled.

1 - Conflict match handling is enabled.

dialplan.x.digitmap.timeOut

Set the time, in seconds, the phone waits for digit input before placing a call when the phone is offhook.

Note: The default value varies depending on the setting for the `device.baseProfile` setting.

Generic (default) - Null

Lync (default) - 4

0-100 seconds

Change causes system to restart or reboot.

dialplan.x.digitmap

Note: The default value varies depending on the setting for the `device.baseProfile` setting.

Generic (default) - Null

Lync (default) - 4

string - max number of characters 100

Change causes system to restart or reboot.

dialplan.x.digitmap.mode

Specify whether a dial plan uses Poly digit map rules or regular expressions (regex) to manage line switching.

digitmap (default) - The dial plan uses a digit map defined in `dialplan.x.digitmap` to manage line switching.

regex - The dial plan uses regular expression rules defined in `dialplan.x.digitmap` to manage line switching.

Note: Poly Trio systems don't support dial-string manipulation using regex at this time.

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.

dialplan.x.originaldigitmap

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. 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 - 100 KB

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 - 200 KB

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

Element	Definition	Permitted Values
<code>fn</code>	The contact's first name	UTF-8 encoded string of up to 40 bytes ¹
<code>ln</code>	The contact's last name	UTF-8 encoded string of up to 40 bytes ¹
<code>ct</code>	Contact Used by the phone to address a remote party in the same way that a user manually dials a string of digits or a SIP URL. Also used to associate incoming callers with a particular directory entry. The maximum field length is 128 characters. Note: You can't duplicate this field or leave it <code>Null</code> .	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL
<code>sd</code>	Speed Dial Index Associates a particular entry with a speed dial key for one-touch dialing or dialing.	Null, 1 to 20
<code>lb</code>	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 <code>Null</code> , then the first and last names form the label. A space is added between first and last names.	UTF-8 encoded string of up to 40 bytes ¹
<code>pt</code>	Protocol The protocol to use when placing a call to this contact.	SIP or Unspecified

Element	Definition	Permitted Values
rt	Ring Tone When incoming calls match a directory entry, this field specifies the ringtone to use.	Null, 1 to 21
dc	Divert Contact The address to forward calls to if the Auto Divert feature is enabled.	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL
ad	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.	0 or 1
ar	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.	0 or 1
bw	Buddy Watching If set to 1, this contact is added to the list of watched phones.	0 or 1
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 set by the icons.x parameter.	1-24

Feature Activation and 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 dialog showing call information details. The dialog closes after 40 seconds, or you can press **Exit** to close it and return to the active call screen. You can set how long the dialog 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.computeraudioconnector.enabled

0 (default) - Disable the computer audio connector feature.

1 - Enable the computer audio connector feature.

feature.flexibleLineKey.enable

0 (default) - Disables the Flexible Line Key feature.

1 - Enables the Flexible Line Key feature.

feature.lclConferenceDtmfRelay.enabled

0 (default) - Relay DTMF received by the host on one leg to another.

1 - Do not relay DTMF received by the host on one leg to another.

feature.nfc.enabled

0 - Disable NFC.

1 (default) - Enable NFC.

feature.photoIntegration.enable

0 - Disable photo integration feature.

1 (default) - Enable photo integration 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 Computer Connections option doesn't 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 system web interface server for user and administrator features.

The web server supports both basic and digest authentication. You can't configure the authentication user name and password.

httpd.enabled

Base Profile = Generic

1 (default) - The web server is enabled.

0 - The web server is disabled.

Change causes system to restart or reboot.

httpd.cfg.enabled

Base Profile = Generic

1 (default) - The system web interface is enabled.

0 - The system web interface is disabled.

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 system web interface is allowed only over a secure tunnel (HTTPS) and non-secure (HTTP) is not allowed.

0 - Access to the system web interface 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 you install a license on a phone, you can't remove it.

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.

Poly phones support three chord sets. Each chord set has different chord names, represented by x in the following parameters.

- callProg, where x can be one of the following chord names:

- dialTone
- busyTone
- ringback
- reorder
- stutter_3
- callWaiting
- callWaitingLong
- howler
- recWarning
- stutterLong
- intercom
- callWaitingLong
- precedenceCallWaiting
- preemption
- precedenceRingback

- spare1 to spare6
- misc, where x can be one of the following chord names:
 - spare1 to spare9
 - cs1 to cs12
- ringer, where x can be one of the following chord names:
 - 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 Flexible Call Appearances section under the column "Registrations."

msg.bypassInstantMessage

0 (default) - Displays the **Message Center** and **Instant Messages** menus when a user presses the **Messages** or **MSG** key.

1 - Bypasses the menus and goes to voicemail.

msg.mwi.x.led

1 (default) - The LED flashes as long as the phone has new unread voicemail messages for any line.

0 - Red MWI LED doesn't flash when there are new unread messages for the selected line.

x is an integer referring to the registration indexed by `reg.x`.

mwi.sharedLineIcon.enable

1 (default) - Shows that the message waiting indicator appears for all the registered lines.

0 - The message waiting indicator shows only for the first line appearance if there are multiple lines registered on the phone.

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 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.eula.accepted

0 (default) - Accept manually the product EULA agreement on the Poly Trio system at the initial start-up.

1 - The EULA agreement is automatically accepted on the Poly Trio system at the initial start-up.

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 log in.

Null (default)

String

prov.login.password.encodingMode

The default encoding mode for the text in the **Password** field on the **User Login** screen.

123 (default)

Alphanumeric

prov.login.userId.encodingMode

The default encoding mode for the text in the **User ID** field on **User Login** screen.

Abc (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 it receives a request for restart or reconfiguration.

request.delay.type

Specifies whether the phone should restart or reconfigure.

call (default) - The phone executes the request when there are no calls.

audio - The phone executes the request when there is no active audio.

Change causes system to restart or reboot.

User Preferences Parameters

Use the following parameters to set phone user preferences.

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**.

1 - **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.idleRestingState

menu (default) – The idle screen displays the **Home** screen menu.

calendar – The idle screen displays a top-level calendar.

dialpad – The idle screen displays 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.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.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 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.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.

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 `sa f . 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 PVOS 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.

URL (default) - NULL

upgrade.plcm.server.url

The URL of the PVOS 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 the following 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 the following 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 are lost. Actual jitter above the maximum value always results in packet loss. If legacy `voice.audioProfile.x.jitterBuffer.*` parameters are explicitly specified, they are used to configure the jitter buffer and these `voice.rxQoS` parameters are 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 is 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 are ignored.

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

Use the following parameters configure 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

SDP Parameters

Use the following parameters to configure the Session Description Protocol (SPD).

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.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 you set `voice.codecPref.iLBC.13_33kbps`, and `voice.codecPref.iLBC.15_2kbps` is Null.
- If you set both `voice.codecPref.iLBC.13_33kbps` and `voice.codecPref.iLBC.15_2kbps`, 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.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 aren't 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, see `video.forceRtcpVideoCodecControl`. For an account of all parameter dependencies refer to "I-Frames."

section.

0 - The phone doesn't include the SDP attribute "a=rtcp-fb".

1 (default) - The phone includes the SDP attribute "a=rtcp-fb" into offers during outbound SIP calls.

Download Location Parameter for Language Files

The following parameter specifies the download location of the translated language files for the system web interface (Web Configuration Utility).

webutility.language.plcmServerUrl

Specifies the download location of the translated language files for the system web interface.

`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 lists 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 XMPP presence.

0 (Default)

1

Session Header Parameters

You can enable session header parameters to convey information between phones about the SIP message.

Use the following parameters to configure session header components.

voIpProt.SIP.supportFor100rel

1 (default) - The phone advertises support for reliable provisional responses in its offers and responses.

0 - The phone doesn't offer 100rel and rejects offers requiring 100rel.

voIpProt.SIP.keepalive.sessionTimers

0 (default) - The phone doesn't declare a timer in the Support header in an INVITE. The call doesn't disconnect when the phone doesn't receive UPDATE packet. The phone still responds to a re-INVITE or UPDATE and follows the session timer to send re-INVITE or UPDATE if the remote endpoint asks for it.

1 - The session timer is enabled and the call disconnects when the phone doesn't receive an 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 disconnects when the phone doesn't receive an UPDATE packet within the specified timer.

0 - The session timer is disabled and the call received on the registered line doesn't disconnect when the phone doesn't receive an UPDATE packet.

Device Parameters

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

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

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

If you configure any parameter values using the `<device/>` parameters, any subsequent configuration changes you make from the system web interface or phone local interface do not take effect after a phone reboot or restart.

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 if you make configuration changes through the system web interface or phone interface. 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.

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 be 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, Polycom recommends that you test the new configuration files on two phones before initializing 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.xxxvalue`.

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 in XML that you can use to configure feature settings.

This guide documents parameters using parameter lists. Be sure to familiarize yourself with basic XML and parameter list conventions to successfully change configurations.

Using XML

Poly parameters are attributes of XML elements. Element names don't affect the behavior of parameters or operation of your phone, and you can customize as needed.

When configuring the 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 `parameter="value"` pair is equivalent to an XML `attribute="value"` pair. For example:

```
<element1>
  <element2 feature.acousticFenceUI.enabled="1" />
</element1>
```

Parameter List Template and Examples

Parameter details can vary depending on the complexity of the parameter.

The following template shows the general parameter list conventions and details.

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.

The following sample parameter lists show a few example parameters 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" />
```

reg.x.callsPerLineKey

Set the maximum number of concurrent calls for a single registration `x` that 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`.

24 (default)

1 - 24

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 [Poly 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 - Disable the phone auxiliary port.

1 (default) - Enable the phone auxiliary port.

Change causes system to restart or reboot.

device.baseProfile

NULL (default)

Generic - Sets the base profile to Generic for OpenSIP environments.

Lync - Sets the base profile for Skype for Business deployments.

USBOptimized - 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.

Change causes system to restart or reboot.

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="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 sends 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="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 - DHCP is disabled.

1 (default) - DHCP is enabled.

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

Sets the secondary server where the phone directs 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

Sets the primary server where the phone directs DNS queries.

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 host name to the DHCP registration server using `Polycom_<MACaddress>`.

String — The maximum length of the host name 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 - Disabled

1 - Enabled

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 - Disabled

1 - Enabled

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.

EAP-None

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.etherModeLAN

Set the LAN port mode that sets the network speed over Ethernet.

Poly recommends that you don't change this setting.

0 - Auto (default)

1 - 10HD

2 - 10FD

3 - 100HD

4 - 100FD

5 - 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.

-1 - Disables the PC port

0 - Auto (default)

1 - 10HD

2 - 10FD

3 - 100HD

4 - 100FD

5 - 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 can't configure the `device.net.etherStormFilterPpsValue` parameter.

1 - You can configure the `device.net.etherStormFilterPpsValue` parameter.

device.net.ipAddress

Set the phone's IP address.

This parameter is disabled when `device.dhcp.enabled="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.lldp.extendedDiscover

0 to 3600 - Duration (in seconds) of LLDP extended discovery duration applied in both the application and updater

0 (default)

Change causes system to restart or reboot.

This parameter overrides `net.lldp.extendedDiscovery`.

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="1"`.

Subnet mask

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 to 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 reprovisions. 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, one 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

IP address

Domain name string

URL

If you modify this parameter, the phone provisions again. The phone also reboots if the configuration on the provisioning server changes.

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) isn't 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 system web interface, the path to the software version you specify displays in the drop-down menu on the **Software Upgrade** page.

NULL (default)

String

0 to 255 characters

device.prov.user

The username required for the phone to log in to the provisioning server (if required).

If you modify this parameter, the phone reprovisions, 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 - Disabled

1 - Enabled

For information, see [Zero-Touch Provisioning](#).

device.sec.configEncryption.key

Set the configuration encryption key used to encrypt configuration files.

String

For more information, see the section on 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 certificates can't 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 is 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 is 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 and 8192 bytes for the device certificate.

0 (default) - Disabled

1 - Enabled

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 - Disables common name validation.

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.showOOB

Set to display the setup wizard when the system powers on as if the system is powering on for the first time.

1 (default) – The system displays a setup wizard when it powers on.

0 – The system doesn't display a setup wizard when it powers on.

device.ntp.gmtOffset

Set the GMT offset, in seconds, to use for daylight saving time, corresponding to -12 to +13 hours.

-43200 to 46800

device.ntp.gmtOffsetcityID

Sets the correct time zone location description that displays on the phone menu and in the system web interface.

NULL (default)

0 to 127

For descriptions of all values, refer to the Time Zone Location Description.

device.ntp.serverName

Enter the SNTP server where 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 Parameters for Wi-Fi

Use the following `<device/>` parameters to configure device settings for Wi-Fi.

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.wifi.country

Enter the two-letter code for the country where you are operating the Poly Trio solution 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.

0 (default)

1

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 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

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

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

Enter the WPA2-Enterprise password.

device.wifi.wpa2Ent.user

Enter the WPA2-Enterprise user name.

Diagnostics and Status

There are a variety of screens and logs that display on Poly devices that enable you to review performance information about the phone, help you diagnose and troubleshoot problems, view error messages, and test the phone's hardware.

Review the latest Release Notes for your product at [Voice Support](#) 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.

Task

- 1 Go to **Settings > Status** and select a status menu item.
- 2 View the following information:

Menu Item	Available Information
System Information	<ul style="list-style-type: none">• Model• Part Number• Platform (Profile)• MAC Address• Wi-Fi MAC Address (on supported models)• Bluetooth MAC Address (on supported models)• IP Address• Version• Updater Signature• System Name
Platform	<ul style="list-style-type: none">• Phone's serial number or MAC address• Current IP address• Updater version• Application version• Names of the configuration files in use• Address of the provisioning server
Network	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Detailed status of each of the phone's configured lines
Diagnostics	<ul style="list-style-type: none">• 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

Upload a Phone's Configuration Files to Provisioning Server

You can upload the phone's current configuration files from the local interface or the system web interface to the provisioning server to help debug configuration problems.

You can upload a configuration file for every active source as well as the current non-default configuration set.

Task

1 Go to **Settings > Advanced > Admin Settings > Upload Configuration**.

2 Choose the files to upload:

- **All Sources**
- **Configuration Files**
- **Local**
- **Web**
- **SIP**

For example, if you select **All Sources**, the phone uploads the `<MACaddress>-update-all.cfg` file.

If you use the system web interface, you can also upload **Device Settings**.

3 Select **Upload**.

The phone uploads the configuration file to the location you specified in the `prov.configUploadPath` parameter.

Perform Network Diagnostics

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

Task

1 Go to **Settings > Status > Diagnostics > Network**.

2 Enter a URL or IP address.

Rebooting the Phone at a Scheduled Time

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

Scheduled Reboot Parameters

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

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 phone. 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

Resetting a Phone to Factory Defaults

You can reset the entire phone or some of the phone's configurations to factory defaults using the local interface.

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

- **Reset Local Configuration:** Clears the override file generated when you make changes using the phone's local interface.
- **Reset Web Configuration:** Clears the override file generated by changes made using the system web interface.
- **Reset 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 software application, log, configuration, and override files. Note that if the override file is stored on the provisioning server, the phone redownloads the override file when you provision the phone again. Formatting the phone's file system doesn't delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the phone.
- **Reset to Factory:** Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the Poly Voice Software application and updater remain intact.
- **Reset to Factory Partial:** Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the Poly Voice Software application, updater, and administrator password remain intact.
- **Reset User Data:** Resets the call list and removes all contacts from the phone and server.
- **Out-of-Box Wizard:** Resets the selections made during the initial out-of-box setup wizard. You can then make the selections again, and the phone reboots.

Reset the Phone and Configuration

You can reset the phone and phone configuration partially or completely.

Task

- 1 On the phone's local interface, go to **Settings > Advanced > Administration Settings**.
- 2 Select **Reset to Defaults** and choose a reset option:
 - **Reset Local Configuration**
 - **Reset Web Configuration**
 - **Reset Cloud Configuration**
 - **Reset Device Settings**
 - **Format File System**
 - **Reset to Factory**
 - **Reset to Factory Partial**
 - **Reset User Data**
 - **Out-of-box Wizard**

Factory Reset the Poly Trio System at Power-Up

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

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

Important: Because this process resets the administrator password to the default, you must change the administrator password to use the phone or the system web interface.

Task

- 1 Power on the system.
- 2 When the Poly logo shows on the screen, press and hold the four corners of the LCD screen.
- 3 Let go when the **Mute** keys begin flashing.

Factory Reset the Poly Trio System from the Local Interface

You can reset Poly Trio systems to the factory default settings from phone's local interface.

Task

- » 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 to Factory Configuration Parameters

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

`up.basicSettings.factoryResetEnabled`

- 0 (default) - Doesn't display the **Reset to Factory** option under **Basic** settings.
- 1 - Displays the **Reset to Factory** option under **Basic** settings.

`feature.restrictPerDataUploadMenu.enabled`

- 1 (default) - Displays the **Restrict Personal Data Upload** menu under **Basic** settings.
- 0 - Doesn't display the **Reset to Factory** menu under **Basic** settings.

`feature.clearPerInfoMenu.enabled`

- 1 (default) - Displays the **Clear Personal Information** menu under **Basic** settings.
- 0 - Doesn't display the **Clear Personal Information** menu under **Basic** settings.

`device.system.recoveryType`

Defines what settings the phone resets via MKC updater boot-up when a user tries a factory reset.

FullRecovery (default) - All settings are returned to factory default.

PreserveAdmin - All settings are returned to factory default except the administrator password.

CloudProv - All settings are returned to factory default except the administrator password and provisioning. Provisioning is changed to ZTP.

Status Indicators on Poly Trio C60 Systems

Trio C60 systems use LEDs to indicate the status of the system.

Poly Trio Status Indicators

Status	Description
Off	Device is in an idle state or powered off.
Green	In a call with audio unmuted.
Red	Microphones are muted. Device is in a call or in idle state.
Amber	Power on LED diagnostic.
Amber/Red/Green/Off Repeating	Recovery in progress.

Monitoring the Phone's Memory Usage

If you use a range of phone features, customized configurations, or advanced features, manage phone memory resources.

If your deployment includes a combination of phone models, consider configuring each phone model separately with its own features instead of applying all features to all models.

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

- The phone reboots or freezes up.
- The phone doesn't download all ringtones, directory entries, backgrounds, or XML dictionary files.

Check Memory Usage from the Phone

View a graphical representation of the phone's memory usage on the phone's local interface.

Load and configure the features and files you want to make available on the phone's local interface.

Task

- 1 Go to **Settings > Status > Diagnostics**.
- 2 Select **Graphs > Memory Usage**.

Viewing Memory Usage Errors in the Application Log

Each time the phone's minimum free memory goes below 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

To free up memory on your phone, review the following table for the amount of memory each customizable feature uses. Reduce the amount of memory you need the feature to use.

Phone Memory Resources

Feature	Typical Memory Size	Description
Custom idle display image	15 KB	The average size of the display image is 15 KB. Custom idle display image files should also be no more than 15 KB.

Feature	Typical Memory Size	Description
Local contact directory	42.5 KB	The phones are optimized to display a maximum of 250 contacts. Each contact has four attributes and requires 170 B. A local contact directory of this size requires 42.5 KB. To reduce memory resources used by the local contact directory: <ul style="list-style-type: none"> • Reduce the number of contacts in the directory. • Reduce the number of attributes per contact.
Corporate directory	Varies by server	The phones are optimized to corporate directory entries with five to eight contact attributes each. The size of each entry and the number of entries in the corporate directory vary by server. If the phone can't display directory search results with more than five attributes, make additional memory resources available by reducing memory requirements of another feature.
Ringtones	16 KB	The ringtone files range in size from 30 KB to 125 KB. If you use custom ringtones, limit the file size to 16 KB. To reduce memory resources required for ringtones, reduce the number of available ringtones.
Background images	8 KB to 32 KB	The phones are optimized to display background images of 50 KB. To reduce memory resources required for background images, reduce the number and size of available background images.
Local interface language	90 KB to 115 KB, depending on language	The language dictionary file used for the phone's user interface ranges from 90 KB to 115 KB for languages that use an expanded character set. To conserve memory resources, use XML language files for only the languages you need.
System web interface	250 KB to 370 KB	

Poly Lens

Poly Lens enables you to monitor and manage system health with actionable insights, including device status and usage for Poly Trio systems.

Note: When Poly Trio systems use the Microsoft Teams base profile, administrators can find call analytics data in the Microsoft Teams device management portal.

Poly phones send the following details to Poly Lens:

- Device asset
- Device network
- Device diagnostics

Poly phones send device details to Poly Lens in the following situations:

- The phone restarts or reboots.
- The phone receives an on-demand request from the cloud.
- The admin updates or changes device details.

Poly Lens Parameter

Use the following parameter to enable Poly Trio systems to share usage data with Poly Lens.

Important: You must disable the `feature.pcc.enabled` parameter before enabling the phone to share data with Poly Lens. If you leave `feature.pcc.enabled` enabled, your phone may not be able to communicate properly with Poly Lens.

feature.lens.enabled

0 (default) - The system doesn't share data with Poly Lens.

1 - The system shares data with Poly Lens.

Change causes the system to restart or reboot.

System Logs

System log files assist when troubleshooting issues.

System log files contain information about system activities and the system configuration profile. After you set up system logging, you can retrieve system log files.

The detailed technical data in the system log files can help Poly Global Services resolve problems and provide technical support for your system. Your support representative may ask you to download log archives and send them to Poly Global Services.

You must contact Poly Customer Support to obtain the template file (techsupport.cfg) that contains the parameters that configure log levels.

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.

- **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 PVOS.

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)

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.

Logging Levels

Logging Level	Description
0	Debug only
1	High detail class event
2	Moderate detail event class
3	Low detail event class
4	Minor error
5	Major error – will eventually incapacitate the system
6	Fatal error

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

- Time or time/date stamp, in one of the following formats:
 - 0 - milliseconds – 011511.006 = 1 hour, 15 minutes, 11.006 seconds since booting
 - 1 - absolute time with minute resolution 0210281716 - 2002 October 28, 17:16
 - 2 - absolute time with seconds resolution 1028171642 - October 28, 17:16:42
- 1-5 character component identifier (such as "so")
- Event class
- Cumulative log events missed due to excessive CPU load
- The event description

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.

4 (default)

0 - 6

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)

0 - 6

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.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, appsp, bluet, bdiag, brow, bsdir, cap, cdp, cert, cfg, cipher, clink, clist, cmp, cmr, copy, curl, daa, dapi, dasvc, dbs, dbuf, dhcpc, 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, mrci, net, niche, obsp, osd, pcap, pcd, pdc, peer, pgui, pkt, pmt, poll, pps, pres, pstn, ptt, push, pwrsv, rdisk, res, restapi, rtos, rtls, sec, sig, sip, slog, so, srtp, sshc, ssps, statc, statn, style, sync, sys, ta, task, tls, trace, ttrs, usb, usbio, util, utilm, 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 Time Stamp Formats table for time stamp 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 Poly 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 Poly Trio System Logs

You can upload system log files to your provisioning server.

When you upload log files, the system copies the log files from the phone to the provisioning server and creates new files named <MACaddress>-now-xxx.log.

Task

- 1 Go to **Settings > Advanced** and enter the administrator password.
- 2 Go to **Administration Settings > Upload Configuration**.
- 3 Select one or more sources to upload from:
 - All Sources
 - Configuration Files
 - Local
 - MR
 - Web
 - SIP
- 4 Select **Upload**.

Uploading Logs to a USB Flash Drive

You can configure your Trio C60 phone to copy application and boot logs to a USB flash drive connected to the phone.

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.

Upgrading the Software

Upgrade software with the user-controlled software upgrade feature. New software versions may offer only small enhancements to improve the user experience, or they may be large software upgrades that offer new features.

The upgrade process varies depending on the software version that is currently running on your phone and the version that you want to upgrade to.

Upgrade UC Software Using a USB Flash Drive

Use a USB flash drive to upgrade the software on your .

Changes you make using a USB flash drive override the settings you configure using a centralized provisioning server (if applicable).

Task

1 Do one of the following:

- Format a blank USB 2.0 USB flash drive using FAT32.
- Delete all files from a previously formatted USB flash drive.

2 Download the UC software from the [Poly Online Support Center](#).

3 Copy the configuration files you want to use to the root of the USB flash drive.

You must copy the minimum required configuration files to the drive:

- Primary configuration file: 000000000000.cfg.
- Poly Trio C60: 3111-86240-001.sip.ld

4 Insert the USB flash drive into the 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.

Upgrading the Software on a Single Phone

Use the **Software Upgrade** tool in the system web interface 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 you make to individual phones using the system web interface 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 the system web interface (Web Configuration Utility).

If a user postpones a software update, configuration changes and software version updates from both the server and the system web interface are postponed. When the user chooses to update, configuration and software version changes from both the server and system web interface are sent to the phone.

This feature doesn't work if you enable ZTP.

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 doesn't 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.optionToIgnore

You can configure the phone to give the user the ability to ignore software updates completely, or ignore until the next reboot or sync event.

1 - The Ignore and Ignore until next Reboot/Sync softkeys display on the phone's local interface during a software upgrade alert.

0 (default) - Users can defer software upgrades up to three times.

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 UC Software with Windows Device Manager

Update phones in USB phone mode through your connected Windows computer using **Device Manager**.

Device Manager locates and downloads the UC software update, then pushes the update to the phone. This is helpful if the phone's system web interface or USB port is disabled or unavailable.

Configure Windows to Update UC Software via Device Manager

Set up your Windows computer to search for and push a UC software update using **Device Manager** to a connected phone in USB phone mode.

Task

1 On your Windows computer, open the **Registry Editor** (regedit.exe).

Note: Windows may prompt you asking if you want to make changes to your computer before it opens **Registry Editor**. Accept the prompt to proceed.

- 2 Go to HKLM\SOFTWARE\Microsoft\
HKLM may also display as HKEY_LOCAL_MACHINE.
- 3 Create the following subkeys: \DriverFlighting\Partner\.
- 4 Under the \Partner subkey, create a string named `TargetRing` and enter `Drivers` as the value.
- 5 Close the **Registry Editor**.

Update UC Software Using a Windows Computer

Update your phone in USB phone mode (USB optimized) using the connected Windows computer.

Make sure that the phone is in USB phone mode, powered on, and connected to a computer with the latest Windows updates. Make sure you configure your computer to update your phone with **Device Manager**.

Task

- 1 On the computer, open **Device Manager**.
- 2 Locate the connected Poly phone as a device.

Tip: The phone may display in the following locations within **Device Manager**:

- Other devices\
• Universal Serial Bus controllers\Other\
• Universal Serial Bus controllers\Other\

- 3 Right-click the phone entry and select **Update Driver > Search Automatically for updated driver software**.

Note: This process may take some time.

- 4 Select **Finish** to begin updating the phone.

Disable UC Software Updates through Windows

Prevent the phone from updating through Windows **Device Manager** in USB phone mode.

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

Note: You can still update UC software using the system web interface or a USB flash drive.

Task

- 1 Open the configuration file.
- 2 Disable UC software updates through Windows **Device Manager**.

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

- 3 Save the configuration file.

Troubleshooting

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

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from [Poly Support](#). For information on using different configuration methods, see [Methods for Configuring the Phones](#).

Updater Error Messages and Possible Solutions

If a fatal error occurs, the phone doesn't boot up.

If the error isn't fatal, the phone boots up but its configuration might be changed. Most updater errors are logged to the phone's boot log. However, if the phone is having trouble connecting to the provisioning server, the phone isn't likely to upload the boot log.

The following table describes possible solutions to updater error messages.

Error Message	Cause and Possible Solution
Failed to get boot parameters via DHCP	The phone doesn't have an IP address and therefore can't boot. <ul style="list-style-type: none">• 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.• Check the DHCP configuration.
Application <file name> is not compatible with this phone!	An application file was downloaded from the provisioning server, but it cannot be installed on this phone. Install a compatible software image on the provisioning server. Be aware that there are various hardware and software dependencies.
Could not contact boot server using existing configuration	The phone cannot contact the provisioning server. Possible causes include: <ul style="list-style-type: none">• Cabling issues• DHCP configuration• Provisioning server problems 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.
Error, application is not present!	The phone doesn't have an application stored in device settings and can't boot because an application could not be downloaded. <ul style="list-style-type: none">• Download compatible UC Software version to the phone using one of the supported provisioning protocols. 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.

UC Software Error Messages

If an error occurs in the UC Software, an error message and a warning icon display on the phone.

The following table describes possible UC Software error messages.

UC Software Error Messages

Error Message	Cause
<p>Config file error: Files contain invalid params: <filename1>, <filename2>,...</p> <p>Config file error: <filename> contains invalid params</p> <p>The following contain pre-3.3.0 params: <filename></p>	<p>These messages display if the configuration files contain these deprecated parameters:</p> <ul style="list-style-type: none"> • 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 <p>These messages also display if any configuration file contains more than 100 of the following errors:</p> <ul style="list-style-type: none"> • Unknown parameters • Out-of-range values • Invalid values <p>To check that your configuration files use correct parameter values, refer to <i>Using Correct Parameter XML Schema, Value Ranges, and Special Characters</i>.</p>
Line: Unregistered	This message displays if a line fails to register to the call server.
Login credentials have failed. Please update them if information is incorrect.	This message displays when the user enters incorrect login credentials on the phone. Update the credentials at Status > Basic > Login Credentials .
Missing files, config. reverted	This message displays when errors in the configuration and a failure to download the configuration files force the phone to revert to its previous (known) condition with a complete set of configuration files. This also displays if the files listed in the <MAC Address>.cfg file aren't present on the provisioning server.
Network link is down	Indicates that the phone can't establish a link to the network and persists until the link problem is resolved. Call-related functions, and phone keys are disabled when the network is down but the phone menu works.

Network Authentication Failure Error Codes

Error messages display on the phone if 802.1X authentication fails.

The error codes display on the phone when you press the **Details** key. Error codes are also included in the log files.

Event Code	Description	Notes
1	Unknown events	An unknown event by '1' can include any issues listed in this table.
2	Mismatch in EAP Method type Authenticating server's list of EAP methods doesn't match with the clients'.	

Event Code	Description	Notes
30xxx	<p>TLS Certificate failure The phone displays the following codes:</p> <ul style="list-style-type: none"> • 000 - generic certificate error • 042 - bad cert • 043 - unsupported cert • 044 - cert revoked • 045 - cert expired • 046 - unknown cert • 047 - illegal parameter • 048 - unknown CA 	See section 7.2 of RFC 2246 for further TLS alert codes and error codes.
31xxx	<p>Server Certificate failure 'xxx' may use the following values:</p> <ul style="list-style-type: none"> • 009 - Certificate not yet Valid • 010 - Certificate Expired • 011 - Certificate Revocation List • (CRL) not yet Valid • 012 - CRL Expired 	
4xxx	<p>Other TLS failures 'xxx' is the TLS alert message code). For example, if the protocol version presented by the server is not supported by the phone, then 'xxx' is 70, and the EAP error code is 4070.</p>	See section 7.2 of RFC 2246 for further TLS alert codes and error codes.
5xxx	<p>Credential failures 5xxx - wrong user name or password</p>	
6xxx	<p>PAC failures:</p> <ul style="list-style-type: none"> • 080 - No PAC file found • 081 - PAC file password not provisioned • 082 - PAC file wrong password • 083 - PAC file invalid attributes 	
7xxx	<p>Generic failures:</p> <ul style="list-style-type: none"> • 001 - dot1x cannot support (user) configured EAP method • 002 - dot1x can't support (user) configured security type • 003 - root certificate couldn't be loaded • 174 - EAP authentication timeout • 176 - EAP Failure • 185 - Disconnected 	

Power and Start-Up Issues

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

Power or Start-up Issue	Possible Solutions:
The phone has power issues or the phone has no power.	<p>Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do the following:</p> <ul style="list-style-type: none"> • Verify that no lights appear on the unit when it's powered up. • Check to see if the phone is properly plugged into a functional AC outlet. • Make sure that the phone isn't plugged into an outlet controlled by a light switch that is turned off. • If the phone is plugged into a power strip, try plugging directly into a wall outlet instead.
The phone doesn't boot.	<p>If the phone doesn't boot, there may be a corrupt or invalid firmware image or configuration on the phone:</p> <ul style="list-style-type: none"> • Ensure that the provisioning server is accessible on the network and a valid software load and valid configuration files are available. • Ensure that the phone is configured with the correct address for the provisioning server on the network.

Screen and System Access Issues

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

Issue	Cause and Possible Solution
There's no response from feature key presses.	<p>If your phone keys don't respond to presses:</p> <ul style="list-style-type: none"> • Press the keys more slowly. • Check to see whether or not the key has been mapped to a different function or disabled. • Make a call to the phone to check for inbound call display and ringing. If successful, try to press feature keys while a call is active to access a directory or buddy status. • On the phone, go to Menu > Status > Lines to confirm that the line is actively registered to the call server. <p>Reboot the phone to attempt reregistration to the call server. Go to Menu > Settings > Advanced > Reboot Phone).</p>
The display shows the message "Network Link is Down".	<p>This message displays when the LAN cable isn't properly connected. Do the following:</p> <ul style="list-style-type: none"> • Check the termination at the switch or hub end of the network LAN cable. • Check that the switch or hub is operational (flashing link/status lights). • On the phone, go to Menu > Status > Network. Scroll down to verify that the LAN is active. • Ping the phone from a computer. <p>Reboot the phone to attempt reregistration to the call server. Go to Menu > Settings > Advanced > Reboot Phone).</p>

Calling Issues

The following table provides possible solutions to common .

Issue	Cause and Possible Solution
There's no dial tone.	<p>If there's no dial tone, power may not be correctly supplied to the phone. Try the following:</p> <ul style="list-style-type: none"> • Check that the display is illuminated. • Make sure the LAN cable is inserted properly at the rear of the phone; try unplugging and reinserting the cable. • If you use in-line powering, check that the switch is supplying power to the phone.
The phone doesn't ring.	<p>If there's no ringtone but the phone displays a visual indication when it receives an incoming call, do the following:</p> <ul style="list-style-type: none"> • 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.	<p>If the phone displays an icon indicating that a line is unregistered, reregister the line and place a call.</p>

Display Issues

The following table provides tips for resolving display screen issues.

Issue	Cause and Possible Solution
There's no display or the display is incorrect.	<p>If there's no display, power may not be correctly supplied to the phone. Do the following:</p> <ul style="list-style-type: none"> • Check that the display is illuminated. • Make sure that the power cable is inserted properly at the rear of the phone. • If you're using PoE powering, check that the PoE switch is supplying power to the phone. <p>Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to <i>Capture Your Device's Current Screen</i>.</p>
The display is too dark or too light.	<p>The phone contrast may be set incorrectly. Do one of the following:</p> <ul style="list-style-type: none"> • Adjust the contrast. • Reboot the phone to obtain the default level of contrast.
The display is flickering.	<p>Certain types of older fluorescent lighting may cause the display to flicker. If your phone is in an environment with fluorescent lighting, angle or move the Poly phone away from the lights.</p>
The time and date are flashing.	<p>If the time and date are flashing, the phone is disconnected from the LAN or there's no SNTP time server configured. Do one of the following:</p> <ul style="list-style-type: none"> • Reconnect the phone to the LAN. • Configure an SNTP server. <p>Disable the time and date if you don't want to connect your phone to a LAN or SNTP server.</p>

Software Upgrade Issues

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

Issue	Cause and Possible Solutions
Some settings or features aren't working as expected on the phone.	<p>The phone's configuration may be incorrect or incompatible.</p> <p>Check for errors on the phone by going 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.</p>
The phone displays a Config file error message for five seconds after it boots up.	<p>You're 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've installed on the phones.</p> <p>Correct the configuration files, remove the invalid parameters, and restart the phone.</p>
When using the system web interface to upgrade phone software, the phone is unable to connect to the Poly Hosted Server.	<p>Occasionally, the phone is unable to connect to the Poly-hosted server because of the following:</p> <ul style="list-style-type: none">• The Poly-hosted server is temporarily unavailable.• There's no software upgrade information for the phone to receive.• The network configuration is preventing the phone from connecting to the Poly-hosted server. <p>To troubleshoot the issue:</p> <ul style="list-style-type: none">• Try upgrading your phone later.• Verify that new software is available for your phone using the Poly UC Software Release Matrix.• Verify that your network's configuration allows the phone to connect to <code>http://downloads.polycom.com</code>. <p>If the issue persists, try manually upgrading your phone's software.</p>