Poly Edge E Series Phones Administrator Guide PVOS 8.5.0

SUMMARY

This guide helps you understand how to set up and manage your Poly Edge E Series phones.

Table of contents

1 Before You Begin 1
Audience, purpose, and required skills 1
Documentation Feedback 1
Poly Edge E Series phones model and part numbers 1
2 Getting Started 3
Priority of configuration and provisioning methods 3
Default Configuration File 4
Configure a phone using Simple Setup 4
Configure a Phone Through the System Web Interface 4
Configure a phone using a USB flash drive 5
3 Phone Accessibility 6
Text-to-Speech 7
Enable Text-to-Speech for Incoming Calls 7
Enable Text-to-Speech for Audio Feedback 7
Configure the Text-to-Speech Voice 8
Configure Large Text Mode 8
Enable High Contrast Mode 8
Enable Color Correction 8
4 Setting Up the Phone 10
Hardware and Power 11
Power Poly Phones 11
Power Saving on the Phones 11
Configure Power Saving 11
Disable Power Saving 12
Complete the Setup Wizard 12
Managing Peripheral Devices 13
Disable Headset Use 13
Connect a Computer to a Network Through the Phone 13
Hot Desking or Hoteling With NFC 13
5 Poly Edge E Series Expansion Module 14

Overview of the Poly Edge E Expansion Module 14
Supported Expansion Modules 14
Powering a Second Expansion Module with Edge E500 Series 15
Verify the power source for an Edge E500 Series phone 15
Expansion Module Line Keys 15
Smart Paging on Poly Edge E Expansion Modules 17
Smart Paging Distribution Scenarios 17
6 Network Settings 18
Bluetooth settings 19
Disable Bluetooth Radio 19
Disable Bluetooth Discovery 19
Update the Bluetooth device name 19
Configure Bluetooth features 20
Configure network signaling validation 20
Configuring Internet Protocol settings 23
Configure a static IPv4 address 23
Enable IPv4 ICMP redirects 23
DHCP IP Address 24
Set the DHCP boot server option in IPv4 mode 24
Enable DHCP IP Address Cache 24
Jitter buffer and packet error concealment 27
Configure jitter buffer for wired network voice traffic 27
Configure jitter buffer for IP multicast voice traffic 27
Set 802.1p/Q priority 28
Provisional Polling of Phones 30
Configure polling for provisioning updates 30
Configure Provisional Polling for Multiple Phones at Random Times 31
IP Type-of-Service 33
Enable IP Type-of Service 33
Static DNS cache 34
Configure the SIP Server for Static DNS Cache 34
Configure the Static DNS Cache with A Record IP Addresses 35
Configure the Static DNS Cache with NAPTR and SRV Records 36
Real-Time transport protocol 38
Configure RTP for FECC 38
Configure RTP media ports 39
Wi-Fi network connectivity 40
Configure Wi-Fi Using a Configuration File 40
Configure Wi-Fi using the local interface 41
Remove Wi-Fi from the Basic Settings Menu 42
Restrict Wi-Fi connectivity to WPA3 only 42
Web proxy 43
Supported HTTP/HTTPS web proxy services 43

Manually configure web proxy access 43
Configure STUN settings 44
Enable and configure TWAMP 44
Technical Report-069 46
Configure TR-069 in the System Web Interface 46
Enable and configure TR-069 using a Configuration File 46
TR-106 Parameters Mapped to Poly Parameters 47
TR-104 Parameters Mapped to Poly Parameters 49
Supported TR-069 Remote Procedure Call (RPC) Methods 50
Enable GZIP Encoding 51
Configure NAT 51
Create a Custom TCP Keep-Alive Message 52
Create a Custom UDP Keep-Alive Message 52
7 Certificates 53
Using the factory-installed certificate 53
Creating CSRs 54
Create a CSR on the local interface 54
Download and install certificates 54
Custom URL locations for LDAP server CAs 56
Define the download URL location for the LDAP server CA 56
Confirm the installed LDAP server certificates 56
Enable OCSP 57
Enable and configure SCEP 57
Custom Wi-Fi Certificates 60
Install and Choose a Root CA Wi-Fi Certificate 60
Install and Choose a Client Wi-Fi Certificate 60
8 Securing the Phone 62
Phone passwords 63
User role login denial when default user password is detected 63
Configure password settings 63
Set the administrator password on the local interface 63
Set the user password on the local interface 64
California SB-327 password requirement compliance 64
Locking the phone 65
Lock the basic settings menu 65
Enable phone lock 65
Set an automatic phone lock 65
Define authorized contacts to call from a locked phone 66
Enable Do Not Disturb when the phone locks 66
Remotely unlock a phone 66
Power Up an Unlocked Phone 66
Allow Answering When the Phone is Locked 67
Advanced user access to administration settings 68

Enable advanced user access 68
Disable advanced user access to network settings 69
Disable advanced user access to TLS security 69
System web interface security settings 70
Configure a security banner for the system web interface 70
Two-factor authentication for system web interface and diagnostic access 70
Configure two-factor system web interface authentication 70
Locking the system web interface after failed login attempts 70
Configure the system web interface lockout 71
Disable the system web interface lockout 71
Configure session management rules 71
Hide the MAC address 72
Encryption 73
Encrypt files for upload 73
Change the encryption key 73
SIP digest authentication methods 75
Enable SHA-256 and SHA-512-256 SIP digest authentication methods 75
Enable Voice over Secure IP 75
Enable and Configure 802.1X Security 76
Poly Edge E FIPS compatibility mode 78
Enable FIPS 140-3 encryption 78
9 SIP Server and Line Configuration 79
Supported Registrations 79
SIP server registration 80
Configure VoIP server DHCP settings 80
SIP signaling failure for outgoing calls 81
Server redundancy 82
Configure server redundancy for a registered line 82
Configure server redundancy for VoIP 84
IP Multimedia Subsystem Features 86
Enable 3GPP IP Multimedia 86
Enable the P-Early-Media Header 87
Remove the Outbound Proxy Address from the Route Header 87
Add Path Extension Header to Request Message 87
Subscribe to Registered Line State Change Notifications 88
Reject Calls with Network Determined User Busy Events 88
Include Service Route Information in VQMon Messages 89
Enable Support for the 199 Response Code 89
Enable Advice of Charge 89
Configure SIP subscription timers 90
Configure the SIP instance identification settings 91
Configure SIP header warnings 91
DNS SIP Server Name Resolution 92
For Outgoing Calls (INVITE Fallback) 92

Customer Phone Configuration 93
Local digit map 94
Configure a local digit map 94
Change the dialing timeout 94
Change the international dialing prefix 95
10 Configuring Audio Settings 96
Automatic gain control 96
Noise suppression 97
Poly NoiseBlockAI 97
Disable Poly NoiseBlockAI 97
Acoustic Fence 97
Enable Polycom Acoustic Fence for Handset Calls 97
Enable Polycom Acoustic Fence for Headset Calls 98
Add Acoustic Fence Options to the Local Interface 98
Dynamically Deactivate Acoustic Fence in Full-Screen Mode 99
Configure VAD 99
Comfort noise 100
Configure comfort noise for speakerphone calls 100
Configure Comfort Noise for Handset Calls 100
Enable AEC for Headsets 101
Audio codecs 102
Supported Audio Codec Specifications 102
Set audio codec priority 103
Configure the SILK audio codec 105
Configure the Opus audio codec 105
Poly Computer Audio Connector 108
Configuring Ports for the Poly Computer Audio Connector 108
Enable the Poly Computer Audio Connector 108
Enable the Poly Computer Audio Connector Using the Local Interface 109
11 Configuring Call Controls 110
Do Not Disturb 111
Disable Do Not Disturb 111
Enable call server-based Do Not Disturb 111
Enable call server-based Do Not Disturb on a registered line 112
Call hold 113
Configure call hold reminders 113
Configure hold music 113
Change the Reinvite Method 114
Configure default call transfer type 114
Call forwarding 115
Forward calls while busy 115
Forward calls while DND is active 115
Forward unanswered calls 116
Disable call forwarding 116

Convert the call timer to display in seconds 116
Call waiting alerts 118
Silence the ringtone for call waiting 118
Disable call waiting alerts 118
Configure Call Waiting for a Specific Line 118
Use network signaling for caller ID 119
Enable and configure STIR/SHAKEN caller ID validation 119
Enable the remote party disconnect alert 120
Voicemail 122
Configure voicemail settings 122
Disable voicemail 122
Enable local call recording 122
Missed Call Notifications 124
Disable the Recent Calls Softkey 124
Conference call host management 125
Enable conference host to place participants on hold 125
End a conference call when the host disconnects 125
Disable conference management options 125
Configure automatic dialing 126
Configure Directed Call Pickup 126
Configure the Call Park and Retrieve Star Code 127
Configure Last Call Return 127
Enable the conference meeting Dial-In Options list 127
Multiple call appearances 129
Configure the number of line keys per registration 129
Configure the maximum number of concurrent calls per registration 129
Shared lines 130
Enable a shared line 130
Shared call appearances 130
Configure line-seize on shared lines 130
Enable call diversion on shared lines 131
Immediately reject incoming calls on shared lines when on DND 131
Enable barge-in on a shared line 131
Configure unique outbound caller IDs on shared lines 132
Enable private hold on shared lines 132
Set a Ring Delay Timer for Incoming Calls 132
SIP-B Automatic Call Distribution 133
Enable ACD 133
Simplify ACD State Controls 133
Configure bridged line appearance 134
Extend the amount of time the expanded call view displays 134
Configure bridged line appearance 134
Busy Lamp Field 136

BLF Feature Options 136
SIP Server Support for BLF Configurations 136
Subscribe to a Busy Lamp Field Resource List on a Call Server 136
Configure a Busy Lamp Field Resource in the Configuration File 137
Enable SIB-B Group Call Pickup 138
Enable Instant Messaging 139
PTT and Group Paging 140
Configure phones to receive group pages 140
Configuring PTT 140
Enable and Configure PTT 141
Block a Phone from Sending Outgoing PTT Calls 141
Add a Label to a PTT Channel 141
Add a Label to a Specific PTT Group 142
Configure an Emergency PTT Channel 142
Configure the PTT Group to Use for Emergency Pages 142
Change the IP Multicast Address and Port 143
Intercom calls 144
Enable intercom calls 144
Creating a custom intercom softkey 144
MLPP for AS-SIP 145
Enable AS-SIP 146
Set Call Priority and Precedence Levels 146
Setting Call Precedence with a Digit Map 146
Set the Preemption Screen Display Time 147
Configure a Custom Namespace for Precedence Calls 147
Precedence Display by Phone Model 147
Preemption Behavior for Low Priority Calls 148
VQMon reports 149
Configure VQMon alerts 149
Configure VQMon reports 150
12 Configuring emergency services 151
Enhanced 911 (E.911) 152
Manually Set the Phone's Location for Emergency Calls 152
Configure E.911 Location for Ribbon Communications 152
Configure Emergency Instant Messages 153
Silent distress call 154
Creating a distress number 154
Create a distress number contact entry 155
Configure a number as an emergency number 155
Populate a directory file with contact information 155
Configure distress numbers 157
Configure a text to speech distress message 157
Configure a distress number softkey 158
13 Configuring Phone Settings 159
User profiles 160

Enable multiple user profiles on the phone 160
User profile authentication 160
User profile server authentication 160
Enable the phone to use server authentication 160
Create a generic user profile for server authentication 161
Create user profiles for server authentication 162
User profile phone authentication 162
Create a user configuration file 162
Convert a phone to user-based deployment 163
Create default credentials and a profile for a phone 163
Require a user login 164
Mask the user password entry 164
Enable user login persistence 164
Presence Status 165
Enable Presence Status to Display on the Phone 165
Disable Presence Softkeys 165
Microphone mute 166
Enable microphone mute/unmute alert 166
Configure mute reminder alert interval 166
Enable microphone mute persistence 166
Enable Persistent Call Volume 166
Disable DTMF tones 167
Audible notifications and sounds 169
Set the audible notification and sound output 169
Disable the phone's welcome sound 169
Disable audible notifications and sounds 170
Disable the voicemail stutter dial tone 170
Ringtones and visual incoming call indicators 170
Supported ring classes 170
Disable distinctive ringtones signaled through Alert-Info 171
Disable the ability to change the ringtone 171
Configure the call waiting tone 172
Distinctive ringtones 172
Assign a distinctive ringtone to a registered line 172
Assign a distinctive ringtone based on Alert-Info headers 173
Sound effects 173
Add a sample audio file 173
Configure sound effect patterns 174
Sound effect pattern examples 175
Call progress tone patterns 175
Ringtone patterns 176
Miscellaneous sound effect patterns 177
14 Directories and Contacts 179
Local contact directory 180
Set the maximum number of contacts in the local directory 180
Creating directory files 180

Create a Per-Phone Personal Directory File 180
Create a Global Directory File 181
Populate a Directory File with Contact Information 181
Configure When Directory Files Update 183
Disable the local contact directory 183
Create a speed dial entry in the directory file 183
Disable local speed dial edits 184
Prioritize Local Directory Changes 185
Remotely Delete Device Directory Contacts 185
Corporate directory 186
Connecting to a Corporate Directory Using LDAP 186
Connect to a corporate directory using LDAP 186
Configure the LDAP Server Base Domain 186
Configure the LDAP Server Connection Port 187
Configure the LDAP Search Query Filter Prefix String 187
Configure LDAP Server Credentials 187
Configure LDAP Search Attributes 187
Securely store LDAP credentials 189
Call lists 190
Disable the missed call list 190
Disable the placed call list 190
Disable the received call list 190
Disable all call lists 191
Disable consultation call logging 191
List consecutive calls individually 191
Enable Exchange call log synchronization 191
15 Configuring the Local Interface 192
Localizing the user interface 193
Edit phone languages 193
Change the Keyboard Layout 194
Enable Pinyin Text on the Phone 194
Configure the phone's display name 194
Configuring labels 196
Create a custom Home screen label 196
Configure unique line labels for registration lines 196
Time and date display 198
Disable the time and date on the idle display 198
Configure Time and Date Display Settings 198
Change the Date Format 199
Contact Support Menu 201
Enable and Configure the Contact Support Menu 201
Add Help Desk Contact Information 201
Add Help Desk Hours and Contact Information 202
Add a Customer Logo to the Contact Support Menu 202
Customize the QR Code 203
Set Up a Custom Background 203

Add a Customer Logo to the Home Page 204
Digital Picture Frame 206
Map Digital Picture Frame Location 206
Adjust the Digital Picture Frame Refresh Duration 206
Disable the Digital Picture Frame 206
Support for REST APIs 208
REST API parameter 208
Enhanced Feature Keys 209
Some Guidelines for Configuring Enhanced Feature Keys 209
Contact Directory Macros 210
Special Characters 210
Enhanced Feature Key Example Configurations 210
Mapping Internal Key Functions 211
Macro Definitions 215
Macro Actions 216
Prompt Macro Substitution 217
Expanded Macros 217
Example Macros 217
LED indicators 218
LED indicator pattern types 218
LED Pattern Parameters 218
Set an LED Pattern for Active Calls 219
Set an LED pattern on BLF for held calls 220
Set an LED pattern for incoming calls 220
Set an LED pattern for self-parked calls 221
Set an LED pattern for remote-parked calls 221
Configure LED behavior for locally held calls 221
Configuring Line Key LEDs 222
Disable the Headset Key LED in Headset Memory Mode 222
Surround Lighting Bar 223
Surround lighting bar pattern types 223
Surround LED Lighting Bar Pattern Parameters 223
Activate Surround Lighting Bar Patterns 224
Enable Mute Indication on the Surround Lighting Bar 224
Enable Digital Headset Indication on the Surround Lighting Bar 225
Disable Surround Lighting Bar in Power Saving Mode 225
Disable halo when DnD is active 225
Disable surround lighting bar when DnD is active 225
Flexible Line Key Assignment 227
Line Key Registration Assignments 227
Line Key Numbering 227
Configure Flexible Line Keys 228
Flexible Line Key Assignment Categories and Index 229
Using the Any Category 230
Assigning Busy Lamp Field (BLF) and Presence to Line Keys 230
Assign BLF to a Line Key 230
Assign Presence to Line Keys 231

Poly Edge E400 Series Secondary Screen 232
Specifying the Location of Lines, BLFs, EFKs, and Speed Dial Favorites 232
Specify the Location of a Registered Line 232
Specify the Location of a BLF Resource List 232
Specify the Location of a BLF Resource 233
Specify the Location of an EFK 233
Specify the Location of a Speed Dial Favorite 233

16 Phone Maintenance 235

Cloud-Based Configuration and Management Methods 236
Enable PDMS-SP Onboarding 236
Poly Lens 237

Analytics support for Poly Cloud Services 238
Importing and exporting configurations 238
Busy Lamp Field Analytics 238
Shared Call Appearance Analytics 238
User Interface Analytics 239
Uptime Analytics 239
Hardware Analytics 239
Device Details Sent to the Cloud 241
Device Asset Details 241
Secondary Device Details 241
Service Details 242
Device Network Details 243

Monitoring the phone's memory usage 245
Phone memory resources 245
Check memory usage from the local interface 246
Configure a phone memory alert 246
Memory usage errors in the application log 246

Capturing the Phone's Screen 247
Enable Screen Capture 247
Capture the Phone's Screen 247

Rebooting the Phone 248
Reboot the Phone 248
Reboot the phone at a scheduled time 248
Disable the phone boot status message 249

Upgrading the Software 250
Important update information for PVOS 9.0.0 250
Downgrading PVOS 9.X.X to earlier software versions 250
Information removed and retained after downgrading 251
Configure software rollback prevention 251
Downgrade restriction parameters 252
Upgrading the software on a single phone 252
Configure user-controlled software updates and polling 252
Update PVOS using a USB flash drive 253

Resetting a Phone to Factory Defaults 254
Reset the Phone and Configuration 254

Enable Users to Reset the Phone to Factory 254

17 Third-Party Servers 256

Cisco BroadWorks server 257
Authentication with Cisco BroadWorks XSP Service Interface 257
Features that Require Cisco BroadWorks XSP Authentication 257
Authenticate phones using SIP credentials 257
Authenticate phones using Cisco BroadWorks XSP credentials 258
UC-One Integration 258
Features Supported with the UC-One Integration 258
Required Cisco BroadWorks Platform 259
Enable UC-One integration 259
Cisco BroadWorks Directory Support 259
Types of Cisco BroadWorks Directories 259
Enable Cisco BroadWorks Directories 260
Configure the UC-One directory 260
Enable the Default Search View for the Enterprise Directory 261
UC-One Call Control Features 261
Enable UC-One on Poly Phones 261
Enable Users to Log In Using UC-One Credentials 261
Enable anonymous call rejection 262
Enable simultaneous ring 262
Enable line ID blocking 262
Enable Remote Office 262
BroadWorks Anywhere 263
Enable BroadWorks anywhere 263
Create an EFK for BroadWorks Anywhere 263
Hide the UC-One Settings icon on the Home screen 264
BroadWorks Call Decline 264
Enable the Reject Softkey for Shared Lines 264
Flexible Seating 264
Feature Conditions with Flexible Seating 264
Flexible Seating Feature Limitations 265
Configure Flexible Seating 265
BroadWorks Configuration Tags for Flexible Seating 266
Executive and Assistant Lines 266
Configure a Phone for Executive or Assistant Lines 266
Disable the Pick Call and Barge-in Softkeys 267
Create EFKs for the Executive and Assistant Menus 267
Enhanced Call Park 268
Configure Enhanced Call Park 268
Default Retrieval Star Code 268
Configure Retrieval Star Code for Parked Calls 269
Enable Audio Notifications for Parked Calls 269
Enable Cisco BroadWorks Server-Based Call Features 269
Enable Cisco BroadWorks Server-Based Call Forwarding 269
Hoteling 270
Limitations with Hoteling and Feature-Synchronized ACD 270
Enable and Configure Hoteling 270

Feature-Synchronized ACD 270
Feature-Synchronized ACD Services 271
Enable Feature-Synchronized ACD 271
SIP Call Server for Feature-Synchronized ACD 271
Centralized Call Recording 271
Centralized Recording or Local Call Recording 272
Call Recording Alerts 272
Enable Centralized Call Recording 272
Block Call Recording on a Registered Line 272
Call Recording Modes 272
Visual Security Classification for Cisco BroadWorks Calls 273
Enable phones to display the security classification 273
Configure Key System Emulation 274
Ribbon Communications Server 277
Multiple Appearance Directory Number - Single Call Appearance (MADN-SCA) 277
MADN-SCA Parameters 277
Configuring Privacy on a MADN-SCA Line 279
Example MADN-SCA Configuration 279
Global Address Book (GAB) 279
Global Address Book Parameters 280
Example GAB Configuration 281
Personal Address Book (PAB) 282
Personal Address Book Parameters 282
Example Personal Address Book Configuration 282
Enhanced 911 (E.911) Location for Ribbon Communications 283
Enhanced 911 (E.911) Location Parameters for Ribbon Communications 283
Manually Set the Phone's Location 283
Emergency Instant Messages 284
Emergency Instant Message Parameters 284
Enable Server-Specific Features 284
18 Diagnostics and Status 286
Network Ping 287
Ping a Network Address from the Local Interface 287
Ping a Network Address from the System Web Interface 287
Traceroute 289
Send a Traceroute from the Local Interface 289
Send a Traceroute from the System Web Interface 289
DNS Testing 290
Configure a Test DNS Server Account 290
Run a DNS Test from the System Web Interface 291
Display the Phone's DNS Cache 291
NTP Server Connection Testing 292
Configure an NTP Test Address 292
View NTP Server Test Information 292
19 Troubleshooting 293
Find a Phone's Information 293

System Logs 294
Configuring Log Files 294
Logging Levels 294
Enable Log Uploads to a USB Flash Drive 295
Retrieve Logs Using the System Web Interface 295
Retrieve Logs from the Support Information Package 295
Upload a Phone's Configuration Files 296
Test Phone Hardware 296
Capturing your phone screens 297
Capture Your Phone's Screen Through the System Web Interface 297
Capture Your Phone's Expansion Module Screen Through the System Web Interface 297
Configure Remote Packet Capture 297
Updater error messages and possible solutions 298
PVOS error messages 299
Network authentication failure error codes 300
Troubleshooting power and start-up issues 302
Power and start-up issues 302
The phone has power issues 302
The phone doesn't boot up 302
Troubleshooting screen and system access issues 304
Screen and system access issues 304
There's no response from feature keys 304
The display indicates that the network link is down 305
Troubleshooting calling issues 306
Calling issues 306
There's no dial tone 306
There's no dial tone on one of the audio paths 307
The phone doesn't ring 307
Unregistered line icon 307
Lifting the handset does not answer calls when the ringtone is silent 307
Troublehooting display issues 309
Display issues 309
There's no display or the display is incorrect 309
The display is too dark or too light 310
The phone display is flickering 310
The time and date are flashing 310
Audio Issues 310
Troubleshooting audio issues 311
..... 312
Software upgrade issues 312
Phone settings or features aren't working 312
Phones display a Configuration file error message 313
Phones can't connect to the Poly-hosted server 313
Provisioning Issues 314

Troubleshooting provisioning issues 314
Run a Diagnostics Check 315
Run a diagnostics check 316
Preparing to Troubleshoot Issues 317
View Warnings 317
Remove warnings 317
Speakerphone 317
Troubleshooting speakerphone 317
USB Port 317
USB not detected 318
Troubleshooting Bluetooth headset issues 319
Bluetooth Headset Issues 319
Bluetooth settings don't display 319
Headset doesn't pair automatically 319
Troubleshooting recording issues 320
Recording Issues and Solutions 320
Recording fails immediately after starting 320
Recording fails during a call 320
Recording canceled after removing USB flash drive 321
Unsupported USB headset causes recording to fail 321
Viewing the Phone's Status 322
View System Information 322
Check the status of the calendar 322
View the PAB status 322
View the GAB Status 322
20 Getting help 323
HP Inc. addresses 323
Document information 324

1 Before You Begin

This guide describes how to administer, configure, and provision Poly phones and accessories.

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

- Poly Edge E100 and E220
- Poly Edge E300 Series, including E300, E320, and E350
- Poly Edge E400 Series, including E400 and E450
- Poly Edge E500 Series, including E500 and E550
- Poly Edge E Expansion Module

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

Documentation Feedback

We welcome your feedback to improve the quality of Poly documentation.

Please email Documentation Feedback if you have any queries or suggestions related to this documentation.

Poly Edge E Series phones model and part numbers

The following table lists the product names and software model numbers for Poly Edge E Series phones. Software model numbers are used by the phone when requesting software files and in some networking protocols such as DHCP or LLDP as an identifier rather than the model name.

Table 1-1 **Poly Edge E Series software model numbers**

Product name	Model name	Software model number
Poly Edge E100	EdgeE100	3111-86980-001
Poly Edge E220	EdgeE220	3111-86990-001
Poly Edge E300	EdgeE300	3111-87815-001
Poly Edge E320	EdgeE320	3111-87000-001
Poly Edge E350	EdgeE350	3111-87010-001
Poly Edge E400	EdgeE400	3111-87835-001
Poly Edge E450	EdgeE450	3111-87030-001
Poly Edge E500	EdgeE500	3111-87855-001
Poly Edge E550	EdgeE550	3111-87050-001

2 Getting Started

Poly offers several methods to configure or provision your phone.

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

Poly recommends configuring your phones using a cloud-based service such as Poly Lens. Alternatively, you can configure the phone's settings using simple setup, the system web interface, or a USB flash drive. You can also use configuration files through the system web interface to copy phone settings from one phone to another.

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

⚠ **CAUTION:** In a DHCP network environment, the phone must be able to resolve DNS information either through a network server or static cache to communicate with your provisioning server. This is true even if the DHCP server returns the provisioning server address in IPv4 format. If you disable DNS in a DHCP network environment, you can't provision your phone.

If you manually configure the provisioning server, you also need to configure a primary DNS server. Optionally, you can configure a secondary DNS server.

Priority of configuration and 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's a priority among the methods that impacts your phone deployment when you use multiple methods simultaneously. If there's 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
3. System web interface
4. Poly Clariti Manager
5. Centralized provisioning

6. Default phone values

For example, when you provision the phones using a provisioning server and then 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

Default Configuration File

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

The default name for the configuration file is `00000000000.cfg`. Use the default name or rename the default configuration file. The file name must contain at least five characters and end with `.cfg`.

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

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

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

Configure a phone using Simple Setup

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

1. Find your phone's IP address by pressing the checkmark button in the center of the phone's navigation circle.
2. Enter the phone's IP address into a web browser and then enter the administrator password.
3. Select **Call Configuration** > **Simple Setup**.
4. Configure your SIP server, outbound proxy, and SIP account settings.

Configure a Phone Through the System Web Interface

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

1. Enter your phone's IP address into a web browser.

   To find your phone's IP address, go to **Settings** > **Status** > **System Information**.
2. Select **Admin** as the login type and enter the administrator password.
3. Go to **Utilities** > **Import & Export Configuration**.

4. Choose the file to export from the **Export Configuration (except Device Settings)** drop-down menu.
5. Select **Export**.
6. Open the configuration file.
7. Enter or update the parameters in the **Configuration** list.
8. Save the configuration file.
9. Go to **Utilities** > **Import & Export Configuration**.
10. Select **Import**.
11. Select the configuration file.
12. Select **OK**.

Configure a phone using a USB flash drive

Manually configure one phone at a time with a USB flash drive.

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

1. Download the PVOS version for your phone from Poly Lens and unzip the folder.
2. Copy the contents of the PVOS package to the root folder of the USB flash drive. Use the entire contents of the software package or select files piecemeal. You must use at least the following minimum required configuration files:

   - Primary configuration file: `000000000000.cfg`.

   You can also use `firmware.sip.ld` and other configuration files for additional provisioning.
3. **Optional:** Create configuration files with settings and parameters.
4. **Optional:** Modify `000000000000.cfg` to reference the configuration files in the CONFIG_FILES attribute. Save the file.
5. Insert the USB flash drive into a USB port on the phone, enter the administrator password, and power cycle the phone.

Wait several minutes for your device to restart.

3 Phone Accessibility

Configure phone accessibility options.

Text-to-Speech

With the **Text-to-Speech** accessibility feature, you can hear functions and information about the phone spoken out loud. The phone also provides feedback about incoming calls.

When you enable **Text-to-Speech**, the phone offers the following functionality:

- You can receive notifications and audio feedback about incoming calls.
- When you single press the following keys, the phone reads information about the keys out loud. Press the key again to use the key.

NOTE: This feature isn't supported for the dialpad, navigation, select, or EM line keys.

  - A line key on the phone
  - A softkey
  - Home
  - Back
  - Hold
  - Transfer
  - Headset
  - Speakerphone
  - Mute
  - Pagination
  - Page left and right keys on the Edge E400 Series

Enable Text-to-Speech for Incoming Calls

Configure the phone to read user interface elements aloud for functions and information.

1. Open the configuration file.
2. Enable text to speech.

```
accessibility.texttospeech.enabled="1"
```

3. Save the configuration file.

Enable Text-to-Speech for Audio Feedback

Enable the **Text-to-Speech** feature to hear audio descriptions of phone functions and information.

1. Go to **Menu** > **Settings** > **Accessibility**.
2. Enable **Text-to-Speech**.
3. To enable audio feedback from the hardware keys, press and hold the center navigation button.

Configure the Text-to-Speech Voice

Configure the voice that the phone uses when Text-to-Speech is enabled.

1. Open the configuration file.
2. Configure the Text-to-Speech voice with one of the following options. The default is `slt`.
   - kal16
   - awb
   - rms
   - slt

   ```
   accessibility.textToSpeech.voice="<voice option>"
   ```
3. Save the configuration file.

Configure Large Text Mode

Configure the text size for the phone.

You can configure the phone's onscreen text size to make it more accessible for users with vision-related disabilities.

1. Open the configuration file.
2. Configure the text size.

   The available values are `Normal`, `Large`, and `Bold`. The default is `Normal`.

   ```
   ui.accessibility.textStyle="<value>"
   ```
3. Save the configuration file.

Enable High Contrast Mode

Configure the phone to provide more contrast between the screen elements and the background.

1. Open the configuration file.
2. Enable **High Contrast** mode.

   ```
   ui.accessibility.highContrast.enabled="1"
   ```
3. Save the configuration file.

Enable Color Correction

Enable color correction to allow users to apply a color filter to their phone's home screen.

When this feature is enabled, users can apply color filters with the following color correction modes:

- Greyscale

- Protanomaly (Red-Green)
- Deuteranomaly (Green-Red)
- Tritanomaly (Blue-Yellow)

1. Open the configuration file.
2. Enable color correction.

```
ui.accessibility.colorCorrection.enabled="1"
```

3. **Optional:** Configure the color correction mode.

   Permitted values:

   - Greyscale
   - Tritanomaly
   - Protanomaly
   - Deuteranomaly

```
ui.accessibility.colorCorrection.mode="<color_filter>"
```

4. Save the configuration file.

4 Setting Up the Phone

After you set up and power on your phone, configure its features.

See the setup sheets applicable to your phone and its peripheral devices at Poly Support.

Hardware and Power

Use PoE or an optional power supply to power Poly phones. Configure or disable power saving settings.

Power Poly Phones

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

IMPORTANT: If you're using a power supply, make sure you use the correct power supply for your phone.

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

Power Saving on the Phones

The power-saving feature automatically turns off the phone's LCD display when it's not in use. Power saving is enabled by default.

Configure the following power-saving options for the phone:

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

NOTE: When you enable power-saving mode and the phone is in low-power state, the red LED indicator slowly blinks to show that the phone still has power.

Configure Power Saving

Configure power-saving mode for office hours and off hours on your phone.

The phone remains in office hours mode until it completes the duration, after which it enters off hours mode. Configure office hours on a certain workday by setting a start hour and duration in hours. Also configure the allowed period of idle time in minutes before the system enters power-saving mode.

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Configure office hours for each workday.

   Repeat this step for each workday, as set by the value for *<Day>*. For example, `Monday`.

```
powerSaving.officeHours.startHour.<Day>="<Hour value>"
powerSaving.officeHours.duration.<Day>="<Hour value>"
powerSaving.idleTimeout.officeHours="<Minute value>"
```

3. Configure the allowed period of idle time in minutes before the phone enters power-saving mode during off hours.

   When the system isn't in office hours mode, it's in off hours mode. The default is 1. Permitted values are 1 to 10.

```
powerSaving.idleTimeout.offHours="<Minute value>"
```

4. Configure how long user input, such as touching the screen or pressing a button, extends the period of idle time in minutes.

   Incoming calls, whether the user answers them or not, resets the idle timeout. This applies for both office hours and off hours. The default is 10. Permitted values are 1 to 20.

```
powerSaving.idleTimeout.userInputExtension="<Minute value>"
```

5. Save the configuration file.

Disable Power Saving

Disable power saving so the phone never enters a low-power state.

1. Open the configuration file.
2. Disable power saving on the phone.

```
powerSaving.Enable="0"
```

3. Save the configuration file.

Complete the Setup Wizard

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

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

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

3. Review the End-User License Agreement (EULA) and select **Accept**.

   You can also review the EULA at HP Support.

4. Select a system language.
5. Set your time zone ID.
6. Select **Next** and confirm your selection.

The phone starts in your selected base profile.

Managing Peripheral Devices

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

Disable Headset Use

Prevent the phone from using headsets plugged into it.

- Disable headset use.

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

Connect a Computer to a Network Through the Phone

Connect your computer to the network through your Poly phone.

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

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

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

Hot Desking or Hoteling With NFC

Near-field Communication (NFC) enables users to log in to phones in hoteling or hot desking situations from a smartphone running a service provider or platform partner app.

A partner can use NFC technology on Edge E Series phones to enable users to log in to a desk phone through a mobile device. This method requires the partner app to read the NFC tag for key device identifying information and use that to trigger a reconfiguration process that sends a new config file to the phone from the partner's provisioning server.

NOTE: For additional details, see *Near Field Communication (NFC) for Hoteling and Hotdesking Applications on Poly Edge E Series Phones: Feature Profile 72444* on the Poly Edge E Series support page.

5 Poly Edge E Series Expansion Module

Poly Edge E400 and Edge E500 Series phones support the Poly Edge E Expansion Module.

Poly Edge E EMs enable users to perform the following tasks:

- Handle large call volumes on a daily basis
- Expand phone functions
- Accept, screen, dispatch, and monitor calls
- Reduce the number of lost customer calls
- Shorten transaction times
- Increase the accuracy of call routing

Overview of the Poly Edge E Expansion Module

This section provides information on the features available on the Poly Edge E Expansion Module.

The following features are available on the Poly Edge E Expansion Module:

- Color LCD 480 × 854 pixel display
- Up to 66 programmable keys with 22 line keys on 3 display pages
- LED indicators for line keys and page keys
- Side USB port for connecting and charging low-powered devices, such as a USB headset

NOTE: If the phone can't power a USB device connected to the expansion module, the phone powers down the expansion module until the user disconnects the USB device.

Supported Expansion Modules

The following table provides the number of connected Poly Edge E Expansion Modules and the total number of line keys supported by Poly Edge E Series phones.

Table 5-1 **Supported Expansion Modules and Total Line Keys by Poly Edge E Series Phone Model**

Phone Model	Maximum Connected Expansion Modules	Total Line Keys
Edge E400	1	86 • 8 on primary screen • 12 on secondary screen • 66 on EM
Edge E450	1	86 • 8 on primary screen • 12 on secondary screen • 66 on EM
Edge E500	2	144 • 12 on phone • 66 on EM 1 • 66 on EM 2
Edge E550	2	144 • 12 on phone • 66 on EM 1 • 66 on EM 2

Powering a Second Expansion Module with Edge E500 Series

To power a second expansion module on Edge E500 Series phones, you must power the phone using PoE+ (802.3at) or an AC adapter.

Verify the power source for an Edge E500 Series phone

Verify that your Edge E500 Series phone has sufficient power for two expansion modules.

1. Go to **Settings** > **Status** > **Platform** > **Phone**.
2. Select **Power Source**.

   If the power source is PoE+, then you can use two expansion modules with an Edge E500 Series phone.

Expansion Module Line Keys

The line keys on Poly phones and expansion modules are numbered sequentially, and the line key numbering on an expansion module depends on how many lines the phone supports.

For example, an Edge E550 phone has 12 physical line keys and supports up to 48 lines when you enable pagination, numbered 1 to 48. Connecting the EM disables pagination, so the first line on the connected expansion module is line 13.

Smart Paging on Poly Edge E Expansion Modules

The smart paging feature arranges line key assignments and distributes pages on the expansion modules based on the number of expansion modules connected to a supported phone.

Smart paging applies only when you connect more than one expansion module to a supported phone. If you connect only one expansion module, the order of pages is sequential even if smart paging is disabled.

NOTE: When you enable the flexible line key feature, the expansion module ignores the smart paging configuration and line key assignments display on the designated line key.

Smart Paging Distribution Scenarios

With Smart Paging, the expansion module distributes the line key pages across the connected expansion modules.

If you only have one expansion module connected to your phone, the pages are ordered sequentially on the module. Press the first, second, or third **Page** key to view the corresponding pages.

If you have two expansion modules connected to your phone, the pages are ordered non-sequentially. The pages display on the two expansion modules in the following order:

6 Network Settings

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

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

Bluetooth settings

Configure Bluetooth settings, disable Bluetooth entirely, or disable certain features.

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

Disable Bluetooth Radio

By default, the phone enables Bluetooth radio. Disable Bluetooth radio to make the phone not discoverable.

IMPORTANT: Disabling Bluetooth radio also disables Poly Fast Pair.

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Disable Bluetooth radio.

```
bluetooth.radioOn="0"
```

3. Save the configuration file.

Disable Bluetooth Discovery

Bluetooth is enabled by default, but to completely disable Bluetooth for security reasons, also disable Bluetooth discovery.

NOTE: Your Edge E is discoverable only when the Bluetooth menu is open.

1. Open the configuration file.
2. Disable Bluetooth discovery.

   NOTE: As of PVOS 8.1.0, this parameter is deprecated.

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

3. Save the configuration file.

Update the Bluetooth device name

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

1. Open the configuration file.
2. Update the Bluetooth device name. The maximum length is 20 characters.

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

3. Save the configuration file.

Configure Bluetooth features

Adjust the default Bluetooth values based on your deployment requirements.

1. Open the configuration file.
2. Set the maximum time, in seconds, that the phone attempts to connect with other devices.

   The default value is `0`, which disables the discoverable timeout. The value is 0 to 3600.

   NOTE: As of PVOS 8.1.0, this parameter is deprecated.

   ```
   bluetooth.discoverableTimeout="<Max time>"
   ```

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

   IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

   By default, 10 devices remain in the phone's memory. The value range is 0 to 10.

   ```
   bluetooth.device.maxPaired="<Max number of devices>"
   ```

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

   By default, the phone remains paired for 30 minutes (1800 seconds). The value ranges from 1800 to 18000 seconds. The default is 10800 seconds.

   ```
   bluetooth.device.pairedTimeout="<Max time>"
   ```

5. Save the configuration file.

Configure network signaling validation

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

Choose one of the following options for validating incoming signaling:

;lp====

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

- Both source IP address validation and digest authentication.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set a signaling validation method. Replace *x* with the desired number of SIP request validation settings. The maximum is 20.

   The following values apply:

   - `Null` (default): No validation is made.
   - `Source`: Ensure the phone receives the request from an IP address of a server belonging to the set of target registration servers.
   - `digest`: Challenge requests with digest authentication using the local credentials for the associated registration (line).
   - `both or all`: Apply both of the above methods.

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

3. Set the SIP requests to apply the validation. Replace *x* with the desired number of SIP request validation settings. The maximum is 20.

   The following values apply:

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

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

4. Specify the events to validate with the event header. Replace *x* with the desired number of SIP request validation settings. The maximum is 20. For each *x*, configure up to 20 event values (*y*).

   - `Null` (default): All events are validated.
   - A valid string - The specified event is validated.

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

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

5. Save the configuration file.

Configuring Internet Protocol settings

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

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

Configure a static IPv4 address

Configure IPv4 mode in the phone's local interface.

Connect your phone to an Ethernet network connection.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Network Interfaces** > **Ethernet Menu**.
2. Select **IP Mode** > **IPv4** .
3. Select **IPv4 Configuration**.
4. Clear the **DHCP** check box.
5. Configure the following settings:
   - **IP Address**
   - **Subnet Mask**
   - **IPv4 Gateway**
6. Back out of the menus. When prompted, select **Save Config**.

   The phone restarts.

Enable IPv4 ICMP redirects

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

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the following parameters to allow the phone to write the configuration to flash.

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

3. Enable ICMP redirects.

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

4. Save the configuration file.

DHCP IP Address

The phone enables DHCP by default.

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

Set the DHCP boot server option in IPv4 mode

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

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the phone to get the boot server details from the custom options number provided through DHCP.

   The following values apply:

   - `0` (Default) - The phone gets the boot server address from option 66.
   - `1` - The phone gets the boot server details from the custom option number provided through DHCP.
   - `2` - The phone uses the boot server configured through the **Server** menu.
   - `3` - The phone uses the custom option first or uses option 66 if the custom option isn't present.

```
device.dhcp.bootSrvUseOpt="<value>"
device.dhcp.bootSrvUseOpt.set="1"
```

3. Save the configuration file.

Enable DHCP IP Address Cache

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

Make sure your configuration file includes `device.set="1"`.

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

DHCP IP address cache stores the following lease parameters:

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

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

DHCP IP address cache has the following limitations:

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

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

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

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

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

```
device.net.cachedIPAddressRetryTime="<value>"
device.net.cachedIPAddressRetryTime.set="1"
```

4. Save the configuration file.

Jitter buffer and packet error concealment

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

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

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

Configure jitter buffer for wired network voice traffic

Configure jitter buffer for wired network voice traffic.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

1. Open the configuration file.
2. Enter an average jitter setting, in milliseconds. The default is `20`. The range of values is 20 to 80.

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

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

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

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

4. Save the configuration file.

Configure jitter buffer for IP multicast voice traffic

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

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

If you explicitly specify legacy `voice.audioProfile.x.jitterBuffer.*` parameters, they are used to configure the jitter buffer and the `voice.rxQoS.*` parameters are ignored.

1. Open the configuration file.
2. Enter an average jitter setting in milliseconds. The default is `240`.

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

3. Enter maximum jitter setting in milliseconds. The default is `480`.

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

4. Save the configuration file.

Set 802.1p/Q priority

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

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

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

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

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

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

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

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

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

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

6. Save the configuration file.

Provisional Polling of Phones

Configure phones to poll the server for provisioning updates automatically.

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

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

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

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

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

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

Configure polling for provisioning updates

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

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable automatic polling for updates.

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

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

   The default is `03:00`.

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

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

   The default is `Null`.

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

5. Set the provisioning polling period, in seconds.

   The default is `86400`. The integer value must be greater than 300 seconds.

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

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

6. Set the provisioning polling mode.

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

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

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

7. Save the configuration file.

Configure Provisional Polling for Multiple Phones at Random Times

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

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

1. Open the configuration file.
2. Enable automatic polling for updates

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

3. Set polling to random.

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

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

```
prov.polling.period="604800"
```

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

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

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

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

7. Save the configuration file.

IP Type-of-Service

The type-of-service field in an IP packet header consists of four type-of-service (TOS) bits and a 3-bit precedence field.

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

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

Enable IP Type-of Service

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

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

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable ToS.

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

3. Save the configuration file.

Static DNS cache

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

Note the following when configuring the static DNS cache:

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

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

Configure the SIP Server for Static DNS Cache

Configure the SIP server settings to use static DNS cache.

Note the following when you configure the static DNS cache:

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

   The default is `Null`.

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

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

   The default is `Null`.

   NOTE: All the parameters you configure in this list override the parameters specified in `voIpProt.server.*`.

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

4. Set the SIP server port .

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

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

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

5. Set the transport method the phone uses to communicate with the SIP server.

   The following values apply:

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

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

   - `TCPpreferred` - The phone prefers TCP as the transport but uses UDP if TCP fails.
   - `UDPOnly` - The phone uses only UDP.
   - `TLS` - If TLS fails, transport fails. Leave `reg.x.server.y.port` empty (defaults to 5061) or set to `5061`.
   - `TCPOnly` - The phone uses only TCP.

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

6. Save the configuration file.

Configure the Static DNS Cache with A Record IP Addresses

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

Configure the SIP server information.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.

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

   The default is `Null`.

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

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

   The default is `Null`.

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

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

   The default is `300`. The value range is 300 to 2147483647.

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

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

5. Save the configuration file.

Configure the Static DNS Cache with NAPTR and SRV Records

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

Configure the SIP server information.

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

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

This also happens when using the registration-specific parameters for the SIP server and outbound proxy configuration:

- `reg.x.server.y.address="<string>"`
- `reg.x.server.y.port="0"`

or

- `reg.x.outboundProxy.address="<string>"`
- `reg.x.outboundProxy.port="0"`

It also applies for global SIP server configuration:

- `voIpProt.server.x.address="<string>"`
- `voIpProt.server.x.port="0"`

This SRV request produces a list of servers ordered by weight and priority, enabling you to specify subdomains for separate servers, or you can create partitions of the same system. Note

that while making SRV queries and transport is configured as TCP, the phone adds the prefix `<service.proto.>` to the configured address/FQDN but doesn't remove the subdomain prefix. The phone can resolve a single SRV query to many different servers, session border controllers (SBCs), or partitions ordered by weight and priority.

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Configure the DNS cache NAPTR parameters. Replace *y* with the desired server key value.

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

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

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

4. Save the configuration file.

Real-Time transport protocol

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

Configure RTP ports for your environment in the following ways:

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

  This is useful for communicating through firewalls. When you use a fixed transport port, all RTP traffic sends to and arrives on that specified port. Incoming packets are sorted by the source IP address and port, which enables the phone to multiplex multiple RTP streams.
- Specify the phone's RTP port range. The phone supports conferencing and multiple RTP streams, and it can use several ports concurrently.

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

Configure RTP for FECC

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the FECC port range configuration for OpenSIP registrations.

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

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

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

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

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

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

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

5. Save the configuration file.

Configure RTP media ports

Configure the RTP media ports.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the maximum supported end range for the audio ports.

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

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

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

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

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

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

4. Save the configuration file.

Wi-Fi network connectivity

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

Note the following when using Wi-Fi:

- The phone still requires power using a power adapter for power when using Wi-Fi.
- The phone doesn't support Wi-Fi captive portals or Wireless Display (WiDi).

Your phone supports the following wireless modes and security standards:

- WPA2 Personal
- WPA2 Enterprise
- WPA3 Personal
- WPA3 Enterprise
- WPA2 Personal + WPA3 Personal
- WPA2 Enterprise + WPA3 Enterprise
- 2.4 GHz / 5 GHz operation
- IEEE 802.11a radio transmission standard
- IEEE 802.11b radio transmission standard
- IEEE 802.11g radio transmission standard
- IEEE 802.11n radio transmission standard

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

Configure Wi-Fi Using a Configuration File

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

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

Make sure your configuration file includes `device.set="1"`.

NOTE: Poly Edge E100, E220, E300, E320, E400, and E500 phones don't support Wi-Fi.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the parameter to be written to the phone's flash.

1. Open the configuration file.

2. Enable Wi-Fi.

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

3. **Optional:** Set a country of operation.

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

```
device.wifi.country="<Alpha-2 country code>"
device.wifi.country.set="1"
```

4. Enable DHCP for Wi-Fi.

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

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

```
device.wifi.ssid="<SSID>"
device.wifi.ssid.set="1"
```

6. **Optional:** Specify your Wi-Fi network security mode.

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

7. Save the configuration file.

Configure Wi-Fi using the local interface

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

1. Go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Network Interfaces** > **Wi-Fi Menu**
2. **Optional:** Set a country of operation.

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

   a. Select **Country of operation**
   b. Choose your country from the list.
   c. Select the back arrow.

3. Select **Wi-Fi**.

4. Toggle Wi-Fi on and select the back arrow.

   The phone reboots.

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

6. Select an available Wi-Fi network.

7. **Optional:** If required, enter the Wi-Fi network's security password.

8. Select **Connect**.

   The phone connects to the network.

Remove Wi-Fi from the Basic Settings Menu

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

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

1. Open the configuration file.

2. Remove the wireless menu option from the **Basic** menu.

```
feature.wifiUserSettings.enabled="0"
```

3. Save the configuration file.

Restrict Wi-Fi connectivity to WPA3 only

Administrators can enforce a policy that prevents clients from using legacy security protocols.

When you enable this restriction, Wi-Fi scan results only display access points (SSIDs) that are configured on router devices that can support WPA3 connectivity. The scan results page will show "(WPA3)" at the top to indicate that WPA3-only enforcement is active.

Because a wireless router might broadcast multiple SSIDs with different security configurations, not every SSID on a WPA3-capable router is guaranteed to support WPA3. For this reason, WPA3 restrictions are enforced only when a client attempts to connect to a specific SSID, not during the initial scan. Users will see an error message if they attempt to connect to an SSID that does not use the WPA3 security protocol.

1. In the system web interface, go to **Network** > **Wi-Fi**.

2. Toggle on the **Allow only WPA3 Connections** option.

Web proxy

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

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

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

Supported HTTP/HTTPS web proxy services

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

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

- Generic services
- HTTP/HTTPS provisioning
- Core file upload

Manually configure web proxy access

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable web proxy.

```
feature.wpad.enabled="1"
```

3. Enter the web proxy server address.

   The default is `Null`. The maximum string length is 255 characters.

```
feature.wpad.proxy="<string>"
```

4. **Optional:** Enable and configure basic authentication on the web proxy server. The default is `Null`. The maximum string length is 255 characters.

   NOTE: Poly phones don't support advanced web proxy authentication, such as NTLM.

```
feature.wpad.basicAuth.enabled="1"
```

```
feature.wpad.proxy.username="<string>"
feature.wpad.proxy.password="<string>"
```

NOTE: As of PVOS 8.0.0, the following parameter is deprecated:

```
feature.wpad.basicAuth.enabled
```

5. Save the configuration file.

Configure STUN settings

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable STUN.

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

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

3. Enter the STUN server IP address.

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

4. **Optional:** Enter a port number. The default value is `3478`. The range of values is 1 to 65535.

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

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

   In the parameter, replace *x* with the line number.

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

6. Save the configuration file.

Enable and configure TWAMP

PVOS supports Two-Way Active Measurement Protocol (TWAMP). Enable and configure TWAMP to review packet loss and latency between endpoints.

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

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

For more information on TWAMP, see A Two-Way Active Measurement Protocol (TWAMP).

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open configuration file.
2. Enable TWAMP.

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

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

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

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

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

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

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

6. Save the configuration file.

Technical Report-069

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

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

You can configure Poly phones with an ACS server, including username and password, using DHCP option 43 for IPv4.

Configure TR-069 in the System Web Interface

Configure TR-069 from the system web interface.

1. In the system web interface, go to **Servers** > **Provisioning Server** > **TR-069 Menu**.
2. Select **Enable**.
3. Enter the values as needed in the provided fields.

   - ACS URL
   - ACS Username
   - ACS Password
   - CPE Username
   - CPE Password
   - Periodic Inform
   - Inform Interval
   - Managed Upgrades
4. Select **Save**.

Enable and configure TR-069 using a Configuration File

Configure TR-069 using configuration parameters.

Make sure your configuration file includes `device.set="1"`.

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

NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the phone to write the parameter to the phone's flash.

1. Open the configuration file.

2. Enable TR-069.

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

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

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

4. Enter the TR-069 ACS server URL.

```
device.tr069.acs.url="<valid URL>"
device.tr069.acs.url.set="1"
```

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

```
device.tr069.acs.username="<username>"
device.tr069.acs.username.set="1"device.tr069.acs.password="<password>"
device.tr069.acs.password.set="1"
```

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

```
device.tr069.cpe.username="<username>"
device.tr069.cpe.username.set="1"
device.tr069.cpe.password="<password>"
device.tr069.cpe.password.set="1"
```

7. Enable the phone to send CPE information to the ACS server using the Inform call method.

```
tr069.periodicInform.enabled="1"
tr069.periodicInform.enabled.set="1"
```

8. Set the interval (in seconds) with which the phone attempts to connect with the ACS and send the Inform message.

```
tr069.periodicInform.interval="<number of seconds>"
tr069.periodicInform.interval.set="1"
```

   The value ranges from 0 to 36000. The default is 18000.

9. Enable the phone to use the ACS to only seek out available upgrades.

```
device.tr069.upgradesManaged.enabled="1"
device.tr069.periodicInform.interval.set="1"
```

10. Save the configuration file.

TR-106 Parameters Mapped to Poly Parameters

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

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

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

Table 6-1 Device and Device.DeviceInfo

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

Table 6-2 Device.ManagementServer

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

Table 6-3 Device.LAN

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

TR-104 Parameters Mapped to Poly Parameters

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

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

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

Table 6-4 VoiceService.{i}.VoiceProfile.{i}

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

Table 6-5 VoiceService.{i}.VoiceProfile.{i}.SIP

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

Table 6-6 VoiceService.{i}.VoiceProfile.{i}.SIP.EventSubscribe.{i}

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

Table 6-7 VoiceService.{i}.VoiceProfile.{i}.RTP

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

Table 6-8 VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP

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

Table 6-9 VoiceService.{i}.VoiceProfile.{i}.ButtonMap.Button.{i}

TR-104 ACS parameter names	Poly Parameters	Writable
ButtonName	`softkey.X.label`	Yes

Table 6-9 VoiceService.{i}.VoiceProfile.{i}.ButtonMap.Button.{i} (continued)

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

Table 6-10 VoiceService.{i}.VoiceProfile.{i}.Line.{i}

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

Table 6-11 VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP

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

Table 6-12 VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures

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

Supported TR-069 Remote Procedure Call (RPC) Methods

The following table lists the supported RPC methods.

Table 6-13 RPC Methods

RPC Method	Description
GetRPCMethods	Discovers the set of methods supported by the phone.
SetParameterValues	Modifies the value of one or more phone parameters.
GetParameterValues	Obtains the value of one or more phone parameters.
GetParameterNames	Discovers the parameters accessible on a particular phone.
GetParameterAttributes	Reads the attributes associated with one or more phone parameters.
SetParameterAttributes	Modifies attributes associated with one or more phone parameters.

Table 6-13 RPC Methods (continued)

RPC Method	Description
Reboot	Reboots the phone.
Download	Causes the phone to download a specified file from the designated location. Supported file types for download: • Firmware Image • Configuration File
FactoryReset	Resets the phone to its factory default state.
TransferComplete	Informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	Adds a new instance of an object defined on the phone.
DeleteObject	Removes a particular instance of an object.

Enable GZIP Encoding

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

1. Open the configuration file.
2. Enable GZIP encoding.

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

3. Save the configuration file.

Configure NAT

Configure the NAT settings for your phone.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

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

3. Specify the keep-alive interval, in seconds.

   The default is `0`. The value range is 0 to 3600.

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

4. Set the initially allocated RTP port.

   The default is `0`. The value range is 0 to 65440.

   NOTE: This parameter overrides the `tcpIpApp.port.rtp.mediaPortRangeStart` parameter.

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

5. Set the port used for SIP signaling.

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

   NOTE: This parameter overrides the `voIpProt.local.port` parameter.

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

6. Save the configuration file.

Create a Custom TCP Keep-Alive Message

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

1. Open the configuration file.
2. Create a custom string to use as the payload of a TCP keep-alive message. You can't leave the string value blank.

   The default string is `CRLFCRLFCRLFCRLFCRLFCRLFCRLFCRLF`.

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

3. Save the configuration file.

Create a Custom UDP Keep-Alive Message

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

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

   The default string is `CRLFCRLF`.

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

3. Save the configuration file.

7 Certificates

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

Using the factory-installed certificate

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

The certificate, signed by the Polycom Root (CA), is suitable for all security requirements. View the Certificate Revocation List (CRL)—a list of all expired certificates signed by the Polycom Root CA—at http://crl.polycom.com/crl.

IMPORTANT: The device certificate expires 15 years after the date of manufacture. The Polycom Root CA certificate expires on March 9, 2044.

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

Creating CSRs

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

Create a CSR on the local interface

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

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

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

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

   A **CSR generation completed** message displays.

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

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

Download and install certificates

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

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

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

1. Go to **Settings** > **Advanced** > **Administrative Settings** > **TLS Security**.
2. Do one of the following:
   - To install a CA, select **Custom CA Certificates**.

- Download and Install Certificates on page 54
- To install a device certificate, select **Custom Device Certificates**.

3. Select **Install**.
4. Enter the URL where the certificate is stored. Note that the phone can't accept chevrons (<, >) in the URL field.

   `http://server.domain.com/ca.crt`

   The certificate downloads, and the certificate's MD5 fingerprint displays to verify that you're installing the correct certificate.
5. Select **Accept**.

   The certificate installs successfully.

Custom URL locations for LDAP server CAs

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

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

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

Define the download URL location for the LDAP server CA

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the corporate directory feature.

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

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

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

4. Set the TLS profile to `application profile 1`.

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

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

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

6. Save the configuration file.

Confirm the installed LDAP server certificates

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

1. Select **Settings** > **Advanced**.
2. Go to **Administrative Settings** > **TLS Security** > **Custom CA Certificates** > **Application CA 7**.
3. Confirm that phone downloaded and installed the correct certificates.

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

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

Enable OCSP

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

Make sure your configuration file includes `device.set="1"`.

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to use OCSP.

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

3. Save the configuration file.

Enable and configure SCEP

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

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the SCEP feature.

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

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

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

4. Specify the user name and password to authenticate with the SCEP server.

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

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

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

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

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

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

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

8. 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`. The default is `12`. The value range is 1 to 24.

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

9. Specify the time, in seconds, to wait between poll attempts when the SCEP server returns a Certificate Enrollment Response Message with `pkiStatus` set to `pending`. The default is `300` (5 minutes). The value range is 300 to 3600.

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

10. Specify the time interval, in hours, to retry certificate renewal. The default is `86400` (24 hours). The value range is 28800 to 259200 (8 to 72 hours).

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

11. Specify the percentage of the certificate validity percentage threshold to initiate a renewal. The default is `80`. The value range is 50 to 100.

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

12. Specify the number of times to retry the enrollment process in case of enrollment failure. The default is `12`. The value range is 1 to 24.

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

13. Specify the time interval, in seconds, to retry the enrollment process in case of enrollment failure. The default is `300` (5 minutes). The value range is 300 to 3600.

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

14. Specify the message type a phone uses in certificate renewal requests. The default is `1`. Set the parameter to `0` if the phone requires interoperability with specific servers, such as the Microsoft Device Enrollment Service (NDES). If set to `0`, the phone uses the PKCSReq message type in certificate renewal requests.

```
SCEP.useRenewalReqMessageType
```

15. Save the configuration file.

Custom Wi-Fi Certificates

You can install custom wireless network certificates for added security.

For wireless network certificates:

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

  The phone can't connect to both Ethernet and Wi-Fi at the same time.
- The phone retains installed and saved certificates until you choose to forget the network.
- Poly phones don't support certificates obtained via SCEP.

Install and Choose a Root CA Wi-Fi Certificate

Install a custom certificate for connecting to your wireless network.

NOTE: CA and client certificates must be PEM encoded. Client private keys must be PKCS#8 PEM encoded. Only the Platform 1 and 2 CA and device credentials can be used for Wi-Fi authentication.

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

This task describes using the configuration file. To use the system web interface instead, go to **Security** > **Certificates** > **Install Certificate**.

1. Open the configuration file.
2. Install the certificates.

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

```
device.sec.TLS.customCaCert1.set="1"
```

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

```
device.sec.TLS.customCaCert2.set="1"
```

3. Choose the certificate to use.

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

```
device.wifi.wpa2End.caCert.name.set="1"
```

4. Save the configuration file.

Install and Choose a Client Wi-Fi Certificate

For added wireless network security, install a client certificate.

NOTE: CA and client certificates must be PEM encoded. Client private keys must be PKCS#8 PEM encoded. Only the Platform 1 and 2 CA and device credentials can be used for Wi-Fi authentication.

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

This task describes using the configuration file. To use the system web interface instead, go to **Security** > **Certificates** > **Install Certificate**.

1. Open the configuration file.
2. Install the certificates.

```
sec.TLS.customDeviceCert1="<value>"
```

```
device.sec.TLS.customCaCert1.set="1"
```

```
sec.TLS.customDeviceCert2="<value>"
```

```
device.sec.TLS.customCaCert2.set="1"
```

3. Choose the certificate to use.

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

```
device.wifi.wpa2End.caCert.name.set="1"
```

4. Save the configuration file.

8 Securing the Phone

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

Phone passwords

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

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

- User password: `123`

User role login denial when default user password is detected

Edge E phones now deny access users who log in to the system web interface using the default users password. The user account must have a unique password to log in.

Configure password settings

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

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: These settings override any locally set passwords.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the minimum allowed password character counts for administrative and user passwords.

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

3. Set the administrator and user passwords.

NOTE: You can't set the administrator password as the default password: `456`.

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

4. Save the configuration file.

Set the administrator password on the local interface

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

1. Open the configuration file.
2. Select **Settings** > **Advanced**.

3. Enter the default password and select **Enter**.
4. Select **Change Admin Password**.
5. 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 (`<, >`).
6. Save the configuration file.

Set the user password on the local interface

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

1. Select **Settings** > **Advanced**.
2. Enter the user password and select **Enter**.

   The default user password is `123`.
3. Select **Change User Password**.
4. On the *Change User Password* screen, enter your old and new user password and select **Enter**.

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

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

California SB-327 password requirement compliance

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

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

If the phone is automatically redirected to the provisioning server using DHCP Options, and the provisioning server changes the admin password in the configuration file, you don't need to manually change the admin password.

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

Locking the phone

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

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

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

Lock the basic settings menu

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

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

1. Open the configuration file.
2. Enable the password requirement on the **Basic** settings menu.

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

3. Save the configuration file.

Enable phone lock

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

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

1. Open the configuration file.
2. Enable the phone lock feature.

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

3. Save the configuration file.

Set an automatic phone lock

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

1. Open the configuration file.
2. Set the amount of idle time, in seconds, before the phone locks automatically. If you set the value to `0`, automatic locking is disabled. The value range is 0 to 65535.

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

3. Save the configuration file.

Define authorized contacts to call from a locked phone

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

1. Open the configuration file.
2. Configure up to five authorized contacts that users can call with a locked phone.

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

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

3. Save the configuration file.

Enable Do Not Disturb when the phone locks

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

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

1. Open the configuration file.
2. Configure the phone to activate DND at the same time it locks.

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

3. Save the configuration file.

Remotely unlock a phone

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

1. Open the configuration file.
2. Disable the phone lock parameter.

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

3. Save the configuration file.

Power Up an Unlocked Phone

Configure the phone to power up in the unlocked state.

1. Open the configuration file.
2. Enable the power up unlocked parameter.

   ```
   phoneLock.powerUpUnlocked="1"
   ```

3. Save the configuration file.

Allow Answering When the Phone is Locked

Configure the phone to allow the user to answer calls when the phone is locked.

1. Open the configuration file.
2. Enable the allow answer on lock parameter.

```
phoneLock.allow.answerOnLock="1"
```

3. Save the configuration file.

Advanced user access to administration settings

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

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

Users can access all administrator features except the following:

- Line configuration
- Call server configuration
- Test automation

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

Enable advanced user access

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

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

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

3. Configure an advanced user password for the phone.

   This password grants access to the **Advanced** menu, but it doesn't grant access to the **Admin** menu.

   NOTE: This setting overrides the locally set advanced user password.

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

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

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

5. Save the configuration file.

Disable advanced user access to network settings

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

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

1. Open the configuration file.
2. Remove the **Network** option under **Settings** in the system web interface.

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

3. Save the configuration file.

Disable advanced user access to TLS security

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

1. Open the configuration file.
2. Remove the **TLS** option under **Settings** > **Network** in the system web interface.

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

3. Save the configuration file.

System web interface security settings

Configure security settings for the system web interface.

Configure the following options:

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

Configure a security banner for the system web interface

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

1. Open the configuration file.
2. Enable the security banner feature.

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

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

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

4. Save the configuration file.

Two-factor authentication for system web interface and diagnostic access

You can now choose to enforce two-factor authentication for access to the phone's system web interface.

You can apply two-factor authentication to all access attempts. You can also waive it for a configurable period after the first approval, with further waiver restrictions available based on the connection's source IP or the diagnostic service being accessed.

For more two factor authentication options please refer to the {Xref Error! Target does not exist.}Two-factor authentication parameters section of the Parameter Reference Guide.

Configure two-factor system web interface authentication

To increase the security when accessing the system web interface, you can require two steps to sign in.

1. Open the configuration file.
2. Set the following parameter to require two-factor authentication.

```
feature.mfa.enabled="1"
```

3. Save the configuration file.

Locking the system web interface after failed login attempts

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

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

Configure the system web interface lockout

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

1. Open the configuration file.
2. Configure the number of allowed failed attempts. The value range is 3 to 20.

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

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

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

4. Configure, in seconds, how long the system web interface stays locked. The value range is 60 to 300.

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

5. Save the configuration file.

Disable the system web interface lockout

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

1. Open the configuration file.
2. Disable the system web interface lockout.

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

3. Save the configuration file.

Configure session management rules

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

The phone enforces session duration limits that determine when users must re-authenticate. You can customize these limits as needed.

The system web interface allows up to ten concurrent sessions. A single session has a default maximum duration of 1500 seconds.

If you change the password, all existing sessions expire and you must log in with the new password.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

This task describes using the configuration file. To use the system web interface instead, go to **Access** > **Network** > **Session Duration** > **REST Session Duration (seconds)**.

1. Open the configuration file.
2. Set the duration of a single session in the idle state, in seconds. The default is `1500`. The value range is 60 to 86400.

```
httpd.rest.session.duration.sec="<session duration>"
```

3. Save the configuration file.

Hide the MAC address

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

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Hide the MAC address from users.

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

3. Save the configuration file.

Encryption

Encryption ensures that information remains secure. Configure your phone to encrypt configuration files before sending them to the provisioning server over your network.

Encrypt files for upload

Configure the phone to encrypt files you upload to the provisioning server.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable encryption for the following file types:
   - Configuration file:

     ```
     sec.encryption.upload.config="1"
     ```

   - Call lists:

     ```
     sec.encryption.upload.callLists="1"
     ```

   - Contact directory:

     ```
     sec.encryption.upload.dir="1"
     ```

   - MAC address configuration file:

     ```
     sec.encryption.upload.overrides="1"
     ```

3. Save the configuration file.

Change the encryption key

Change the encryption key on the phones to maintain secure files.

NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the phone to write the parameter to the phone's flash.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Place all encrypted configuration files that you want to update on the provisioning server.

   The phone may restart multiple times.

2. Enter the new key into the configuration file included in the list of files downloaded by the phone, specified in `000000000000.cfg` or *<MACaddress>*`.cfg`.

3. Open the configuration file.
4. Specify a new encryption key:

```
device.sec.configEncryption.key.set="1"
device.sec.configEncryption.key="<encryption key>"
```

5. Save the configuration file.
6. Provision the phone.
7. After you update the encryption key, you must decrypt the files on the server with the old encryption key, then encrypt again it with the new key. Alternatively, you can make the files available in unencrypted format.
8. Delete any configuration override files from the provisioning server so that the phone replaces them when it successfully starts.

   The phone automatically restarts another time to use the new encryption key.

SIP digest authentication methods

RFC 8760 updates RFC 3261 by modifying the SIP digest authentication to add support for additional secure digest algorithms (SHA-256 and SHA-512-256) and replace the older and obsolete MD5 algorithm.

Enable SHA-256 and SHA-512-256 SIP digest authentication methods

Configure the following parameters to enable SHA-256 and SHA-512-256 SIP digest authentication schemes.

1. Open the configuration file.
2. (Optional) Disable the MD5 setting.

```
voipProt.SIP.auth.digest.md5.enabled="1"
```

3. Enable the SHA-256 setting.

```
voipProt.SIP.auth.digest.sha256.enabled="1"
```

4. Enable the SHA-512-256 setting.

```
voipProt.SIP.auth.digest.sha512-256.enabled="1"
```

5. Save the configuration file.

Enable Voice over Secure IP

Enable Voice over Secure IP (VoSIP) to increase the level of security for calls over certain lines. When you enable VoSIP, the voice signals travel securely between endpoints without the need to introduce multiple lines in the Session Description Protocol (SDP).

The following are advantages for using VoSIP:

- The voice signals are encrypted, enabling safe and secure signal transmission between phones.
- Signaling and media to the cloud-hosted product are encrypted.

Configure your phones to dynamically select either Secure Real Time Protocol (SRTP) or Real Time Protocol (RTP) when making a call. The choice depends on the media security protocols negotiated between the phone and outbound proxy server using VoSIP.

1. Open the configuration file.
2. Enable the VoSIP protocol. Replace *x* with the desired line key value.

```
reg.x.rfc3329MediaSec.enable="1"
```

3. Save the configuration file.

Enable and Configure 802.1X Security

Configure your phone to work on a network secured with 802.1X authentication. With this feature enabled, you can configure credentials the phone provides to authenticate on your secured network. Poly phones support IEEE 802 standards.

NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the phone to write the parameter to the phone's flash.

To set up an EAP method requiring a device or CA certificate, configure a TLS Platform Profile 1 or TLS Platform Profile 2 to use with 802.1X. For more information on EAP authentication protocol, see RFC 3748: Extensible Authentication Protocol.

The phone supports the following 802.1X EAP authentication methods:

- EAP-TLS (requires device and CA certificates)
- EAP-PEAPv0-MSCHAPv2 (requires CA certificates)
- EAP-PEAPv0-GTC (requires CA certificates)
- EAP-TTLS-MSCHAPv2 (requires CA certificates)
- EAP-TTLS-GTC (requires CA certificates)

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

This task describes using the configuration file. To use the system web interface instead, go to **Network** > **LAN** > **LAN Options** > **Ethernet 802.1x**.

1. Open the configuration file.
2. Enable 802.1X authentication.

```
device.net.dot1x.enabled="1"
device.net.dot1x.enabled.set="1"
```

3. Set the username and password for 802.1X authentication. You don't need to set a password if you set `EAP-TLS` for the 802.1X EAP method.

```
device.net.dot1x.identity="<username>"
device.net.dot1x.identity.set="1"
device.net.dot1x.password="<password>"
device.net.dot1x.password.set="1"
```

4. Set an 802.1X EAP method.

   The following values apply:

   - EAP-TLS
   - EAP-PEAPv0-MSCHAPv2

- EAP-PEAPv0-GTC
- EAP-TTLS-MSCHAPv2
- EAP-TTLS-GTC

```
device.net.dot1x.method="<EAP method>"
device.net.dot1x.method.set="1"
```

5. Set an 802.1X EAP workaround.

```
device.net.dot1x.eapWorkaround="0"
```

6. Save the configuration file.

Poly Edge E FIPS compatibility mode

Beginning with the Poly Voice Software 8.3.0 release, Poly Edge E phones will operate in a FIPS (Federal Information Processing Standards) compatible mode (that ensures use of cryptographic algorithms and methods approved by the U.S. government).

The Poly Edge E series uses the OpenSSL 3.1.2 crypto module, which NIST validated for FIPS 140-3 compatibility under certificate #4985.

While FIPS mode provides a higher level of security and data protection, it limits the Poly Edge E series to using only FIPS-approved algorithms, preventing the use of potentially weaker or unvalidated algorithms.

IMPORTANT: The following legacy services known to require use of 3DES or SHA-1 algorithms will no longer be compatible unless FIPS mode is disabled:

- The SCEP (Simple Certificate Enrollment Protocol) offered by NDES on the Microsoft windows server.
- CA certificates signed using the SHA-1 algorithm
- Custom device credentials using the SHA-1 algorithm or RSA key sizes less than 2048 bits

For information on configuration changes review the {Xref Error! Target does not exist.}Poly Edge E Parameter Reference Guide FIPS configuration.

Enable FIPS 140-3 encryption

The Federal Information Processing Standard (FIPS 140-3) compliance is a cryptographic function. Enable phones to use the FIPS 140-3 compliant cryptography.

NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the phone to write the parameter to the phone's flash.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable FIPS 140-3 encryption.

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

3. Save the configuration file.

9 SIP Server and Line Configuration

PVOS supports SIP 2.0 based on RFC 3261. Configure the SIP server connection and the lines on the phone.

Supported Registrations

Depending on the phone model, the number of supported registrations varies.

Table 9-1 Poly Edge E Series Supported Registrations

Model	Registrations
Edge E100	8
Edge E220	16
Edge E300 Series	32
Edge E400 Series	34
Edge E500 Series	34

SIP server registration

After the phone starts, it registers to all configured servers.

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

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

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

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

Configure VoIP server DHCP settings

Configure how the phone reacts to DHCP changes.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to check the DHCP server for an IP address.

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

3. Set the DHCP option.

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

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

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

4. **Optional:** Enable the phone to request a string. Otherwise, the phone requests an IP address.

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

5. **Optional:** Enable the outbound proxy address to be a string. Otherwise, the phone requests an IP address.

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

6. Set the outbound proxy option for DHCPv4.

   The default is `120`. The value range is 120 to 254.

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

7. Define the outbound proxy option for DHCPv6.

   The default is `21`. The value range is 0 to 254.

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

8. Save the configuration file.

SIP signaling failure for outgoing calls

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

⚠ **CAUTION:** If the phone uses DNS to resolve the address for servers, the phone attempts to contact the DNS server to resolve the address of all servers in its list before initiating a call. This may happen due to the DNS server being unavailable or because the TTL for the DNS records has expired.

These attempts time out, but the timeout mechanism can cause long delays (for example, 2 minutes) before the phone call proceeds using the working server. To prevent this issue, use long TTLs. Poly recommends deploying an on-site DNS server as part of the redundancy solution.

SIP signaling failure depends on the SIP protocol you use.

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

  If the phone attempts signaling through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it isn't the last server in the list, the phone uses the maximum number of retries using the configurable retry timeout.

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

  1. The phone tries to call the working server.
  2. If the working server doesn't respond correctly to the INVITE, the phone tries the next server in the list. The phone tries even if there's no current registration with these servers. This can happen if the internet connection goes down but the registration to the working server isn't yet expired.
  3. If the second server is also unavailable, the phone tries all possible servers (even those not currently registered) until it either succeeds in making a call or exhausts the list, at which point the call fails.

Server redundancy

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

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

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

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

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

Configure server redundancy for a registered line

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

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

3. Configure the mode for failover/failback. Replace *x* with the desired line key value.

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

The following values apply:

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

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

4. Configure the time to wait, in seconds, before failback occurs. Replace *x* with the desired line key value.

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

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

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

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

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

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

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

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

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

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

8. Configure the SIP server port where the phone sends all requests. Replace *x* with the desired line key value.

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

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

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

   The following values apply:

   - `DNSnaptr` (default)
   - `TCPpreferred`
   - `UDPOnly`
   - `TLS`
   - `TCPOnly`

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

10. Save the configuration file.

Configure server redundancy for VoIP

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the server to register concurrently with other servers. Replace *y* with the desired server key value.

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

3. Set the failback mode to set a timeout. Replace *x* with the desired line key value.

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

4. Enter a time, in seconds, for the server to attempt to connect to the primary servers after a failback. Replace *x* with the desired line key value.

   The default is `3600`. The value range is 0 and 60 to 35535.

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

5. Set how the server fails over.

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

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

6. Set how the server signals a fail over.

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

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

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

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

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

8. Save the configuration file.

IP Multimedia Subsystem Features

Ege E Series phones support several IP Multimedia Subsystem (IMS) server features.

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

Enable 3GPP IP Multimedia

Enable the phone to support any IP Multimedia Subsystem (IMS) features.

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

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

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

1. Open the configuration file.

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

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

3. Save the configuration file.

Enable the P-Early-Media Header

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

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

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

1. Open the configuration file.
2. Do one of the following:
   - Enable the phone to support p-early-media on all outgoing calls.

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

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

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

3. Save the configuration file.

Remove the Outbound Proxy Address from the Route Header

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

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

1. Open the configuration file.
2. Remove the outbound proxy address in the route header. Replace *x* with the registered line number.

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

3. Save the configuration file.

Add Path Extension Header to Request Message

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

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

1. Open the configuration file.
2. Support and include the path extension header field in the Register request message for a registered line. Replace *x* with the registered line number.

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

3. Save the configuration file.

Subscribe to Registered Line State Change Notifications

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

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

1. Open the configuration file.
2. Do one of the following:
   - Subscribe the phone to state change notifications for all lines.

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

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

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

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

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

3. Save the configuration file.

Reject Calls with Network Determined User Busy Events

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

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

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

1. Open the configuration file.
2. Do one of the following:
   - Reject calls when the phone detects an NDUB event on all lines.

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

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

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

3. Save the configuration file.

Include Service Route Information in VQMon Messages

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

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

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to include service route information in VQMon messages.

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

3. Save the configuration file.

Enable Support for the 199 Response Code

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

1. Open the configuration file.
2. Enable support for the 199 response code.

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

3. Save the configuration file.

Enable Advice of Charge

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

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

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

1. Open the configuration file.
2. Display call charge information on the phone.

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

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

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

4. Save the configuration file.

Configure SIP subscription timers

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

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

You can also configure the following options:

- A subscription expiry independently of the registration expiry
- An overlap period for a subscription independently of the overlap period for the registration
- A subscription expiry and subscription overlap for global SIP servers and per-registration SIP servers

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the amount of time, in seconds, after which the phone attempts to resubscribe at the beginning of an overlap period. Replace *x* with the desired server key value. The default value is `60`. The value range is 5 to 65535.

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

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

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

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

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

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

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

6. Save the configuration file.

Configure the SIP instance identification settings

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

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

This feature complies with RFC 3840.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to send *sip.instance* in the REGISTER request for line 1.

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

3. Save the configuration file.

Configure SIP header warnings

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

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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

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

3. Specify a list of accepted SIP warning codes to display. Leave `Null` to enable the phone to accept all warning codes. Separate multiple codes with a comma.

NOTE: Only codes between 300 and 399 are supported.

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

4. Save the configuration file.

DNS SIP Server Name Resolution

Configure DNS SIP server name resolution.

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

If a port is given, the only lookup is an A record. If no port is given, NAPTR and SRV records are tried before falling back on A records if NAPTR and SRV records return no results. If no port is given, and none is found through DNS, port 5060 is used. If the registration type is TLS, port 5061 is used.

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

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

Use the format:

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

This SRV request produces a list of servers ordered by weight and priority, enabling you to specify 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 doesn't remove the sub-domain prefix, for example sip.example.com becomes `_sip._tcp.sip.example.com`. A single SRV query can be resolved into many different servers, session border controllers (SBCs), or partitions ordered by weight and priority, for example, `voice.sip.example.com` and `video.sip.example.com`. Alternatively, use DNS NAPTR to discover what services are available at the root domain.

For Outgoing Calls (INVITE Fallback)

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.

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.

Local digit map

The local digit map feature assists with off-hook dialing and helps the phone conform to a dial plan.

Digit maps consist of a single string or a list of strings. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of RFC 3435.

When dialing a number, the digit map behavior is based on the following:

- Any string of a digit map matches: The phone places the call automatically.
- No string matches: You can specify the phone's behavior.
- The number ends with **#**: You can specify the phone's behavior.

You can specify digit map timeout. This is the time between the caller dialing a number and the phone placing the call.

Configure a local digit map

Specify the digit map used for the dial plan.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

The default digit map is as follows:

```
[2-9]11|0T|+011xxx.T|0[2-9]xxxxxxxxx|+1[2-9]xxxxxxxx|[2-9]xxxxxxxxx|
[2-9]xxxT
```

1. Open the configuration file.
2. Configure the local digit map according to your dial plan.

```
dialplan.digitmap="<digit map string>"
```

3. **Optional:** Configure a line registration-specific digit map. *X* is the value of the specific line or registration.

NOTE: Line registration-specific digit maps take precedence over the global digitmap configuration.

```
dialplan.x.digitmap="<digit map string>"
```

4. Save the configuration file.

Change the dialing timeout

Specify a timeout in seconds for each segment of the digit map. After a user presses a key, the phone waits this many seconds before matching the digits to a dial plan and dialing the call.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Specify the timeout, in seconds, for the digit map. Provide the timeout in a string with positive integers separated by a vertical bar (|).

```
dialplan.digitmap.timeOut="< n|n|n|n|n|n >"
```

3. **Optional:** Specify the timeout, in seconds, for a line registration-specific digit map. Provide the timeout in a string with positive integers separated by a vertical bar (|). *X* is the value of the specific line or registration.

NOTE: Line registration-specific digit maps take precedence over the global digitmap configuration.

```
dialplan.x.digitmap="< n|n|n|n|n|n >"
dialplan.x.digitmap.timeOut="< n|n|n|n|n|n >"
```

4. Save the configuration file.

Change the international dialing prefix

By default, users enter a plus (+) symbol before dialing an international phone number to identify to the switch that they placed an international call. Change the international call prefix to 0 instead of the plus symbol.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Set `0` as the international call prefix.

```
call.internationalPrefix.key="1"
```

3. Require your local country's exit code to place an international call.

```
call.internationalDialing.enabled="0"
```

4. Save the configuration file.

10 Configuring Audio Settings

Configure modifications to the default audio configurations to optimize the audio quality of your phones.

Automatic gain control

Automatic gain control (AGC) boosts the volume of near-end conference participants. AGC is enabled by default to ensure far-end audio clarity.

NOTE: You can't disable this feature. Changing the default settings may cause accessibility concerns for people who use audio augmentation assistive technology.

If you are running an application that also provides AGC through the software, Poly recommends that you disable the application AGC.

Noise suppression

Poly phones offer multiple options to suppress background noise during calls. Some options are integrated into the phone itself, but you can configure others.

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

Poly NoiseBlockAI

The default configuration enables Poly NoiseBlockAI on Poly Edge E Series phones.

Poly NoiseBlockAI suppresses background noise while a call participant actively speaks. It also reduces interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter. Call recipients hear only the intended speaker's voice.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

Disable Poly NoiseBlockAI

Disable Poly NoiseblockAI on your phones.

1. Open the configuration file.
2. Disable Poly NoiseBlockAI.

```
voice.ns.hf.block="0"
```

3. Save the configuration file.

Acoustic Fence

Acoustic Fence technology suppresses background noise sent to the far end. This feature is particularly useful in call center environments where background noise can impact far-end audio quality.

Acoustic Fence works with the following devices:

- Phone handsets
- Wired headsets connected to the headset port
- USB headsets connected to the phone

NOTE: Acoustic Fence doesn't support Bluetooth headsets.

Enable Polycom Acoustic Fence for Handset Calls

Enable Polycom Acoustic Fence for handset calls to remove unwanted background noise from calls.

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.

2. Enable noise suppression for handset calls.

```
voice.ns.hs.enable="1"
```

3. Enable Polycom Acoustic Fence for handset calls.

```
voice.ns.hs.enhanced="1"
```

4. **Optional:** Configure the Polycom Acoustic Fence threshold for handset calls.

   A lower number removes less background noise, while a higher number removes more background noise. The default value is `8`.

```
voice.ns.hs.nonStationaryThresh="<1 to 10>"
```

5. Save the configuration file.

Enable Polycom Acoustic Fence for Headset Calls

Enable Polycom Acoustic Fence for headset calls to remove unwanted background noise from calls.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable noise suppression for headset calls.

```
voice.ns.hd.enable="1"
```

3. Enable Polycom Acoustic Fence for headset calls.

```
voice.ns.hd.enhanced="1"
```

4. Configure the Polycom Acoustic Fence threshold for headset calls.

   A lower number removes less background noise while a higher number removes more background noise. The default value is `8`.

```
voice.ns.hd.nonStationaryThresh="<1 to 10>"
```

5. Save the configuration file.

Add Acoustic Fence Options to the Local Interface

Add the Polycom Acoustic Fence menu items to the phone's **Basic** menu.

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.

2. Enable the **Acoustic Fence** menu item on the phone's local interface.

```
feature.acousticFenceUI.enabled="1"
```

3. Save the configuration file.

Dynamically Deactivate Acoustic Fence in Full-Screen Mode

Enable the phone to dynamically deactivate Acoustic Fence when users change the view to full screen mode in a video call.

1. Open the configuration file.
2. Enable the phone to dynamically deactivate Acoustic Fence when in full-screen mode.

```
video.disableAFOnFullScreen="1"
```

3. Save the configuration file.

Configure VAD

Set the threshold for determining what is considered background noise using Voice activity detection (VAD).

Voice activity detection (VAD) conserves network bandwidth. VAD detects periods of silence in the transmit data path so the phone doesn't transmit unnecessary data packets for outgoing audio.

For compression algorithms without an inherent VAD function, such as G.711,the phone uses the codec-independent processing specified in RFC 3389.

G.711 Appendix II, in RFC 3389, defines the payload format for G.711 use in packet-based multimedia communication systems.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

For more information about VAD, see Voice Activity Detection parameters in the *Parameter Reference Guide*.

1. Open the configuration file.
2. Enable VAD.

```
voice.vadEnable="1"
```

3. Set the VAD threshold in decibels. The default value is `25`.

   Sounds louder than the VAD threshold are considered voice. Sounds below the threshold are considered background and muted from the call.

```
voice.vadThresh="<0 to 30>"
```

4. Save the configuration file.

Comfort noise

Comfort noise ensures a consistent background noise level to provide a natural call experience for speakerphone and handset calls.

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

NOTE: Comfort noise isn't related to the comfort noise packets the phone generates when you enable VAD.

Configure comfort noise for speakerphone calls

Add comfort noise to a hands-free call to ensure that the line isn't completely silent when callers aren't talking.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

Comfort noise provides a minimal level of audio on the line to ensure callers that the call is still connected. You can add and adjust the level of comfort noise for speakerphone and headset calls.

1. Open the configuration file.
2. Enable comfort noise for speakerphone calls.

```
voice.cn.hf.enable="1"
```

3. **Optional:** Adjust the comfort noise level.

   The phone's default value of `30` is quite loud. Enter a higher number to reduce the comfort noise. A lower number increases the comfort noise.

```
voice.cn.hf.attn="<0 to 90>"
```

4. Save the configuration file.

Configure Comfort Noise for Handset Calls

Add comfort noise to a handset call to ensure that the line isn't completely silent when callers aren't talking.

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable comfort noise for handset calls.

```
voice.cn.hs.enable="1"
```

3. **Optional:** Adjust the comfort noise level.

   The default value is `35`.

```
voice.cn.hs.attn="<0 to 90>"
```

4. Save the configuration file.

Enable AEC for Headsets

The default configuration enables acoustic echo cancellation (AEC) for both the handset and speakerphone. Enable AEC for connected Poly Bluetooth headsets to reduce echo during calls.

AEC includes the following features:

- Talk state detector: Determines whether the near-end user, far-end user, or both are speaking.
- Linear adaptive filter: Adaptively estimates the loudspeaker-to-microphone echo signal and subtracts that estimate from the microphone signal.
- Nonlinear processing: Suppresses any echo remaining after the linear adaptive filter.

1. Open the configuration file.
2. Enable AEC for headsets.

```
voice.aec.bt.hd.enable="1"
```

3. Save the configuration file.

Audio codecs

Configure the audio codecs for your phones.

This section provides basic information for configuring audio codecs. For more information on configuring audio codecs, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

Supported Audio Codec Specifications

The following table provices specifications for audio codecs supported on Poly phones.

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

Table 10-1 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.711	RFC 1890	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722 Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16 ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.	RFC 3551	64 Kbps	80 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1	RFC 3047	24 Kbps 32 Kbps	40 Kbps 48 Kbps	16 ksps	20 ms	7 kHz
All systems	G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 ksps	20 ms	14 kHz
All systems	G.729AB	RFC 1890	8 Kbps	24 Kbps	8 ksps	20 ms	3.5 kHz
All systems	Opus	RFC 6716	8 to 24 Kbps	24 to 40 Kbps	8 ksps 16 ksps	20 ms	3.5 kHz 7 kHz

Table 10-1 Audio Codec Specifications (continued)

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

Set audio codec priority

Set the codec priority to improve consistency and reduce workload on the phones.

Note the following about audio codec priority:

- Permitted values to set audio codec priority are 1 to 35.
- `1` is the highest priority.
- A value of `0` or `Null` disables the codec.
- A change to the default value doesn't cause a phone to restart or reboot.

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

If you set G.729 and iLBC to the highest priority, Opus doesn't publish.

The phone doesn't answer calls using unsupported codecs. If the phone receives a call using an unsupported codec, the phone answers the call with the first supported codec priority.

The following values represent the configuration defaults. The default configuration sets the priority values from 1 to 8. All codecs **not** listed in the following table have a default priority value of `0` (disabled).

Table 10-2 Audio Codec Priority Default Values

Parameter	Default Priority
`voice.codecPref.Siren22.64kbps`	1
`voice.codecPref.G7221_C.48kbps`	2
`voice.codecPref.Siren14.48kbps`	3
`voice.codecPref.G722`	4
`voice.codecPref.G7221.32kbps`	5
`voice.codecPref.G711_Mu`	6
`voice.codecPref.G711_A`	7
`voice.codecPref.G729_AB`	8

1. Open the configuration file.
2. Set audio codec priority.

```
voice.codecPref.AMRNB="<priority value>"
voice.codecPref.AMRWB="<priority value>"
voice.codecPref.G711_A="<priority value>"
voice.codecPref.G711_Mu="<priority value>"
voice.codecPref.G722="<priority value>"
voice.codecPref.G7221.16kbps="<priority value>"
voice.codecPref.G7221.24kbps="<priority value>"
voice.codecPref.G7221.32kbps="<priority value>"
voice.codecPref.G7221_C.24kbps="<priority value>"
voice.codecPref.G7221_C.32kbps="<priority value>"
voice.codecPref.G7221_C.48kbps="<priority value>"
voice.codecPref.G729_AB="<priority value>"
voice.codecPref.iLBC.13_33kbps="<priority value>"
voice.codecPref.iLBC.15_2kbps="<priority value>"
voice.codecPref.Lin16.8ksps="<priority value>"
voice.codecPref.Lin16.16ksps="<priority value>"
voice.codecPref.Lin16.32ksps="<priority value>"
voice.codecPref.Lin16.44_1ksps="<priority value>"
voice.codecPref.Lin16.48ksps="<priority value>"
voice.codecPref.Opus="<priority value>"
voice.codecPref.SILK.8ksps="<priority value>"
voice.codecPref.SILK.12ksps="<priority value>"
voice.codecPref.SILK.16ksps="<priority value>"
voice.codecPref.SILK.24ksps="<priority value>"
voice.codecPref.Siren7.16kbps="<priority value>"
voice.codecPref.Siren7.24kbps="<priority value>"
voice.codecPref.Siren7.32kbps="<priority value>"
voice.codecPref.Siren14.24kbps="<priority value>"
```

```
voice.codecPref.Siren14.32kbps="<priority value>"
voice.codecPref.Siren14.48kbps="<priority value>"
```

3. Save the configuration file.

Configure the SILK audio codec

Configure the SILK audio codec settings.

1. Open the configuration file.
2. Set the maximum average encoder output bit rate in kpbs for the supported SILK sample rate. Replace *x* with the sample rate.

   Valid sample rates are 8, 12, 16, and 24.

```
voice.audioProfile.SILK.xksps.encMaxAvgBitrateKbps="<value>"
```

   For example:

```
voice.audioProfile.SILK.8ksps.encMaxAvgBitrateKbps="<value>"
```

3. Specify the SILK encoder complexity. The higher the number, the more complex encoding is allowed. The default is `2`. The value range is 0 to 2.

```
voice.audioProfile.SILK.encComplexity="<value>"
```

4. **Optional:** Enable inband forward error correction (FEC) in the SILK encoder.

NOTE: When you enable this parameter, perceptually important speech information is sent twice: once in the normal bit stream and again at a lower bit rate in later packets. This results in an increased bit rate.

```
voice.audioProfile.SILK.encInbandFECEnable="1"
```

5. Set the SILK encoder expected network packet loss percentage. The default is `0`. The value range is 0 to 100.

NOTE: Configuring this value enables less interframe dependency encoded into the bit stream. This results in increasingly larger bit rates but with an average bit rate less than that configured with `voice.audioProfile.SILK.*`.

```
voice.audioProfile.SILK.encExpectedPktLossPercent="<value>"
```

6. **Optional:** Enable discontinuous transmission (DTX) in the SILK encoder.

NOTE: DTX reduces the encoder bit rate to 0 bps during silence.

```
voice.audioProfile.SILK.encDTXEnable="1"
```

7. Save the configuration file.

Configure the Opus audio codec

Configure the Opus audio codec settings.

1. Open the configuration file.
2. Assign the Opus encoder's application type.

   The following values apply:

   - `VoIP` (Default) - Process signal for improved speech intelligibility
   - `Audio` - Favors faithfulness to original input audio
   - `LowDelay` - Configures the minimum possible coding delay by disabling certain modes of operation

```
voice.audioProfile.Opus.appType="<value>"
```

3. Set the preferred encoder transmit bit rate mode.

   The following values apply:

   - `CVBR` (Default) - Constrained variable bit rate
   - `CBR` - Constant bit rate
   - `VBR` - Variable bit rate

```
voice.audioProfile.Opus.BitrateMode="<value>"
```

4. Set the maximum average encoder output bit rate in kpbs.

```
voice.audioProfile.Opus.encMaxAvgBitrateKbps="<value>"
```

5. **Optional:** Enable decoding of forward error correction (FEC) information sent from the far end.

```
voice.audioProfile.Opus.decInbandFECEnable="1"
```

6. **Optional:** Enable inband forward error correction (FEC) in the Opus encoder.

NOTE: When you enable this parameter, perceptually important speech information is sent twice: once in the normal bit stream and again at a lower bit rate in later packets. This results in an increased bit rate.

```
voice.audioProfile.Opus.encInbandFECEnable="1"
```

7. **Optional:** Set the Opus encoder expected network packet loss percentage. The default is `0`. The value range is 0 to 100.

NOTE: This parameter helps the Opus encoder decide what amount of redundant information to send when you enable inband FEC using `voice.audioProfile.Opus.encInbandFECEnable`.

```
voice.audioProfile.Opus.encExpectedPktLossPercent="<value>"
```

8. **Optional:** Enable discontinuous transmission (DTX) in the Opus encoder.

NOTE: DTX skips packet transmission during periods of silence and only sends periodic frames with comfort noise information.

```
voice.audioProfile.Opus.encDTXEnable="1"
```

9. Save the configuration file.

Poly Computer Audio Connector

The Poly Computer Audio Connector feature requires the following to have PC audio playback on the phone:

- The Poly Computer Audio Connector application must be running on the PC.
- The application must be paired with the phone over the same network.

NOTE: Poly Edge E Series does not support streaming audio from a connected PC over a USB cable.

Configuring Ports for the Poly Computer Audio Connector

The following table lists the ports to configure to use the Poly Computer Audio Connector.

Table 10-3 Poly Computer Audio Connector Ports

Port Number	Type	Description	Direction
25802	UDP	Used for audio streaming.	Bidirectional between phone (on port 25802) and PC (on port 25802)
25801	TCP	The Poly Computer Audio Connector application uses a dynamic port to securely connect over TLS to the phone using Auto (PC port) pairing mode.	TLS connection setup is from PC (on a dynamic port) to the phone (on port 25801). Subsequent communication is bidirectional on the same ports.
25804	TCP	The Poly Computer Audio Connector application uses a dynamic port to securely connect over TLS to the phone when using Manual pairing mode.	TLS connection setup is from PC (on a dynamic port) to the phone (on port 25804). Subsequent communication is bidirectional on the same ports.
2181	UDP	Phones use this port for discovery packet broadcasts.	From phone (on port 2181) to broadcast (on port 2181)

Enable the Poly Computer Audio Connector

Enable the Poly Computer Audio Connector to play computer audio through the phone and use the phone as an HD speaker phone.

1. Open the configuration file.
2. Enable the Poly Computer Audio Connector.

```
feature.computeraudioconnector.enabled="1"
```

NOTE: If `feature.computeraudioconnector.enabled` and `feature.btoe.enabled` are enabled at the same time, the BToE menu takes priority and displays instead. To avoid this conflict, disable `feature.btoe.enabled`.

3. Set the pairing mode for Poly Computer Audio Connector. Permitted values are `Auto` (default) and `Manual`.

   Use `Auto` mode when a computer is connected directly to the phone's PC port. Use `Manual` for all other situations.

   ```
   btoe.pairingMode="<pairing_mode>"
   ```

4. Save the configuration file.

Enable the Poly Computer Audio Connector Using the Local Interface

Use the menus available on the phone's local interface to enable the Poly Computer Audio Connector.

1. Go to **Settings** > **Advanced** > **Administration Settings** > **Audio Connector PC Pairing**.
2. Select **Enabled**.

11 Configuring Call Controls

You can configure calling features for the Poly phone once it's connected to your VoIP network.

Do Not Disturb

Disable Do Not Disturb on one or more phones. You can also configure your phones to automatically enter Do Not Disturb when the lines on your call server enter Do Not Disturb.

Disable Do Not Disturb

Prevent the user from enabling Do Not Disturb (DND) on the phone.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Disable DND on the phone.

```
feature.doNotDisturb.enable="0"
```

3. Save the configuration file.

Enable call server-based Do Not Disturb

Poly phones can enter Do Not Disturb (DND) in sync with the call server using an as-feature-event SIP subscription.

Set `reg.x.serverFeatureControl.localProcessing.dnd="0"` before configuring DND.

The following conditions apply for call server-based DND:

-
- If you enable call server-based DND, but don't turn it on with DND enabled on the phone, the **Do Not Disturb** message displays on the phone but incoming calls continue to ring.
- Call server-based DND disables local call forwarding and DND. However, if an incoming call doesn't route through the server, an audio alert may play on the phone.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable the phone to enter DND based on the call server status.

```
voIpProt.SIP.serverFeatureControl.dnd="1"
```

3. Prevent the phone from allowing a user to enable DND locally. This configures the phone to enable DND via the server only.

```
voIpProt.SIP.serverFeatureControl.localProcessing.dnd="0"
```

4. **Optional:** There is a DND SIP layer modifier applicable to local DND (this is not applicable if `serverFeatureControl` is enabled). When enabled, the phone rejects inbound calls when

DND is on with a **486 Busy** response. When disabled, the phone rejects calls with a **603 Decline** response.

```
call.rejectBusyOnDnd="1"
```

5. Save the configuration file.

Enable call server-based Do Not Disturb on a registered line

Configure the phone to enter Do Not Disturb (DND) in sync with the call server using an as-feature-event SIP subscription on a registered line.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to enter DND based on the call server status. Replace *x* with the desired line key value.

```
reg.x.serverFeatureControl.dnd="1"
```

3. Save the configuration file.

Call hold

Enables users to pause activity on an active call so that they can use the phone for another task.

When an active call is placed on hold, a message displays informing the held party that they are on hold.

Poly phones use the preferred call holding protocols by default, and typically don't require additional configuration.

Configure call hold reminders

Configure the phone to send an audible alert after a call is on hold for a specified amount of time.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable call hold reminders.

```
call.hold.localReminder.enabled="1"
```

3. Set how long the phone waits, in seconds, after placing the call on hold before sounding the reminder. The default is `90`.

```
call.hold.localReminder.startDelay="<number of seconds>"
```

4. Set the amount of time, in seconds, the phone repeats the reminder after the initial reminder sounds. The default is `60`.

```
call.hold.localReminder.period="<number of seconds>"
```

5. Save the configuration file.

Configure hold music

Configure the phone to play streaming music for callers while they wait on hold.

Before you configure these settings, do the following:

- Note the URI of your media stream service.
- Set `reg.x.musicOnHold.uri="NULL"`.
- Set `voIpProt.SIP.musicOnHold.uri="NULL"`.

If supported by the call server, you can enter a music-on-hold URI. For more information, see RFC Music on Hold example.

If the reg-specific value exists, the phone uses it for the line. If not, it uses the global `voIPProt` value.

1. Open the configuration file.
2. Configure the URI for the media streaming service.

```
voIpProt.SIP.musicOnHold.uri="<SIP URI>"
```

3. Save the configuration file.

Change the Reinvite Method

Configure the phone to send an `inactive` stream mode parameter when placing a call on hold.

By default, the phone sends a reinvite message with a stream mode parameter of `sendonly` when placing a call on hold.

NOTE: The phone ignores the value of this parameter if you set `voIpProt.SIP.useRFC2543hold="1"`.

1. Open the configuration file.
2. Configure the phone to send an `inactive` stream mode parameter when placing a call on hold.

```
voIpProt.SIP.useSendonlyHold="0"
```

3. Save the configuration file.

Configure default call transfer type

Set the default call transfer type to **Blind Transfer**.

The following call transfer types are available to the phone's users:

- **Blind Transfer**: Complete a call transfer without speaking with the recipient first.
- **Consultative Transfer (Default)**: Complete a transfer after speaking with the recipient.

1. Open the configuration file.
2. Set the default call transfer type to blind transfer.

```
call.defaultTransferType="Blind"
```

3. Save the configuration file.

Call forwarding

Enable users to automatically forward incoming calls to another contact or phone line.

The phone has many call forwarding options:

- Forward calls when busy
- forward calls when DND is active
- Forward unanswered calls
- Limit call forwarding
- Disable call forwarding

Forward calls while busy

Configure the phone to forward incoming calls to a specified contact when the phone is busy.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to forward calls while busy. Replace *x* with the desired line key value.

```
divert.busy.x.enabled="1"
```

3. Specify the contact you want to forward calls to. Replace *x* with the desired line key value.

```
divert.busy.x.contact="<contact address>"
```

4. Save the configuration file.

Forward calls while DND is active

Configure the phone to forward incoming calls to a specified contact when Do Not Disturb (DND) is active.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to forward calls while DND is active. Replace *x* with the desired line key value.

```
divert.dnd.x.enabled="1"
```

3. Specify the contact you want to forward calls to. Replace *x* with the desired line key value.

```
divert.dnd.x.contact="<contact address>"
```

4. Save the configuration file.

Forward unanswered calls

Configure the phone to forward unanswered incoming calls to a specified contact after a specified amount of time.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to forward an unanswered call. Replace *x* with the desired line key value.

```
divert.noanswer.x.enabled="1"
```

3. Specify how long the phone can ring, in seconds, before forwarding the call. The default is `55`.

```
divert.noanswer.x.timeout="<number of seconds>"
```

4. Specify the contact you want to forward calls to. Replace *x* with the desired line key value.

```
 divert.noanswer.x.contact="<contact address>"
```

5. Save the configuration file.

Disable call forwarding

Remove the **Call Forward** option from the **Features** menu, preventing users from forwarding incoming calls.

1. Open the configuration file.
2. Disable call forwarding.

```
feature.forward.enable="0"
```

3. Save the configuration file.

Convert the call timer to display in seconds

Convert the call timer from HH:MM:SS to only seconds.

A call timer displays on the phone's screen during calls, and a separate call duration timer displays the hours, minutes, and seconds for each call in progress.

1. Open the configuration file.

2. Configure the call time to display in seconds.

```
up.timerDisplayInSeconds="1"
```

3. Save the configuration file.

Call waiting alerts

By default, the phone alerts users to incoming calls during an active call. Disable these call waiting alerts or specify ringtones for incoming calls.

Silence the ringtone for call waiting

If the phone receives an incoming call while in an active call, configure the phone to display the incoming call options on the screen but not to play a ringtone.

1. Open the configuration file.
2. Silence the call waiting ringtone.

```
call.callWaiting.ring="silent"
```

3. Save the configuration file.

Disable call waiting alerts

Disable call waiting alerts so that incoming calls don't disrupt the active call.

The phone alerts you to an incoming call while you are in an active call. Enabling the default (1) notifies the user of a second incoming call after ending the first call.

1. Open the configuration file.
2. Disable call waiting alerts.

```
call.callWaiting.enable="0"
```

3. Save the configuration file.

Configure Call Waiting for a Specific Line

You can configure call waiting for a specific line that uses a distinct ringtone.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Set the ring class for line 1.

```
voIpProt.SIP.alertInfo.1.class="custom1"
```

3. Set the ring value for line 1.

```
voIpProt.SIP.alertInfo.1.value="<ringtone name set by
se.rt.custom1.name value>"
```

4. Save the configuration file.

Use network signaling for caller ID

Configure the phone to get caller identification information from network signaling.

By default, the phone checks an incoming call against the local contact directory for caller identification. If the phone finds a match, the matching contact's name displays. Otherwise, the phone displays the incoming phone number.

The phone can't pull caller ID information from an LDAP corporate directory integration.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the phone to use network signaling to get caller ID information.

```
up.useDirectoryNames="0"
```

3. Save the configuration file.

Enable and configure STIR/SHAKEN caller ID validation

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

When you enable STIR/SHAKEN, the phone validates inbound calls based on SIP headers to help mitigate fraudulent acts such as caller ID spoofing. The caller ID validation values are received from the call server and service provider. If the inbound call fails validation, then the phone displays an icon indicating a suspicious incoming call in the caller ID screen. The user can then choose to accept or reject the incoming call.

This feature is dependent on the call server supporting the SIP signaling that's needed to validate the caller ID. Please check with your ITSP administrator on whether this is a supported feature on the call server.

The STIR/SHAKEN attribute can be included in the From or the P-Asserted-Identity header, as part of the SIP URI or as a header parameter, of the SIP INVITE message for the incoming call. For example:

- `P-Asserted-Identity: "Joe Smith" <sip:1111;verstat=TN-Validation-Failed@mysp.com>`
- `P-Asserted-Identity: "Joe Smith" <sip:1111@mysp.com>;verstat=TN-Validation-Failed`
- `From: "Joe Smith" <sip:1111@mysp.com:5060>;verstat=TN-Validation-Passed;tag=2441792347177936713`
- `From: "Joe Smith" <sip:1111;verstat=TN-Validation-Passed@mysp.com:5060>;tag=24417923471779367133`

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.

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 maximum string length is 256 characters.

   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 maximum string length is 256 characters.

   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 maximum string length is 256 characters.

   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 maximum string length is 256 characters.

   The default value is `NO-TN-VALIDATION`.

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

8. Save the configuration file.

Enable the remote party disconnect alert

Enable the phone to audibly notify users when callers on the far end disconnect from an active call.

1. Open the configuration file.

2. Enable the remote party disconnect alert.

   The following values apply:

   - `messageWaiting`
   - `instantMessage`
   - `remoteHoldNotification`
   - `localHoldNotification`
   - `positiveConfirm`
   - `negativeConfirm`
   - `welcome`
   - `misc1` through `misc7`
   - `custom1` through `custom10`

```
call.remoteDisconnect.toneType="<audio tone value>"
```

3. Save the configuration file.

Voicemail

Configure voicemail on your phones. Voicemail records messages for the users if they can't take an incoming call.

Configure voicemail settings

Configure the phone's voicemail server and voicemail settings.

Note the address for the voicemail server.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the URI for the voicemail subscriber. The phone sends a SUBSCRIBE request when it boots up. Replace *x* with the desired registration value.

```
msg.mwi.x.subscribe="<voicemail subscriber URI>"
```

3. **Optional:** Configure an address to reach out to for message retrieval and notifications. Replace *x* with the desired line key value.

```
msg.mwi.x.callBackMode="contact"
msg.mwi.x.callBack="<message center server URI>"
```

4. **Optional:** Enable the phone's screen backlight to light up when a user receives a voice message.

```
up.mwiVisible="1"
```

5. Save the configuration file.

Disable voicemail

Disable the voicemail feature if you don't use voicemail in your deployment. Disabling voicemail also removes the **Voicemail** button from the main menu.

1. Open the configuration file.
2. Disable voicemail.

```
feature.voicemail.enabled="0"
```

3. Save the configuration file.

Enable local call recording

Local call recording enables the phone to record audio calls to a connected USB device.

NOTE: Federal, state, and local laws may legally require that you notify some or all of the call parties when a call recording is in progress.

When users record their calls, the phone saves the recorded audio calls in WAV format and includes a date/time stamp. Users can then playback the recorded audio on the phone itself or a computer.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable local call recording.

```
feature.callRecording.enabled="1"
```

3. Save the configuration file.

Missed Call Notifications

By default, a counter with the number of missed calls displays on the **Recent Calls** icon on the phone.

For missed call configuration options, see the *Poly Edge E Series Phones Parameter Reference Guide*.

Disable the Recent Calls Softkey

Remove the **Recent Calls** softkey from the phone's local interface.

1. Open the configuration file.
2. Disable the **Recent Calls** softkey.

```
softkey.feature.recentCalls="0"
```

3. Save the configuration file.

Conference call host management

Configure the phone to offer additional call controls when it hosts a conference call.

Note the following:

- By default, when the phone hosting a three-party conference call leaves the call, the remaining call participants transfer to a point-to-point call. You can configure the phone to end the call for all call participants if it's the host and leaves the call.
- If the host of a four-party local conference leaves the conference, all parties disconnect and the conference call ends.
- If the host of a centralized conference leaves the conference, each remaining party remains connected.

For more ways to manage conference calls, see Conference Management.

Enable conference host to place participants on hold

Enable the conference host to place call participants on hold during the conference call.

1. Open the configuration file.
2. Enable the conference host to place participants on hold.

```
call.localConferenceCallHold="1"
```

3. Save the configuration file.

End a conference call when the host disconnects

Configure the phone to end a conference call if the phone is the host and it disconnects from the call.

1. Open the configuration file.
2. Enable the phone to end a conference call if it disconnects.

```
call.transferOnConferenceEnd="0"
```

3. Save the configuration file.

Disable conference management options

Disable the conference management options on the phone so users can only attend meetings as participants. Users can still hold three-way conferences, but conference management options aren't available.

1. Open the configuration file.
2. Disable conference management options.

```
feature.nWayConference.enabled="0"
```

3. Save the configuration file.

Configure automatic dialing

Configure the phone to automatically call a specified number when it goes off-hook.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable automatic off-hook dialing. Replace *x* with the registered line number.

```
call.autoOffHook.x.enabled="1"
```

3. Specify the call recipient for automatic off-hook dialing.

```
call.autoOffHook.x.contact="<contact address>"
```

4. **Optional:** Set the calling protocol for the call.

```
call.autoOffHook.x.protocol="<SIP> or <H323>"
```

5. Save the configuration file.

Configure Directed Call Pickup

Enable users to pick up incoming calls to another phone by dialing the extension of that phone.

This feature requires support from a SIP server, and the setup depends on the SIP server. For example, while some SIP servers implement directed call pick-up using a star-code sequence, others implement the feature using network signaling.

1. Open the configuration file.
2. Enable directed call pickup.

   In this case, the phone sends a SIP Invite with Replaces header.

```
feature.directedCallPickup.enabled="1"
```

3. Specify the directed call pickup method. The default value is `legacy`, which uses the star code configured in `call.directedCallPickupString`.

   Set this parameter to `native` for the phone to use a native protocol method.

```
call.directedCallPickupMethod="<call pickup method>"
```

4. Specify the star code for directed call pickup.

   For call servers other than BroadWorks, change the call pickup string from default. The default string is `*97`.

```
call.directedCallPickupString="<star code>"
```

5. Save the configuration file.

Configure the Call Park and Retrieve Star Code

Enable users to park an active call and retrieve parked calls from the call orbit on any phone.

This feature requires support from a SIP server, and the setup depends on the SIP server. For example, while some SIP servers implement directed call pick-up using a star-code sequence, others implement the feature using network signaling. Call park moves the call to a separate address where any phone can retrieve the call.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Configure the star code to initiate the call park, placing the call into park orbit. The default setting is `*68`.

   Choose a value based on your SIP server settings.

   ```
   call.parkedCallString="<value>"
   ```

2. Configure the star code to initiate retrieval of a parked call.

   Choose a value based on your SIP server settings.

   ```
   call.parkedCallRetrieveString="<value>"
   ```

Configure Last Call Return

Poly phones support the ability to quickly dial the last received call using a star code.

This feature requires support from a SIP server. Many SIP servers implement this feature using a specific star code sequence. When enabled, the phone displays an **LCR** softkey that enables users to call the phone address that last called them.

1. Open the configuration file.
2. Enable the last call returned feature.

   ```
   feature.lastCallReturn.enabled="1"
   ```

3. Specify the star code to dial the last returned call. The default is `*69`.

   ```
   call.lastCallReturnString="<star code>"
   ```

4. Save the configuration file.

Enable the conference meeting Dial-In Options list

Reminders for upcoming meetings include options to easily dial in and join the meeting.

When a meeting invite includes a dial-in number, the **Join** button displays on the meeting and the meeting reminder. By default, the **Join** button dials the first available number if the meeting invite includes more than one possible dial-in number.

When enabled, the phone provides multiple dial-in options when the user taps the **Join** button on the onscreen meeting reminder. The phone displays the following dial-in options to join a meeting:

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

1. Open the configuration file.
2. Enable the phone to present a list of dial-in numbers when users select **Join** on meeting reminders.

```
exchange.meeting.join.promptWithList="1"
```

3. Save the configuration file.

Multiple call appearances

With multiple call appearances, users can place one call on hold, and switch to another call while both calls display on the phone.

This feature is one of several features associated with flexible call appearances. If you assign a registered line to multiple line keys, the default number of concurrent calls applies to all line keys.

Configure the number of line keys per registration

Configure the number of line keys allowed per phone line registration.

1. Open the configuration file.
2. Set the number of line keys allowed for the registered line. The default is `1`. The value range is 1 to 48. Replace *x* with the desired line key value.

```
reg.x.lineKeys="<positive integer>"
```

3. Save the configuration file.

Configure the maximum number of concurrent calls per registration

Configure how many concurrent calls the phone allows per registered line.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

You can set the value for the `reg.x.callsPerLineKey` parameter to a value higher than `1`, for example, `3`. After you set the value to `3`, you can have three call appearances on line 1. By default, any additional incoming calls automatically go to voicemail.

If you set more than two call appearances, a call appearance counter displays at the top-right corner of the phone's screen.

1. Open the configuration file.
2. Set the maximum number of concurrent calls for a single registration, *x*. This parameter applies to all line keys using registration *x*.

NOTE: If registration *x* is a shared line, an active call counts as a call appearance on all phones sharing that registration. This parameter overrides the setting for `call.callsPerLineKey`.

```
reg.x.callsPerLineKey="<positive integer>"
```

3. Save the configuration file.

Shared lines

Configure phones to use shared lines and options available to phones on a shared line.

Some office layouts require numerous phones to ring for incoming calls. Shared lines are helpful for teams that handle a high volume of incoming calls, such as a customer service call center.

Enable a shared line

Add a line to multiple phones for teams that benefit from a shared line, such as a call centers.

1. Open the configuration file.
2. Specify the user or the user and host part of the registration SIP URI or the H.323 ID/extension. Replace *x* with the desired line key value. The default is `Null`.

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

3. Set the call signaling type to `Shared`. Replace *x* with the desired registration value.

```
reg.x.type="shared"
```

4. Save the configuration file.

Shared call appearances

Shared call appearance (SCA) enables calls to display all call states—active, inactive, and hold—simultaneously on multiple phones in a group.

To enable SCA on your phone, you must obtain a shared line address from your SIP service provider or configure a shared line address on your phones. SCA is dependent on support from a SIP call server. Poly devices support SCA using the SUBSCRIBE-NOTIFY method specified in RFC 6665.

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

Configure line-seize on shared lines

Enable a shared line user to take control of a line before placing a call.

1. Open the configuration file.
2. Configure the number of line-seize retries. The default is `10`. The value range is 3 to 10.

```
voIpProt.SIP.lineSeize.retries="<value>"
```

3. Configure the line to immediately provide a dial prompt without waiting for the 200 OK registration message. Replace *x* with the registered line number.

```
reg.x.strictLineSeize="1"
```

4. Configure the line-seize timeout, in seconds. After the timeout period a seized line returns to an idle state. Replace *x* with the registered line number. Replace *y* with the desired server key value. The default is `30`. The value range is 0 to 65535. A value of `0` means the line-seize doesn't expire.

```
reg.x.server.y.expires.lineSeize="<line-sieze timeout>"
```

5. Save the configuration file.

Enable call diversion on shared lines

Enable users to divert incoming shared line calls to another line.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable call diversion for shared lines. Replace *x* with the registered line number.

```
divert.x.sharedDisabled="0"
```

3. Enable call forwarding for shared lines.

```
call.shared.disableDivert="0"
```

4. Save the configuration file.

Immediately reject incoming calls on shared lines when on DND

Immediately reject calls to a shared line while the phone is on DND.

IMPORTANT: Configuriguring this parameter will override `call.shared.displayalertwhendnd`.

1. Open the configuration file.
2. Enable call rejection for shared lines.

```
call.shared.rejectDndImmediately="1"
```

3. Save the configuration file.

Enable barge-in on a shared line

Configure phones sharing a line to barge-in on active call.

NOTE: Not all call servers support barge-in on shared lines. Check to make sure it's supported on your call server.

1. Open the configuration file.
2. Enable call barge-in on a specific line. Replace *x* with the registered line number.

```
reg.x.bargeInEnabled="1"
```

3. Save the configuration file.

Configure unique outbound caller IDs on shared lines

Configure unique outbound caller IDs for each appearance of a shared line.

When a shared line is populated across several line keys of the phone, calls that users make from different line keys can send call control service preferences for unique outbound caller IDs, depending on which line appearance is used. The caller ID preference follows the tel, sip, and name-addr format, which you can configure to insert in to either the P-Asserted or P-Preferred identity header.

1. Open the configuration file.
2. Configure the caller ID preferences.

```
voIpProt.SIP.perLineCallerId.header="<HeaderType>"
```

- <HeaderType> can be PAssertedID (default) or PPrefferredID.

```
reg.X.line.Y.callerID="<callerid>"
```

- X represents the SIP registration index and Y represents the line appearance index.
- The <callerID> value must be in the name-addr format and include escaped characters, such as quotation marks or angle brackets, where appropriate.

Example:

```
voIpProt.SIP.perLineCallerId.header="PAssertedID"
reg.1.line.1.callerid="&lt;sip:+155512345678.service.com&gt;"
reg.1.line.2.callerid="&lt;sip:+12053361XXX@10000191.service.com&gt;"
reg.1.line.3.callerID="&lt;tel:+15551234567&gt;"
```

3. Save the configuration file.

Enable private hold on shared lines

Private hold enables users on a shared line to hold a call, transfer a call, or initiate a conference call. The shared line displays as busy to other users sharing the line.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable private hold on the shared line. Replace *x* with the registered line number.

```
reg.x.enablePvtHoldSoftKey="1"
```

3. Save the configuration file.

Set a Ring Delay Timer for Incoming Calls

You can set a timer to delay ringing on incoming calls.

1. Open the configuration file.
2. Set the timer, in seconds, to delay ringing. The value range is 0 to 75.

   When set, the timer withholds all visual and audible information from the user until it elapses.

```
reg.1.ringdelay="<Value>"
```

3. Save the configuration file.

SIP-B Automatic Call Distribution

SIP-B automatic call distribution enables you to use your phones in a call center agent/supervisor role on a supported call server.

This feature supports automatic call distribution (ACD) agent availability, which depends on support from a SIP server.

Enable ACD

Enable the automatic call distribution (ACD) feature on a phone and registered lines.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable ACD login/logout.

```
feature.acdLoginLogout.enabled="1"
voIpProt.SIP.acd.signalingMethod="0"
```

3. Enable ACD login/logout on a registered line. Replace *x* with the registered line number.

```
reg.x.acd-login-logout="1"
reg.x.acd-agent-available="1"
```

4. Save the configuration file.

Simplify ACD State Controls

Configure the phone to hide the ACD softkeys and certain menu options to simplify how users interact with their phone.

The phone hides the following softkeys:

- **ASignIN**
- **ASignOut**
- **Available**

Enabling this parameter also hides menu items found in **Menu** > **Settings** > **Feature** > **ACD**.

1. Open the configuration file.

2. Hide the ACD softkeys and menu options.

```
acd.simplifiedAgentStateControl="1"
```

3. Save the configuration file.

Configure bridged line appearance

Connect calls and lines to multiple phones.

You must get a registered address dedicated for use with your call server provider. In the configuration files, shared lines configure bridged lines. Bridged line appearances don't support the barge-in feature.

IMPORTANT: Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The methods you use vary with the SIP call server you use.

With bridged line appearance enabled, an active call displays simultaneously on multiple phones in a group. By default, the answering phone has sole access to the incoming call. If the answering phone places the call on hold, that call becomes available to all phones of that group. The call state, active, inactive, and held, displays on all of the phones.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

- Assign your registered address to the correct phone line and third-party name. Replace *x* with the desired line key value.

```
reg.x.address="<registered address>"
reg.x.thirdPartyName="<registered address>"
```

Extend the amount of time the expanded call view displays

Extending the viewing time of all calls accessed by a press and hold of a selected line key.

You can now configure the length of time the expanded call view displays on the phone. The timeout option is extended to a maximum of 30 seconds to see which calls remain behind a line key and the actions associated with them.

1. Open the configuration file.
2. Set the length of time the expanded call view displays. The default is 8, and the range is from 5 to 30 seconds.

```
up.lineKeyCallView.Timeout="8"
```

3. Save the configuration file.

Configure bridged line appearance

Connect calls and lines to multiple phones.

You must get a registered address dedicated for use with your call server provider. In the configuration files, shared lines configure bridged lines. Bridged line appearances don't support the barge-in feature.

IMPORTANT: Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The methods you use vary with the SIP call server you use.

With bridged line appearance enabled, an active call displays simultaneously on multiple phones in a group. By default, the answering phone has sole access to the incoming call. If the answering phone places the call on hold, that call becomes available to all phones of that group. The call state, active, inactive, and held, displays on all of the phones.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

- Assign your registered address to the correct phone line and third-party name. Replace *x* with the desired line key value.

```
reg.x.address="<registered address>"
reg.x.thirdPartyName="<registered address>"
```

Busy Lamp Field

The busy lamp field (BLF) attendant console feature enhances support for phone-based monitoring. When you enable BLF, a BLF line key icon displays on the phone screen for users monitoring remote phones. The BLF line key displayed indicates that BLF-related features are available.

BLF Feature Options

There are numerous BLF feature options available on Poly phones.

You can configure the following feature options for BLF:

- Line key labels
- Enhanced feature keys
- Call appearances display (monitoring)
- Call waiting audio notifications
- Caller ID information display
- One-touch call park and retrieve
- One-touch directed call pickup

SIP Server Support for BLF Configurations

This feature requires support from a SIP server, and the setup depends on the SIP server.

When using BLF with a call server, the initial BLF subscription can receive large responses as the number of monitored resources increases. You may need to consult your SIP server partner or Poly channel partner to find out how to configure BLF feature options.

Typically, call servers support one of two methods of BLF configuration:

- Subscribing to a BLF resource list set up on your call server
- Entering BLF resources to a configuration file and the call server directs the requests to those BLF resources

Subscribe to a Busy Lamp Field Resource List on a Call Server

To subscribe a phone to a BLF resource list on a call server, access the call server and set up a list of monitored resources. Add a phone to the resource list by providing it with the call server address.

NOTE: When you configure this feature, the phone ignores individually addressed users configured by `attendant.resourceList` and `attendant.behaviors`.

1. Open the configuration file.
2. Enter the SIP URI for the BLF resource list on the call server.

```
attendant.uri="<SIP URI>"
```

3. **Optional:** To ensure reliable transmission, Poly recommends using Transmission Control Protocol (TCP) for BLF. Add TCP to the attendant URI.

```
attendant.uri="<SIP URI>;transport=tcp"
```

4. Save the configuration file.

Configure a Busy Lamp Field Resource in the Configuration File

To specify BLF resources, enter the address of the BLF resource of the monitored contact, the label that displays beside the line key on the phone, and the resource's type. You can configure up to 50 BLF resources.

A single SIP server has multiple registrations available. Your call server must support dialog event packages to configure BLF resources using this method, as defined in RFC 4235.

NOTE: This process covers the basic setup steps for a single BLF resource entry. See the *Poly CCX Parameter Reference Guide* for more information on the available configuration parameters.

1. Open the configuration file.
2. Specify the line registration to use to subscribe to the BLF resource list. Permitted values for the line registration index are 1 to 34.The default index is `1`.

```
attendant.reg="<index number>"
```

3. Specify the new resource address. Replace *x* with the resource's BLF index number.

```
attendant.resourceList.x.address="<SIP URI address>"
```

4. **Optional:** Configure the resource call signaling address if it's different than the one configured in `attendant.resourceList.x.address`. Replace *x* with the resource's BLF index number.

```
attendant.resourceList.x.callAddress="<SIP URI calling address>"
```

5. Configure a label to display adjacent to the associated line key. The default value is `null`. Replace *x* with the resource's BLF index number.

   If you leave this value as `null`, the label displays as the user portion of the address set in `attendant.resourceList.x.address`.

```
attendant.resourceList.x.label="<label>"
```

6. Configure the resource type (the type of resource being monitored and the default action to perform when pressing the line key). Replace *x* with the resource's BLF index number.

   The default type is `normal` for users' phones, but you can set the type as `automata` if the resource is similar to a call orbit.

   When the type is normal, selecting the BLF key will place a call to the BLF when the phone is idle or in a call. When the type is automata, selecting the BLF key will initiate a blind transfer to the BLF when the phone is in a call.

```
attendant.resourceList.x.type="<resource type>"
```

7. **Optional**: Customize the SIP account used for call and subscription operations per BLF line.

```
attendant.resourceList.x.reg="1"
```

The value of this parameter references index "y" in the parameter `reg.y.address` to determine which phone registration is used for SIP signaling operations by the BLF resource. If the parameter isn't configured, the BLF resource uses the value from `attendant.reg` for SIP operations.

8. **Optional:** Configure the ring tone for the BLF.

```
attendant.resourceList.x.ringType="<ringType>"
```

9. Configure the display pop-up when the BLF has an incoming call. The default is auto.

Permitted values are the following:

- auto (based on global settings of `attendant.behaviors.display.spontaneousCallAppearances.normal` for normal type and `attendant.behaviors.display.spontaneousCallAppearances.automata` for automata type)
- show
- hide

```
attendant.resourceList.x.display.spontaneousCallAppearances="<value>"
```

10. **Optional:** Configure whether the phone disallows parking/transferring the call to the resource if the resource is busy. This is primarily for park orbit resources. The default is 0 (disabled).

```
attendant.resourceList.x.rejectParkOnBusy="1"
```

11. **Optional:** Configure the hold ring tone for the resource. Consult your call server provider to see if this feature is supported. The default value is ringer11.

```
attendant.resourceList.x.hold.ringer="<ringer>"
```

12. Save the configuration file.

Enable SIB-B Group Call Pickup

This feature enables users to pick up incoming calls to any phone within a predefined group of phones, without dialing the extension of another phone.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

This feature requires support from a SIP server and setup of this feature depends on the SIP server.

For example, while some SIP servers implement group call pick-up using a particular star-code sequence, others implement the feature using network signaling.

- Enable SIP-B group call pickup.

```
feature.groupCallPickup.enabled="1"
```

Enable Instant Messaging

Send and receive instant text messages through your phone.

Support for instant messaging varies by call server. Consult your SIP server partner to find out if it supports this feature.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable instant messaging.

```
feature.messaging.enabled="1"
```

3. Save the configuration file.

PTT and Group Paging

Push-to-talk (PTT) and group paging enable users to transmit messages and announcements to configured and subscribed channels.

PTT

PTT is a collaborative tool that enables users to exchange broadcasts to users subscribed to any of the 25 PTT channels, much like a two-way radio. Users transmit pages and PTT broadcasts using a handset, headset, or speakerphone. PTT broadcasts play on the speakerphone, handset, and headset.

In PTT mode, the phone behaves like a walkie-talkie. Users can broadcast audio to a PTT channel and recipients subscribed to that channel can respond to messages.

Group Paging

Group paging enables users to send announcements to recipients subscribed to any of the 25 paging groups. Announcements play through the phone's speakerphone.

Administrators must enable paging before users can subscribe to a page group. You can specify the same IP multicast address in the parameter `ptt.address` for both PTT and group paging modes.

Configure phones to receive group pages

Configure phones to receive pages sent from certain specified phone groups.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable group paging.

```
ptt.pageMode.enable="1"
```

3. Subscribe the phone to a specific group, and enable it to receive pages. Repeat these parameters for each group that you want the phone to receive pages from.

```
ptt.pageMode.group.x.subscribed="1"
```

4. Enable the phone to receive pages from subscribed groups.

```
ptt.pageMode.group.x.allowReceive="1"
```

5. **Optional:** Enable the phone to play paging messages when in an active call.

```
ptt.pageMode.allowOffHookPages="1"
```

6. Save the configuration file.

Configuring PTT

Configure the push-to-talk (PTT) settings and channels for your phone.

Enable and Configure PTT

Enable push-to-talk (PTT) and configure how the phone uses available channels.

1. Open the configuration file.
2. Enable PTT on the phone.

```
ptt.pttMode.enable="1"
```

3. Subscribe the phone to a channel. Channel numbers are 1 to 25. Replace *x* with the number of the channel.

   For example, channel 1 is `ptt.channel.1.subscribed`. All phones subscribed to the same channel can receive PTT messages from other phones subscribed on a channel.

```
ptt.channel.x.subscribed="1"
```

4. Set the default channel to use for PTT transmissions. Channel numbers are 1 to 25.



NOTE: The default channel is 1.

```
ptt.defaultChannel="<channel number>"
```

5. **Optional:** Set the volume of the page without changing normal call volume. The default is -20.

```
ptt.volume="<number between -57 and 0>"
```

6. **Optional:** Enable the phone to play PTT messages while in an active call. By default, the PTT message plays after the user accepts it.

```
ptt.allowOffHookPages="1"
```

7. Save the configuration file.

Block a Phone from Sending Outgoing PTT Calls

Prevent a phone from sending out PTT calls on certain channels. Phones can still receive PTT messages on the channel.

This feature is useful for phones placed in common areas where users may need to hear PTT messages from a certain channel but not send any.

1. Open the configuration file.
2. Block the phone from sending PTT calls on a certain channel. Replace *x* with the number of the channel.

```
ptt.channel.x.allowTransmit="0"
```

3. Save the configuration file.

Add a Label to a PTT Channel

The channel's label displays on the phone when it sends or receives PTT calls.

1. Open the configuration file.

2. Add a label to a channel. Replace *x* with the number of the channel. You can enter up to 64 characters in your label.

```
ptt.channel.x.label="<channel name>"
```

3. Save the configuration file.

Add a Label to a Specific PTT Group

The group label displays on the phone when it sends or receives PTT calls.

1. Open the configuration file.
2. Add a label to a specific group. Repeat this parameter for each group label.

```
ptt.pageMode.group.x.label="<string>"
```

3. Save the configuration file.

Configure an Emergency PTT Channel

Specify a channel to use for emergency PTT messages.

NOTE: The default emergency channel is 25.

1. Open the configuration file.
2. Specify the emergency PTT channel.

```
ptt.emergencyChannel="<channel number>"
```

3. Set the emergency page audio volume relative to the maximum speakerphone volume of the phone.

   Positive values are louder than the maximum and negative values are quieter. The gain to use for emergency page/PTT is the maximum termination gain plus this parameter.

```
ptt.emergencyChannel.volume="<volume variance value>"
```

4. Save the configuration file.

Configure the PTT Group to Use for Emergency Pages

You can specify the PTT group to use for emergency pages.

1. Open the configuration file.
2. Specify the group the phone uses for emergency pages. The default is group 25.

```
ptt.pageMode.emergencyGroup="<group number>"
```

3. Save the configuration file.

Change the IP Multicast Address and Port

Specify the IP multicast address and port for both PTT and group paging.

NOTE: The PTT and group paging features use an IP multicast address. If you want to change the default IP multicast address, make sure that the new address doesn't already have an official purpose as specified in the IPv4 Multicast Address Space Registry.

For more information on PTT and group paging multicast packets, see the *Polycom UC Software PTT/ Group Paging Audio Packet Format Engineering Advisory 70568* at the Poly Online Support Center.

1. Open the configuration file.
2. Enter the new multicast IP address.

```
ptt.address="<IP address>"
```

3. Enter the new port to send and receive PTT and group pages. The value ranges from 0 to 65535.

```
ptt.port="<port>"
```

Intercom calls

Configure intercom networks between multiple phones in your organization.

When users place an intercom call, the dialed contact's phone automatically answers it. Users can quickly pass information to others without interrupting their task to answer the incoming call. An example of useful intercom calls is to notify users that there's another call on hold for them.

Enable intercom calls

Enable the phone to place intercom calls.

This is a server-independent feature, provided the server doesn't alter the Alert-Info header sent in the INVITE.

1. Open the configuration file.
2. Enable intercom calls.

```
feature.intercom.enable="1"
```

3. Add the **Intercom** icon to the phone's *Home* screen.

```
homeScreen.intercom.enable="1"
```

4. **Optional:** Enter the string for the Alert-Info header.

   You can use the following special characters: *@*, -, _, or . . The default is `Intercom`.

```
voIpProt.SIP.intercom.alertInfo="<alphanumeric string>"
```

5. **Optional:** Encapsulate the Alert-Info header set by the `voIpProt.SIP.intercom.alertInfo` parameter with angular brackets ("<" and ">").

```
voIpProt.SIP.intercom.alertInfo.encapsulateWithAngleBrackets="1"
```

6. Save the configuration file.

Creating a custom intercom softkey

Use a custom intercom softkey to initiate intercom calls directly to a specified contact using enhanced feature keys (EFKs).

The **Intercom** softkey displays on the phone by default. You don't have to disable the default **Intercom** softkey to create a custom softkey. You can create an intercom action string for a custom softkey in one of the following ways:

- *<number>*`$Tintercom$`
  A T-type macro that enables you to specify a direct intercom button that always calls the number you specify in *<number>*. This doesn't require additional input.
- `$FIntercom$`
  An F-type macro that behaves as a custom Intercom softkey. The softkey opens the **Intercom** dial prompt to place an intercom call by entering the destination's digits and using a speed dial or BLF button.

MLPP for AS-SIP

Multilevel Precedence and Preemption (MLPP) enables you to configure a precedence level for calls, which is implemented in accordance with the standards set by Assured Services for Session Initiation Protocol (AS-SIP).

Higher precedence calls preempt active calls with a lower precedence level. When the phone receives a call with a higher precedence level than the active call, the phone plays the preemption tone and displays a preemption screen. The user can then answer the incoming higher-precedence call or reject the call. If the user doesn't acknowledge the incoming call, the notification disappears, the current call ends, and the phone answers the incoming call.

MLPP Incoming Call Behavior

MLPP treats incoming calls with the same precedence level as the active call. However, the phone behavior depends on the call state and how many calls are allowed on each line. The phone uses the following precedence rules for incoming calls:

- If only one call is allowed per line, the phone rejects an incoming call with the same precedence level as the active call.
- If multiple calls are allowed per line, then the phone takes the following actions:
  - If the user accepts the new call, it's placed in the first slot. The active call is then placed on hold and moved to the second slot.
  - If all lines and call appearances are at capacity, the phone rejects an incoming call with the same precedence level as the active call.
  - If there is a call on hold and the user acknowledges the new call, the held call is moved to the second slot, and the new call is placed in the first slot.

MLPP with Shared Lines

The phone uses the following precedence rules for shared lines:

- An incoming higher-precedence call preempts the active call.
- If a lower-precedence call is on hold, the preemption screen for the current call doesn't display.

NOTE: Poly recommends that you don't change the default value of the `callsPerLineKey` parameter, which may result in the MLPP feature not working properly for shared lines.

MLPP with Call Transfer

The phone uses the following precedence rules for call transfers:

- **Blind transfer** – Call precedence isn't sent when you perform a blind transfer.
- **Consultative transfer** – Calls sent via consultative transfer are sent with the highest precedence level between the caller and the user transferring the call.

MLPP with Conference Calls

Conference calls occupy one call appearance and are treated as a single call. The phone displays the precedence level of each participant. The precedence level of the conference is determined by the precedence level of the participant with the highest precedence on the call.

New calls received during a conference call are handled according to their precedence levels.

Enable AS-SIP

Enable AS-SIP before configuring MLPP features.

1. Open the configuration file.
2. Enable AS-SIP.

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

3. Save the configuration file.

Set Call Priority and Precedence Levels

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the default priority level for outgoing calls.

```
voIpProt.SIP.assuredService.defaultPriority="<value>"
```

NOTE: The phone overrides this value if it assigns priority from the dial plan for that number.

3. Set the minimum priority level for precedence calls.

```
voIpProt.SIP.assuredService.precedenceThreshold="<value>"
```

4. Save the configuration file.

Setting Call Precedence with a Digit Map

Aside from setting call precedence on the server, you can also configure a digit map in a dial plan to set a number prefix and a namespace. If you enable MLPP and don't configure a precedence level to a number, the phone sends the call at the default precedence level.

Digit Map Configuration

```
dialplan.digitmap=3xxxTP4|4xxxTP5
```

All digits matching the pattern 3xxxTP4 and 4xxxTP5 are sent with precedence 4 and 5 respectively. In this example:

- If the user dials 3434 the call is sent with precedence 4.
- If the user dials 3345 the call is sent with precedence 4.
- If the user dials 4666 the call is sent with precedence 5.

If the dialed number doesn't match any number, then the default precedence is sent based on the value you set with `voIpProt.SIP.assuredService.defaultPriority`.

Set the Preemption Screen Display Time

The preemption screen informs the user that the current call was preempted and displays an **OK** button to acknowledge the preemption. Configure how long the preemption screen displays when a user receives an incoming call with a higher precedence.

If the time for the preempted screen is `0` seconds, then the preemption screen displays until the callee presses the **OK** button.

If a lower-precedence call is on hold and a user receives a higher-precedence call, the preemption screen doesn't display and the preemption tone doesn't play.

1. Open the configuration file.
2. Set the preemption screen display time for the callee's phone. The default time for the preemption screen is 0 seconds for the callee.

```
voIpProt.SIP.assuredService.preemptionAutoTerminationDelay.local="<value>"
```

3. Set the preemption screen display time for the caller's phone. The default time for the preemption screen is 3 seconds for the callee.

```
voIpProt.SIP.assuredService.preemptionAutoTerminationDelay.remote="<value>"
```

4. Save the configuration file.

Configure a Custom Namespace for Precedence Calls

Set the namespace label, priority, and AS-SIP scheme for precedence calls.

1. Open the configuration file.
2. Enter a name for the custom namespace label.

```
voIpProt.SIP.assuredService.namespace.custom.name="<value>"
```

3. Enter the precedence values, from lowest to highest, for the namespace.

```
voIpProt.SIP.assuredService.namespace.custom.priority.x="<value>"
```

4. Enter the namespace scheme to use in SIP signaling.

```
voIpProt.SIP.assuredService.namespace="<value>"
```

5. Save the configuration file.

Precedence Display by Phone Model

The caller's phone displays the precedence of the outgoing call. Callee phones display call precedence on each phone line. Phone models vary in how they display precedence.

In the following list, 1 indicates the lowest precedence and 5 indicates the highest precedence.

- Edge E100/E220: P-1, P-2, P-3, P-4, P-5
- Edge E300 Series: P-1, P-2, P-3, P-4, P-5

- Edge E400 Series: Priority-1, Priority-2, Priority-3, Priority-4, Priority-5
- Edge E500 Series: Priority-1, Priority-2, Priority-3, Priority-4, Priority-5

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.

Table 11-1 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.

VQMon reports

Generate multiple types of performance metrics using the Voice Quality Monitoring (VQMon) parameters.

You can enable three types of voice quality reports:

- Alert – Generated when the call quality degrades below a configurable threshold.
- Periodic – Generated during a call at a configurable period.
- Session – Generated at the end of a call.

Some reports are based on current values, such as jitter buffer nominal delay and round trip delay, while others cover the time period from the beginning of the call until the report is sent, such as network packet loss. The phone generates some metrics using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

Configure VQMon alerts

Configure settings used to generate VQMon alert reports.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Specify the threshold value of listening MOS score (MOS-LQ) that causes the phone to send a critical alert quality report.

   The default is `0`. The value ranges from 0 to 40.

   `voice.qualityMonitoring.collector.alert.moslq.threshold.critical="x"`
3. Specify the threshold value of listening MOS score (MOS-LQ) that causes phone to send a warning alert quality report.

   The default is `0`. The value ranges from 0 to 40.

   `voice.qualityMonitoring.collector.alert.moslq.threshold.warning="x"`
4. Specify the threshold value of one way-delay, in milliseconds, that causes the phone to send a critical alert quality report.

   The default is `0`. The value ranges from 0 to 2000.

   `voice.qualityMonitoring.collector.alert.delay.threshold.critical="x"`

   NOTE: One-way delay includes both network delay and end system delay.
5. Specify the threshold value of one-way delay, in milliseconds, that causes the phone to send a critical alert quality report.

   The default is `0`. The value ranges from 0 to 2000.

```
voice.qualityMonitoring.collector.alert.delay.threshold.warning="x"
```

NOTE: One-way delay includes both network delay and end system delay.

6. Save the configuration file.

Configure VQMon reports

Configure the settings used to generate periodic- and session-based VQMon reports.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable periodically generated reports throughout the call.

```
voice.qualityMonitoring.collector.enable.periodic="1"
```

3. Enable reports to generate after the call.

```
voice.qualityMonitoring.collector.enable.session="1"
```

4. Configure the state that triggers the report.
   - `0` (Default) - Alert states do not cause periodic reports to be generated.
   - `1` - Periodic reports are generated if an alert state is critical.
   - `2` - Period reports are generated when an alert state is either warning or critical.

NOTE: The phone ignores this parameter when you enable `voice.qualityMonitoring.collector.enable.periodic`, since reports are sent throughout the duration of a call.

```
voice.qualityMonitoring.collector.enable.triggeredPeriodic="<value>"
```

5. Configure the time interval, in milliseconds, between successive periodic quality reports.

   The default is `20`. The value range is 5 to 900.

```
voice.qualityMonitoring.collector.period="<value>"
```

6. Save the configuration file.

12 Configuring emergency services

Emergency service settings allow you to customize how your phone and contacts help reach emergency services in a crisis.

Enhanced 911

Poly phones support Enhanced E911 (E911) location-based services. This feature is critical to enable accurate phone routing when users make emergency calls.

The Enhanced 911 (E.911) feature enables the phone to obtain location information to share with responders when users dial 911 to report an emergency. This ensures that the operator dispatches emergency services to the correct location.

Silent distress call

Known as a silent alarm or panic button, distress calls provide emergency responders with important information until you're safe to speak. Schools and academic institutions may use the distress call feature to aid in compliance with US legislation under Alyssa's Law.

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.

Manually Set the Phone's Location for Emergency Calls

Users can manually set their location for emergency calls on the phone's local interface.

Register the phone.

1. Go to **Settings** > **Status** > **Diagnostics** > **Warnings**.
2. Select **Details** to enter a location to the location tree navigation menu.
3. Choose a location and press **Save**.
4. To confirm the setting, go to **Status** > **Location Information**.

   The location information displays in the **Status** menu.

Configure E.911 Location for Ribbon Communications

Enable the Ribbon Communications E.911 feature on the phones and associate them with locations configured in your Ribbon location server. The phone's location can help dispatchers determine where to send responders during an emergency call.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the Ribbon Communications E.911 feature on the phone.

```
feature.genband.E911.enabled="1"
```

3. Enter a description for the phone's location. This description must match the description configured on the location server. For example, *cubicle 105*. The default value is *Other*. The maximum string length is 255 characters.

```
genband.E911.location.description="<description>"
```

4. Enter the location ID corresponding to the location description you entered for the `genband.E911.location.description` parameter. The ID must match the ID configured on the location server. The default value is `0`. The maximum string length is 255 characters.

```
genband.E911.location.locationID="<Ribbon Location ID>"
```

5. Configure the registered line to use to retrieve E.911 location information. The default is `1`. You can set from *1* to *100* for the registered line.

```
genband.E911.registration.line="<registration index>"
```

6. **Optional:** Set the XML schema used during the SIP invite to comply with RFC 5139.

NOTE: Default setting is *RFC4119*.

```
feature.E911.locationInfoSchema="RFC5139"
```

7. Save the configuration file.

Configure Emergency Instant Messages

Enable incoming emergency instant messages and configure how long they display.

Messages display until one of the following occurs:

- The phone times out.
- The phone receives another instant message.
- A dialog message displays.
- The phone receives an incoming call.
- The user presses any key or message on the phone.

1. Open the configuration file.
2. Enable the phone to display emergency instant messages.

```
feature.instantMessaging.enabled="1"
```

3. **Optional:** Configure the timeout, in minutes, the emergency instant messages display on the phone's screen.

   The default is `1`. The value range is 1 to 60.

```
feature.instantMessaging.displayTimeout="<# of minutes>"
```

4. **Optional:** Silence the emergency instant message ringtone.

```
feature.instantMessaging.ring="Silent"
```

5. Save the configuration file.

Silent distress call

In emergency situations, a silent distress call can discreetly provide emergency responders with important information.

NOTE: Silent distress call options are only available in the Poly's OpenSIP app. It is not configurable on the Microsoft Teams or Zoom app.

Known as a silent alarm or panic button, distress calls provide emergency responders with important information until you're safe to speak. Schools and academic institutions may use the distress call feature to aid in compliance with US legislation under Alyssa's Law.

Distress numbers apply unique behaviors when dialed, invoked from a speed dial or custom softkey:

- Triggered distress calls start as one way only unless the handset is offhook. The handsfree microphone sends audio from the room to first responders while incoming audio is blocked until the user presses the soft key labeled as **2-way** or the handset is lifted.
- LEDs and active call screens are dimmed hiding the fact a distress call is active.

  The Edge E series call controls are reduced to only an End Call and 2-way audio toggle. Typical keys for actions like conference, hold, and transfer that can interrupt the call are removed.
- A distress call will temporarily disable advanced audio treatments like Poly NoiseblockAI so that all in-room sound is sent to the far end unfiltered.
- Any call already active or on hold when a distress call is triggered will be ended.
- Inbound calls while a distress call is active are permitted and can be answered, rejected or forwarded as normal using the typical call appearance UI. On handling or ending the inbound call, the distress call will be immediately resumed.
- An optional text to speech (TTS) message is available on the Edge E series which can be configured to repeat a set number of times or indefinitely after a call connects. Switching to 2-way audio will stop the TTS message.
- Accidental dial protection can be added when a speed dial is configured as a distress call by delaying the call start with visible options to cancel it during the delay period or by requiring the press and hold of the speed dial button before the distress call is triggered.
- Accidental dial protection when distress calls are configured as custom softkeys or EFKs can offer a delayed call start with visible options to cancel it during the delay period. Distress call dial protection using a press and hold is not available for custom softkeys or EFKs.

Creating a distress number

Specific numbers may be designated as distress numbers using configuration files or by adding the distress trait to a contact directory entry that matches a configured emergency number.

Distress numbers added using the configuration file will always be sent as a distress call regardless of how the call is created: dialed from the dial pad, triggered by a speed dial, from a call history, from the contact directory, or from a customized hard or softkey.

Emergency contact directory entries that are marked as distress calls will only trigger the distress call behaviours when that contact is used as a speed dial or dialed while viewing the contact card.

Furthermore, starting the call while viewing the contact card will not apply any optional accidental dial protection delays.

IMPORTANT: It is not recommended to set 911, 999, or other regional emergency numbers as distress numbers using the configuration file method.

Create a distress number contact entry

A directory contact used for distress calls must match a number pre-defined as an emergency number in configuration.

Only a pre-existing directory contact can be designated as a distress number by opening the contact editor and scrolling to the bottom to set the Distress setting to enabled. Since a contact cannot be designated as a distress number at the time it is first created, you may need to first add the desired contact entry, save it, and then reopen for additional editing.

If an emergency number is also designated as a distress numbers in a configuration file, then creating a contact directory entry with the same phone number will show the distress field as enabled when viewing that contact, however, the distress field will not be available for modification.

Configure a number as an emergency number

Configure the emergency number and contact details.

1. Open the configuration file.
2. Configure a number as an emergency number.

```
dialplan.routing.emergency.x.value="<contact number>"
```

3. Set the label or description for the emergency contact number.

```
dialplan.routing.emergency.x.description="<emergency_contact>"
```

4. Save the configuration file.

Populate a directory file with contact information

Create the contact entries for the directory files loaded onto your phones.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the `000000000000-directory~.xml` directory file.

   The directory file includes three sample contacts that can serve as templates for new contact entries.

2. Add contact information inside the `<item>` tag.

```
<item>
                <fn>First Name</fn>
                <ln>Last Name</ln>
                <ct>Numeric Contact ID</ct>
```

```
                <sd>Speed Dial Entry</sd>
                <rt>Ringtone</rt>
</item>
```

The following table lists the elements to use when configuring a contact directory file.

Table 12-1 Contact Directory XML Elements

Element	Description	Permitted Values
fn	First name	UTF-8 encoded string up to 40 bytes.
ln	Last name	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL.
ct	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.	20 **NOTE:** You can't duplicate this field or leave it `Null`.
di	Contact directory XML files can designate an entry as a distress number using the <di> element. Set to 1 to enable distress call behavior when this contact is used.	0, 1
sd	Speed dial index Associates a particular entry with a speed dial key.	20
lb	Label for the contact The label of a contact directory item is by default the label attribute of the item. If the label attribute doesn't exist or is `Null`, then the first and last names form the label with a space between first and last names.	UTF-8 encoded string up to 40 bytes.
pt	Protocol The protocol to use when placing a call to the contact.	SIP, H323, or Unspecified
rt	Ringtone When incoming calls match a directory entry, this field specifies the ringtone to use.	Null, 1 to 21
ad	Auto divert Set to `1` to divert callers that match the directory entry to the address specified for the divert contact element.	0, 1 **NOTE:** If you enable auto-divert, it has precedence over auto-reject.

Table 12-1 Contact Directory XML Elements (continued)

Element	Description	Permitted Values
ar	Auto reject Set to `1` to reject callers that match the directory entry specified for the auto reject element.	0, 1 NOTE: If you enable auto-divert, it has precedence over auto-reject.
bw	Buddy watching Set to `1` to add this contact to the list of watched phones.	0, 1
bb	Buddy block Set to `1` to block this contact from watching this phone.	0, 1
up	User photo The contact's photo icon set by the `icons.x` parameter.	1 to 24

3. Optional: Add the distress call trait to contact information inside a contact's <item> tag. For example:

```
<item>
                <fn>Silent Alarm</fn>
                <ln></ln>
                <ct>911</ct>
                <sd>1</sd>
                <di>1</di>
</item>
```

4. Save the configuration file.

Configure distress numbers

Specific numbers may be designated as distress numbers

Configure a number as an emergency number and designate it as a distress call before completing this task.

1. Open the configuration file.
2. Designate a configured emergency number as a distress number.

```
dialplan.routing.emergency.x.value="<emergency number>"
dialplan.routing.emergency.x.distress.value ="1"
```

3. Save the configuration file.

Configure a text to speech distress message

Create a text to speech message that plays once the distress call connects.

You must have designated an emergency number before you configure the text to speech message.

1. Open the configuration file.

2. Configure the text to speech message. For example:

```
dialplan.routing.emergency.x.distress.ttsMessage="Distress...
Distress... Distress... Room 812... Building 2... 555 White Street"
```

   Use a comma to pause between words.

3. Configure the number of times the message repeats.

```
dialplan.routing.emergency.x.distress.ttsRepeatCount="3"
```

4. Configure the delay time between repeats.

```
dialplan.routing.emergency.x.distress.ttsRepeatDelay="3"
```

5. Save the configuration file.

Configure a distress number softkey

Create a custom softkey to dial a distress number.

You have to configuring the target number as an emergency number before creating the softkey.

1. Open the configuration file.
2. Select the distress call number.
3. Label the softkey. For example:

```
dialplan.routing.emergency.2.value="123456"
dialplan.routing.emergency.2.distress.value="1"
softkey.1.enable="1"
softkey.1.action="123456"
softkey.1.use.idle="1"
softkey.1.use.active="0"
softkey.1.label="HELP"
```

4. Save the configuration file.

13 Configuring Phone Settings

You can customize your phone using various applications and keysets.

User profiles

Users can access their personal phone settings from any phone on the network with user profiles.

Remote and mobile workers who don't have a dedicated work space can benefit from this feature. Offices with a common conference phone where multiple users need to access their personal settings can also use user profiles.

NOTE: You can configure all company phones so that anyone can call authorized and emergency numbers when not logged in to a phone. For more information, see `dialplan.routing.emergency.outboundIdentity`.

Users can change their own password on any phone on the network. If a user changes any settings while logged into a phone, the settings save and display the next time that user logs in to another phone. When the user logs out, the corresponding user options clear from the device until someone enables the user profile-related configuration on the phone again.

Enable multiple user profiles on the phone

Configure the phone so that it can accept multiple user profiles.

1. Open the configuration file.
2. Enable the phone to accept multiple users other than the default user.

```
prov.login.defaultOnly="1"
```

3. Save the configuration file.

User profile authentication

Authenticate users with phone-based or server-based authentication methods.

Phone-based authentication authenticates credentials entered by the user against the credentials in the *<user>*`.cfg` file. Server-based authentication passes user credentials to the provisioning server for authentication.

User profile server authentication

Enable users to log in to any phone on the network with their user profile.

To enable server authentication, set up user accounts on the provisioning server so users can authenticate their phones by entering correct server credentials.

The phone downloads log files (`app.log` and `boot.log`) from the generic profile on the provisioning server regardless of user logins.

Enable the phone to use server authentication

Configure the phone to use its provisioning server for user authentication.

Enable the phone to use multiple user profiles.

1. Open the configuration file.

2. Enable server authentication.

```
prov.login.useProvAuth="1"
```

3. Save the configuration file.

Create a generic user profile for server authentication

Create a user profile to use with a provisioning server or locally on a shared phone.

If you enable server authentication of user profiles, the following parameters don't apply:

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

1. Open the configuration file.
2. On the server, create an account and directory for the generic profile.

   `Generic_Profile`
3. In the directory, create a configuration file for the generic profile the phone uses by default.

   `genericprofile.cfg`
4. Open the generic profile configuration file.
5. Include registration and server details, and set the following phone feature parameters:

```
prov.login.enabled="1"
prov.login.useProvAuth="1"
prov.login.persistent="1"
```



NOTE: If you enable `prov.login.enabled` and don't enable `prov.login.useProvAuth`, the phone authenticates users by matching with credentials you store in the *<user>*`.cfg` user configuration file.

6. Save the generic profile configuration file.
7. Create a primary configuration file `000000000000.cfg` for all the phones or a *<MACAddress>*`.cfg` for each phone, and add the generic profile configuration file to the **CONFIG_FILES** field.
8. Set the provisioning server address and provisioning server username and password credentials for the generic user account on the phone at **Settings** > **Advanced** > **Provisioning Server**.
9. Save the configuration file.

The following override files upload to the generic profile directory:

- Log files
- Local interface settings

- System web interface settings
- Call logs
- Contact directory file

Create user profiles for server authentication

Create user profiles in the **Home** directory of each user with a specific configuration file that you store on the provisioning server. User profiles have unique names as well as specific files such as settings, directory, and call lists.

When a user logs in with credentials, the phone downloads the user profile from the provisioning server. When the user logs out, the phone downloads the default user profile using the generic credentials.

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

- Log files
- System web interface settings

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

- Local interface settings
- Contact directory file

1. On the server, create an account and a directory for each user.

   `User1` and `User2`

2. In each user directory, create a configuration file for each user that contains the user's registration details and feature settings.

   `User1.cfg` and `User2.cfg`

3. Open the user profile configuration file.
4. Enable the user profile.

```
prov.login.enabled="1"
```

5. **Optional:** Set the user's default password. The default is `123` until the user changes it.

```
prov.login.localPassword="<string>"
```

6. Save the user profile configuration file.

User profile phone authentication

Enable multiple users to log in to one phone.

Users can provide their credentials on the phone without using a server. This is helpful for shared phones in common areas without a connection to a provisioning server.

Create a user configuration file

Create a configuration file for each user that you want to enable to log in to the phone.

Some things to note about user configuration files:

- If users update their password or other user-specific settings on the phone, the updates save to `<user>-phone.cfg`, not `<MACaddress>-phone.cfg`.
- If users update their contact directory while logged in to a phone, the updates save to `<user>-directory.xml`.
- Directory updates display each time users log in to a phone. For certain phones, the `<user>-calls.xml` contains an up-to-date call list history. This list updates each time users log in to their phone.

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

- `<user>-phone.cfg`
- Web system interface
- Configuration files listed in the primary configuration file (including `<user>.cfg`)
- Default values

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

   If the user's login ID is *user100*, name the user configuration file `user100.cfg`.
2. Open the user configuration file.
3. In each `<user>.cfg` file, you must add and set values for the user's login password.
4. **Optional:** Add and set values for any user-specific parameters you want to add:
   - Registration details, such as the number of lines the profile displays and line labels.
   - Feature settings, such as microbrowser settings.

⚠ **CAUTION:** If you add optional user-specific parameters to `<user>.cfg`, only add parameters that don't force the phone to restart or reboot to complete the update.

5. Save the user configuration file.

Convert a phone to user-based deployment

Configure a phone in a deployment that depends on user login instead of a traditional phone deployment.

1. Open the user configuration file.
2. Copy the `<MACaddress>-phone.cfg` file to `<user>-phone.cfg`.
3. Copy the `phoneConfig<MACaddress>.cfg` file to `<user>.cfg`.
4. Save the user configuration file.

Create default credentials and a profile for a phone

Create a default user profile for the phone to automatically log in to each time a user logs out or the phone restarts.

The default user profile is like any other user profile, except it's designated as the phone's own profile. When the phone logs in using the default login credentials, a default phone profile displays. Users retain the option to log in and view their personal settings.

IMPORTANT: Poly recommends that you create a single default user password for all default user profiles.

1. Open the configuration file.
2. Enter the default user login credentials.

```
prov.login.defaultUser="<Default User Profile Username>"
prov.login.defaultPassword="<Account User Profile Password>"
```

3. Save the configuration file.

Require a user login

Configure the phone to require a user to log in to the phone to use it.

1. Open the configuration file.
2. Require a user to log in to use the phone.

```
prov.login.required="1"
```

3. Save the configuration file.

Mask the user password entry

Use pound signs (#) to mask the user's password on the phone's screen as they enter it.

Password entries on the phone's screen to prevent prying eyes from seeing user's password. For example, `password` displays as `########`.

1. Open the configuration file.
2. Mask the user's password entry with pound signs.

```
prov.login.localPassword.hashed="1"
```

3. Save the configuration file.

Enable user login persistence

Enable the phone to maintain the last user logged in following a phone reboot.

1. Open the configuration file.
2. Enable the phone to retain the last user login when it reboots.

```
prov.login.persistent="1"
```

3. Save the configuration file.

Presence Status

Enable users to monitor the status of other remote users and phones. Poly phones support a maximum of 64 buddies.

By adding remote users to a buddy list, users can monitor changes in the status of remote users in real time or they can monitor remote users as speed-dial contacts. Users can also manually specify their status to override or mask automatic status updates to others and can receive notifications when the status of a remote line changes.

Enable Presence Status to Display on the Phone

Enable phone users to see the presence of other users.

1. Open the configuration file.
2. Enable presence status to display on the phone. The **MyStatus** and **Buddies** softkeys display on the phone.

```
feature.presence.enabled="1"
```

3. Set the line used for presence. Select lines 1 through 34. The phone's default line is line `1`.

```
pres.reg="<line number>"
```

4. Save the configuration file.

Disable Presence Softkeys

Remove the **MyStatus** and **Buddies** softkeys from the phone's local interface to prevent users from manually updating their presence.

1. Open the configuration file.
2. Remove the **MyStatus** and **Buddies** softkeys.

```
pres.idleSoftkeys="0"
```

3. Save the configuration file.

Microphone mute

Microphone mute is an embedded feature on your phone, and you can't configure or disable it. However, you can configure supporting features related to muting the microphone.

Enable microphone mute/unmute alert

Configure the phone to play a tone when a user mutes or unmutes the microphone.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the microphone mute alert.

```
se.touchFeedback.enabled="1"
```

3. Save the configuration file.

Configure mute reminder alert interval

Set the microphone mute reminder alert interval to play tones at a specified amount of time to remind users that their microphone is muted.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Configure the interval, in seconds, to play a tone while the phone is muted. The value range is 5 to 3600.

```
call.mute.reminder.period="<interval period in seconds>"
```

3. Save the configuration file.

Enable microphone mute persistence

With microphone mute enabled, the microphones remain muted for subsequent calls until a user manually unmutes them.

1. Open the configuration file.
2. Disable microphone mute persistence.

```
feature.persistentMute.enabled="1"
```

3. Save the configuration file.

Enable Persistent Call Volume

By default, the phone resets the call volume to the default level for each new call. Configure the phone to retain the call volume set during a call for subsequent calls.

In some countries, regulations state that a phone's receiver volume must reset to a nominal level for each new call. Make sure any changes you make here don't violate local laws or regulations.

Transmit levels are fixed according to the TIA/EIA-810-A standard.

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

Set any or all of these parameters for particular devices to enable the call volume to persist between calls.

1. Open the configuration file.
2. Configure the handset volume to persist between calls.

```
voice.volume.persist.handset="1"
```

3. Configure the speakerphone volume to persist between calls.

```
voice.volume.persist.handsfree="1"
```

4. Configure USB headset volume to persist between calls.

```
voice.volume.persist.usbHeadset="1"
```

5. Configure volume for a connected Bluetooth headset to persist between calls.

```
voice.volume.persist.bluetooth.headset="1"
```

6. Save the configuration file.

Disable DTMF tones

Prevent the phone from playing DTMF tones through the speakerphone.

The phone can encode DTMF tones using the active voice codec or using RFC 2833 compatible encoding. The remote endpoints capabilities determine the coding format decision. The phone generates RFC 2833 tones but doesn't regenerate or use DTMF tones received from the remote end of the call.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

DTMF tones are encoded in the Real-time Transport Protocol (RTP) stream by default. When you disable `tone.dtmf.viaRtp`, DTMF isn't encoded in the RTP stream.

1. Open the configuration file.

2. Disable DTMF tones from playing through the speakerphone.

```
tone.dtmf.chassis.masking="1"tone.dtmf.viaRtp="0"
```

3. Save the configuration file.

Audible notifications and sounds

Configure how audible notifications and sounds play on your phone. Audible notifications and sounds play through the speakerphone by default.

Audible notifications include call progress tones and ringtones, as well as the sound effect patterns or files they play.

Set the audible notification and sound output

Determine where the audible notifications and sounds play during a call.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the output location for audible notifications and sounds.

   The following values apply:

   - `chassis` (Default) - All notifications and sounds play through the speakerphone, regardless of the active location.
   - `handset` - All notifications and sounds play through the handset when it's in use. If it's not in use, notifications and sounds play through the speakerphone.
   - `headset` - All notifications and sounds play through an active headset. If the headset is not active, no notifications or sounds play.
   - `active` - All notifications and sounds play through the handset or headset if they are in use. Otherwise, notifications and sounds play through the speakerphone.

   ```
   se.destination="<value>"
   ```

3. Save the configuration file.

Disable the phone's welcome sound

Disable the welcome sound on your phone.

1. Open the configuration file.
2. Disable the welcome sound.

   ```
   up.welcomeSoundEnabled="0"
   ```

3. Save the configuration file.

Disable audible notifications and sounds

Disable audible notifications and sounds so they don't play on your phones.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Disable audible notifications and sounds.

   NOTE: Disabling this parameter doesn't affect the voicemail stutter dial tone configured in `se.stutterOnVoiceMail`.

   ```
   se.appLocalEnabled="0"
   ```

3. Save the configuration file.

Disable the voicemail stutter dial tone

By default, phones use a stuttered dial tone to indicate a user has voicemail messages. Configure the phone to use a normal dial tone instead.

1. Open the configuration file.
2. Disable the voicemail stutter dial tone.

   ```
   se.stutterOnVoiceMail="0"
   ```

3. Save the configuration file.

Ringtones and visual incoming call indicators

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

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

- `Ring`: Plays an audible ring pattern or call waiting indication.
- `Visual`: Provides a visual-only indication of an incoming call.
- `Answer`: Auto-answers incoming calls when no incoming calls are in progress. Auto-answer continues to work during outgoing calls.
- `Ring-answer`: Provides auto-answer on an incoming call after a certain number or rings.

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

Supported ring classes

The following table provides the available ring classes to create or assign ringtones.

Table 13-1 Ring Classes

Ring Class	Definition
Default	The phone rings for all call types.
Visual	The phone's LED flashes to indicate an incoming call.
AnswerMute	The phone mutes the microphone when you answer a call.
AnswerAuto	The phone auto answers incoming calls.
RingAnswerMute	The phone rings audibly and answers with mute active.
RingAnswerAuto	The phone rings audibly and auto-answers the call.
Internal	The phone rings for internal calls.
External	The phone rings for external calls.
Emergency	The phone rings for emergency calls.
Precedence	
Splash	
Custom*y*	Link to a custom ringtone uploaded to the phone. *y* can be any value from 1 to 17.

Disable distinctive ringtones signaled through Alert-Info

Disable your phones from playing distinctive ringtones that are signaled through the Alert-Info SIP header.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Disable distinctive ringtones that are signaled through the Alert-Info SIP header on your phones.

```
se.rt.enabled="0"
```

3. Save the configuration file.

Disable the ability to change the ringtone

Don't allow users to modify the predefined ringtone from the phone's local interface.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Disable the ability for users to modify the ringtone through the local interface.

```
se.rt.modification.enabled="0"
```

3. Save the configuration file.

Configure the call waiting tone

Configure the call waiting tone used for the specified ring class.

The call waiting pattern must match those defined in the call progress tone pattern list.

1. Open the configuration file.
2. Set the call waiting tone type. Replace *<ringClass>* with the desired ring class.

   The following values apply:

   - `callWaiting` (default)
   - `callWaitingLong`
   - `precedenceCallWaiting`

```
se.rt.<ringClass>.callWait="<tone pattern>"
```

3. Save the configuration file.

Distinctive ringtones

Apply a distinctive ringtone to a specific contact, type of call, or registered line, including internal or external calls.

You can set up distinctive ringing using more than one method. However, the phone uses the highest priority method based on the following:

- Assign ringtones to specific contacts in the contact directory. This option is the first and highest in priority.
-
- Use parameters to map calls to specific ringtones based on call server settings. This option requires server support and is second in priority.
- Users can select a ringtone for each registered line on the phone from the phone's local interface. This option has the lowest priority.

Assign a distinctive ringtone to a registered line

Assign a specific ringtone to a line to identify calls received from a specific line.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Assign a ringtone directly to a registered line. Replace *x* with the registered line number.

```
reg.x.ringType="<ringtone name>"
```

3. Save the configuration file.

Assign a distinctive ringtone based on Alert-Info headers

Use parameters to map calls to specific ringtones based on Alert-Into headers and call server settings. This option requires server support.

1. Open the configuration file.
2. Specify a ring class to apply when the phone matches the value signaled in the Alert-Info header from INVITE requests. Replace *x* with the registered line number.

```
voIpProt.SIP.alertInfo.x.class="<ring class>"
```

3. Specify the string to match in the Alert-Info header in the incoming INVITE request. Replace *x* with the list of Alert-Info strings and the mapped ring class. You can configure up to 22 lists.

   The string has a max length of 128 characters.

```
voIpProt.SIP.alertInfo.x.value="<Alert-Info header string>"
```

4. Save the configuration file.

Sound effects

Customize the audio sound effects that play for incoming calls and other alerts. Patterns, sequences of chord-sets, silence periods, and wave files define sound effects.

The phones use synthesized tones or sampled audio files with `.wav` files that you download from the provisioning server or internet. Phones support the following sampled audio `.wav` file formats:

- Mono 8 kHz G.711 u-Law - Supported on all phones
- Mono G.711 (13-bit dynamic range, 8-khz sample rate)
- G.711 A-Law - Supported on all phones
- Mono L16/8000 (16-bit dynamic range, 8-kHz sample rate) - Supported on all phones
- Mono 8 kHz A-law/mu-law - Supported on all phones
- L8/16000 (16-bit, 8 kHz sampling rate, mono) - Supported on all phones
- Mono L16/16000 (16-bit dynamic range, 16-kHz sample rate)
- L16/16000 (16-bit, 16 kHz sampling rate, mono - Supported on all phones

Phones store ringtone files in volatile memory that allows a maximum size of 600 KB (614,400 B) for all ringtones.

Add a sample audio file

Add a link to a sample audio file (SAF) to use as a ringtone.

NOTE: If you use TFTP, the URL must be in the following format: `tftp://<host>/<pathname> <filename>` . For example: `tftp://somehost.example.com/sounds/example.wav`.

1. Open the configuration file.

2. Enter the filename and file path or URL. Include the name of the file and the `.wav` extension in the path. Replace *x* with the custom audio file's filename.

   - The following values apply:
   - `Null` (Default) - The phone uses a built-in file.
   - `filepath` - Location in the provisioning server where the audio file is located. During startup, the phone attempts to download the file.
   - `URL` - Location of the audio file on the internet. During startup, the phone attempts to download the file. The URL must be compliant with RFC 1738 and go to an HTTP, FTP, or TFTP `.wav` file resource.

```
saf.x="<string>"
```

3. Save the configuration file.

Configure sound effect patterns

Specify the sound effects, patterns, and category that play for different phone functions.

Note the following when configuring these parameters:

- *x* is the pattern name.
- *y* is the instruction number.
- Both *x* and *y* must be sequential.
- *cat* is one of the following pattern categories:
  - `callProg` - Call progress tones
  - `ringer` - Ringtones
  - `misc` - Miscellaneous tones

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Set the sound effect name. Replace *cat* with the pattern category name. Replace *x* with the pattern name. Replace *y* with the instruction number.

   - `sample`
   - `chord`
   - `silence`
   - `branch`

   The default is `Null`. The maximum string length is 255 characters.

```
se.pat.cat.x.inst.y.type="<string>"
```

3. Set the sound effect instruction. Replace *cat* with the pattern category name. Replace *x* with the pattern name. Replace *y* with the instruction number.

   - `sampled` - Sampled audio file number
   - `chord` - Type of sound effect
   - `silence` - Silence duration in ms
   - `branch` - Number of instructions to advance

   The default is `Null`. The maximum string length is 50 characters.

   ```
   se.pat.cat.x.inst.y.value="<string>"
   ```

4. Save the configuration file.

Sound effect pattern examples

Specify the sound effects, patterns, and category that play for different phone functions.

Patterns use a simple script language that enables you to string different chord sets or `.wav` files together with periods of silence. The script language uses the instructions shown in the following table.

Table 13-2 Sound Effect Pattern Instruction Types

Instruction	Definition	Example
sampled (*n*)	Play sampled audio file *n*	`se.pat.misc.custom1.inst.1.type="sampled"` - Sampled audio file instruction type `se.pat.misc.custom1.inst.1.value="2"` - Specifies sampled audio file 2
chord (*n*)	Play chord set *n*	`se.pat.callProg.busyTone.inst.2.type="chord"` - Chord set instruction type `se.pat.callProg.busyTone.inst.2.value="busyTone"` - Specifies sampled audio file `busyTone`
silence (*d*)	Play silence for *d* milliseconds This option doesn't mute Rx audio.	`se.pat.callProg.bargeIn.inst.3.type="silence"` - Silence instruction type `se.pat.callProg.bargeIn.inst.3.value="300"` - Specifies silence lasts 300 milliseconds
branch (*n*)	Advance *n* instructions and execute that instruction *n* must be negative and must not branch beyond the first instruction.	`se.pat.callProg.alerting.inst.4.type="branch"` - Branch instruction type `se.pat.callProg.alerting.inst.4.value="-2"` - Step back 2 instructions and execute that instruction

Call progress tone patterns

Poly phones play call progress tones including busy signals, ringback sounds, and call waiting tones.

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

The following table lists the call progress patterns and their descriptions.

Table 13-3 Call Progress Tones

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

Ringtone patterns

The following table lists the ring pattern names and their default descriptions.

Sampled audio files 1 to 10 all use the same built-in file unless you replace that file with a downloaded file.

Table 13-4 Ringtone Pattern Names

Parameter Name	Ringtone Name	Description
ringer1	Silent Ring	Silent ring NOTE: Silent ring provides a visual indication of an incoming call, but no audio indication. When a phone line is using the silent ring, lifting the handset will not answer incoming calls. To answer the call, use the Answer softkey or touch the line key that is associated with the ringing call.
ringer2	Low Trill	Long single A3 Db3 major warble
ringer3	Low Double Trill	Short double A3 Db3 major warble
ringer4	Medium Trill	Long single C3 E3 major warble

Table 13-4 Ringtone Pattern Names (continued)

Parameter Name	Ringtone Name	Description
ringer5	Medium Double Trill	Short double C3 E3 major warble
ringer6	High Trill	Long single warble 1
ringer7	High Double Trill	Short double warble 1
ringer8	Highest Trill	Long single Gb3 A4 major warble
ringer9	Highest Double Trill	Short double Gb3 A4 major warble
ringer10	Beeble	Short double E3 major
ringer11	Triplet	Short triple C3 E3 G3 major ramp
ringer12	Ringback-style	Short double ringback
ringer13	Low Trill Precedence	Long single A3 Db3 major warble Precedence
ringer14	Ring Splash	Splash
ringer15	N/A	Sampled audio file 1
ringer16	N/A	Sampled audio file 2
ringer17	N/A	Sampled audio file 3
ringer18	N/A	Sampled audio file 4
ringer19	N/A	Sampled audio file 5
ringer20	N/A	Sampled audio file 6
ringer21	N/A	Sampled audio file 7
ringer22	N/A	Sampled audio file 8
ringer23	N/A	Sampled audio file 9
ringer24	N/A	Sampled audio file 10

Miscellaneous sound effect patterns

The following table lists the miscellaneous sound effect patterns and their descriptions.

Table 13-5 Miscellaneous Sound Effect Pattern Parameters

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

Table 13-5 Miscellaneous Sound Effect Pattern Parameters (continued)

Parameter Name	Pattern Name	Description
callParkBLFAudioNotification	call Park BLF Audio Notification	Cadence of parked call audio notification

14 Directories and Contacts

Configure phones with a local contact directory and also link contacts to speed dial buttons

Call logs stored in the **Missed Calls**, **Received Calls**, and **Placed Calls** call lists enable users to view phone events. Events include remote party identification, time and date of call, and call duration.

Local contact directory

Configure phones with a local contact directory and link contacts to speed dial buttons.

Set the maximum number of contacts in the local directory

Configure the maximum number of contacts the phones store.

Phones can store a maximum of 500 contact entries in a contact directory file 4 MB or smaller.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enter the maximum number of contacts allowed in the local directory. The default value is 500 contacts.
3. Save the configuration file.

Creating directory files

Configure a contact directory file that Poly phones use to store frequently used contacts.

The PVOS package includes a contact directory template named `000000000000-directory~.xml`. The contact directory file loads to the provisioning server the first time that you boot up a phone or after a factory reset.

The phone looks for contact directories in the following order:

- An internally stored local directory
- A personal `<MACaddress>-directory.xml` file
- A global `000000000000-directory.xml` file when the phone substitutes `<000000000000>` for its own MAC address

Create a Per-Phone Personal Directory File

Create a personal directory file to load onto a single phone in an update file.

Any changes users make to the contact directory on the phone store on the phone. Upload the information to the provisioning server in the personal directory (*<MACaddress>*`-directory.xml`) file.

1. Locate the XML directory file in the phone's software update folder.

   The default file name is `000000000000-directory~.xml`.
2. Open the directory file.
3. Modify the `directory.xml` file to include the XML for each contact.
4. Remove the tilde (~) from the end of the file name and replace the `000000000000` in the directory file name with the phone's MAC address.

   <MACaddress>`-directory.xml`
5. Save the directory file.

Create a Global Directory File

Create a global directory file to provision to multiple phones.

When you update the global directory file on the provisioning server, the updates download to all phones. The downloaded directory file combines with the local directory on the phone.

1. Locate the XML directory file in the phone's software update folder.

   The default file name is `000000000000-directory~.xml`.

2. Open the directory file.
3. Modify the `directory.xml` file to include the XML for each contact.
4. Remove the tilde (~) at the end of the file name.

   `000000000000-directory.xml`

5. Save the directory file.

Populate a Directory File with Contact Information

Create the contact entries for the directory files loaded onto your phones.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the `000000000000-directory~.xml` directory file.

   The directory file includes three sample contacts that can serve as templates for new contact entries.

2. Add contact information inside the `<item>` tag.

```
<item>
                <fn>First Name</fn>
                <ln>Last Name</ln>
                <ct>Numeric Contact ID</ct>
                <sd>Speed Dial Entry</sd>
                <rt>Ringtone</rt>
</item>
```

The following table lists the elements to use when configuring a contact directory file.

Table 14-1 Contact Directory XML Elements

Element	Description	Permitted Values
fn	First name	UTF-8 encoded string up to 40 bytes.
ln	Family name	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that makes up a valid SIP URL.

Table 14-1 Contact Directory XML Elements (continued)

Element	Description	Permitted Values
ct	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.	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL. NOTE: You can't duplicate this field or leave it `Null`.
sd	Speed dial index Associates a particular entry with a speed dial key.	null (blank) or 1-9999
lb	Label for the contact The label of a contact directory item is by default the label attribute of the item. If the label attribute doesn't exist or is `Null`, then the first and family names form the label with a space between first and family names.	UTF-8 encoded string up to 40 bytes.
pt	Protocol The protocol to use when calling to the contact.	SIP, H323, or Unspecified
rt	Ringtone When incoming calls match a directory entry, this field specifies the ringtone to use.	Null, 1 to 22 default ringer*x* (where *x* 1 to 24)
ad	Auto divert Set to `1` to divert callers that match the directory entry to the address specified for the divert contact element.	0, 1 NOTE: If you enable auto-divert, it has precedence over auto-reject.
ar	Auto reject Set to `1` to reject callers that match the directory entry specified for the auto reject element.	0, 1 NOTE: If you enable auto-divert, it has precedence over auto-reject.
bw	Buddy watching Set to `1` to add this contact to the list of watched phones.	0, 1
bb	Buddy block Set to `1` to block this contact from watching this phone.	0, 1
loc	Location of the speed dial	0 (primary), 1 (secondary)
tl	Title of the contact	64 characters
em	Email address of the contact	120 characters

Table 14-1 Contact Directory XML Elements (continued)

Element	Description	Permitted Values
ol	Outgoing line to use to call to the contact	0 to 33 0 = line registration 1 33 = line registration 34

Configure When Directory Files Update

Enable the phone to download the global directory file more frequently.

By default, a phone that uses a global directory file updates only after it receives a checksync NOTIFY message from the server. When you enable this parameter, the phone also downloads the global directory file following a reboot, configuration change, or software update.

When the phone updates, the following events happen:

- The phone downloads the global directory (`000000000000-directory.xml`) and per-phone (*<MACaddress>*`-directory.xml`) directory files.
- The directory files merge with the phone's directory.
- The phone ignores changes to the global directory that conflict with the phone's personal directory.

NOTE: Setting the `hotelingMode.type` parameter to `2` or `3` overrides this parameter.

1. Open the configuration file.
2. Enable the phone to download the global directory file following a reboot, configuration change, or software update.

```
voIpProt.SIP.specialEvent.checkSync.downloadDirectory="1"
```

3. Save the configuration file.

Disable the local contact directory

If you don't want phone users to store contacts on a phone, disable the local contact directory.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Disable the local contact directory.

```
feature.directory.enabled="0"
```

3. Save the configuration file.

Create a speed dial entry in the directory file

Poly phones support speed dial entriesaccessible from the phone interface.

This example shows adding a speed dial to the main directory file `000000000000-directory.xml` used by all phones.

1. Open the configuration file.
2. In the directory file, locate the contact entry.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<directory>
        <item_list>
                <item>
                        <ln>last name</ln>
                        <fn>first name</fn>
                        <ct>contact entry #</ct>
                        <rt>ringtone</rt>
                </item>
        </item_list>
</directory>
```

3. To assign a speed dial value, add the `<sd>` element with the assigned speed dial number.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<directory>
        <item_list>
                <item>
                         <ln>last name</ln>
                         <fn>first name</fn>
                         <ct>contact entry #</ct>
                         <rt>ringtone</rt>
                         <sd>speed dial #</sd>
                </item>
        </item_list>
</directory>
```

4. Save the configuration file.

When the phone polls the provisioning server, the new entry shows up on all phones.

Disable local speed dial edits

Prevent users from editing the speed dial entries on their phones.

1. Open the configuration file.
2. Disable local edits to speed dial entries.

```
dir.local.readonly="1"
```

3. Save the configuration file.

Prioritize Local Directory Changes

Configure the phone to prioritize local end-user changes rather than allow the server-side MAC-directory file to override local edits.

NOTE: When `dir.local.mode="devicePrioritized"`, changing the value of `dir.local.devicePrioritized.deleteDirectory` may delete the contents of the phone's local directory.

1. Open the configuration file.
2. Enter the value `devicePrioritized`.

   The default is `serverPrioritized`, which allows the server-side MAC-directory file to override local edits.

```
dir.local.mode="devicePrioritized"
```

3. Save the configuration file.

Remotely Delete Device Directory Contacts

You can remotely delete all of the contacts from a phone's device directory without performing a full factory reset.

1. Open the configuration file.
2. To remotely delete the contacts in a phone's device directory, enter any string value. It is recommended to use a timestamp (DD-MM-YYYY-HH:MM:SS).

   NOTE: The default value is Null. Replacing Null with any value triggers the delete action.

```
dir.local.devicePrioritized.deleteDirectory="01-01-2023-01:01:01"
```

3. Save the configuration file.

Corporate directory

Connect your phones to a corporate directory server that supports LDAP version 3. Setting up the corporate directory on the phone enables users to search for and place calls to these directory contacts.

Poly phones support corporate directories with server-side sorting. If the directory doesn't support server-side sorting, the phone performs sorting locally.

NOTE: Use corporate directories that have server-side sorting for better performance. Consult your LDAP administrator when making any configuration changes for the corporate directory. For more information on LDAP attributes, see RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map .

Connecting to a Corporate Directory Using LDAP

Use LDAP to connect to and download contacts from a corporate directory.

Connect to a corporate directory using LDAP

Connect to and download corporate directory contacts to your phones.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

Access to a corporate directory on the phone is read only. Phone users can't add or remove contacts to the corporate directory.

1. Open the configuration file.
2. Enter the IP address or host name of the LDAP server.

```
dir.corp.address="<LDAP IP address or host name>"
```

3. **Optional:** By default, the phone uses the TCP transport protocol to transfer the LDAP file from the server. If your network requires it, change the transport protocol to TLS.

```
dir.corp.transport="TLS"
```

4. Optional: Enable the login prompt if the phone doesn't log in to the LDAP server as part of the phone's configuration.

```
dir.corp.allowCredentialsFromUI.enabled="1"
```

5. Save the configuration file.

Configure the LDAP Server Base Domain

Configure the base domain to use for the LDAP server.

1. Open the configuration file.

2. Configure the base domain. The maximum string length is 255 characters.

```
dir.corp.baseDN="<Base Domain>"
```

3. Save the configuration file.

Configure the LDAP Server Connection Port

Configure the port to connect to the LDAP server.

Set this parameter if the LDAP server is not using the standard ports (389 for TCP transport and 636 for TLS transport.

1. Open the configuration file.
2. Configure the server connection port. The default is 0. Permitted values are 0 to 65535.

```
dir.corp.port="<Server Connection Port">
```

3. Save the configuration file.

Configure the LDAP Search Query Filter Prefix String

Configure the predefined filter prefix string to use for all LDAP search queries.

1. Open the configuration file.
2. Configure the predefined search query filter prefix string. The default is (objectclass=person). The maximum string length is 255 characters.

```
dir.corp.filterPrefix="<search_query_prefix>"
```

3. Save the configuration file.

Configure LDAP Server Credentials

Configure the username and password to use to authenticate the LDAP server.

1. Open the configuration file.
2. Configure the LDAP server username. The maximum string length is 255 characters.

```
dir.corp.user="<user name>"
```

3. Configure the LDAP server password. The maximum string length is 255 characters.

```
dir.corp.password="<password>"
```

4. Save the configuration file.

Configure LDAP Search Attributes

Configure search attributes for LDAP.

For each parameter, *x* is a list of defined attributes to use for searching. You can define up to 8.

1. Open the configuration file.

2. Configure a search attribute name to match an attribute in the directory entries on the LDAP server. The maximum string length is 255 characters.

   Consult the LDAP server for supported attribute names.

```
dir.corp.attribute.x.name="<Attribute Name>"
```

3. Configure the label for the search attribute. The maximum string length is 255 characters.

```
dir.corp.attribute.x.label="<Attribute Label>"
```

4. Configure the attribute type that the phone uses to interpret the returned search results.

   Possible values:

   - first_name
   - last_name (default)
   - phone_number
   - SIP_address
   - H323_address
   - URL
   - other

```
dir.corp.attribute.x.type="<Attribute Type>"
```

5. Configure the filter string for the attribute. The maximum string length is 255 characters.

```
dir.corp.attribute.x.filter="<Filter String>"
```

6. Determine if the filter string criteria is reset or retained after a reboot. The default is 0 (reset after a reboot). To retain filter string criteria after a reboot, set the value to 1.

```
dir.corp.attribute.x.sticky="<0 or 1>"
```

7. Determine if the LDAP search query includes the attribute. The default is 0 (not searchable). To make the attribute searchable, set the value to 1.

```
dir.corp.attribute.x.searchable="<0 or 1>"
```

8. Determine if the wildcard character is appended to the LDAP search query for the attribute. The default is 1 (append wildcard character). To disable appending a wildcard character, set the value to 0.

```
dir.corp.attribute.x.addstar="<0 or 1>"
```

9. Save the configuration file.

Securely store LDAP credentials

Enable multiple users to enter their LDAP user credentials directly in the phone to access the corporate (LDAP) directory and store those credentials on the phone.

Any LDAP credentials that users enter on the phone are encrypted and stored only on the phone. The credentials also persist after the phone restarts or reboots.

1. Open the configuration file.
2. Enable the phone to securely store and encrypt LDAP directory user credentials.

```
dir.corp.persistentCredentials="1"
```

3. Enable the login prompt if the phone doesn't log in to the LDAP server as part of the phone's configuration.

```
dir.corp.allowCredentialsFromUI.enabled="1"
```

4. Save the configuration file.

Call lists

The phone records and maintains user phone events in call lists. Call lists contain call information such as remote party identification, time, and date.

The provisioning server stores the list as an XML file named `<MACaddress>-calls.xml`. If you want to route the call list to another server, use the `CALL_LISTS_DIRECTORY` field in the primary configuration file. All call lists are enabled by default.

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

- Missed calls
- Received calls
- Placed calls

Disable the missed call list

Remove the missed call list on the *Home* screen and dialpad.

The missed call list lists all the incoming calls that the user doesn't answer.

1. Open the configuration file.
2. Disable the missed call list.

```
feature.callListMissed.enabled="0"
```

3. Save the configuration file.

Disable the placed call list

Remove the placed call list on the *Home* screen and dialpad.

The placed call list displays all outgoing calls users make from the phone.

1. Open the configuration file.
2. Disable the placed call list.

```
feature.callListPlaced.enabled="0"
```

3. Save the configuration file.

Disable the received call list

Remove the received call list on the *Home* screen and dialpad.

The received call list displays all incoming calls the user answers.

1. Open the configuration file.
2. Disable the received call list.

```
feature.callListReceived.enabled="0"
```

3. Save the configuration file.

Disable all call lists

Remove the missed call list, placed call list, and received call list from the *Home* screen and dialpad.

Setting this parameter overrides the `feature.callListMissed.enabled`, `feature.callListPlaced.enabled`, and `feature.callListReceived.enabled` parameters.

1. Open the configuration file.
2. Disable all call lists.

```
feature.callList.enabled="0"
```

3. Save the configuration file.

Disable consultation call logging

Prevent the phone from logging consultation calls in call lists.

1. Open the configuration file.
2. Disable consultation call logging so the phone doesn't log them in call lists.

```
callLists.logConsultationCalls="0"
```

3. Save the configuration file.

List consecutive calls individually

By default, the phone call lists collapse consecutive calls to or from the same party into one call entry. Configure the phone to list each call instance individually.

1. Open the configuration file.
2. Configure the phone to list each consecutive call instance individually.

```
callLists.collapseDuplicates="0"
```

3. Save the configuration file.

Enable Exchange call log synchronization

Configure an OpenSIP phone to synchronize the current user's Exchange call logs with the server and display the call history of missed, outgoing, and received calls.

Make sure you set `feature.exchangeCalendar.enabled="1"`.

1. Open the configuration file.
2. Enable the phone to synchronize Exchange call log information, which lists missed, outgoing, and received calls from Exchange contacts.

```
feature.exchangeCallLog.enabled="1"
```

3. Save the configuration file.

15 Configuring the Local Interface

Configure the phone display with various features, functions, and customization options.

Localizing the user interface

Poly phones support multiple languages and keyboard layouts.

Edit phone languages

Edit the language files included with the PVOS package to customize the localized user interface.

Before editing, familiarize yourself with the guidelines on basic and extended character support.

Poly phones support the following languages:

- Arabic
- Simplified Chinese
- Traditional Chinese
- Czech, Czech Republic
- Danish
- Dutch
- English
- French
- German
- Hungarian, Hungary
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Brazilian Portuguese
- Romanian, Romania
- Russian
- Slovenian
- International Spanish
- Swedish

NOTE: The updater is only available in English.

1. Go to the localization folder in your PVOS package.
2. Open the language file in a Unicode-compatible XML editor.

3. Edit the dictionary as desired.

Change the Keyboard Layout

Enable users to choose a keyboard layout based on languages other than the system language.

The phone uses the default keyboard assigned to the language that you set the phone to. For example, setting the phone language to French tells the phone to use the AZERTY keyboard layout.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Press and hold the comma (,) key on the phone's keyboard for one second to access the **Input options** menu.
2. Select **Languages**.
3. Clear the **Use system language** check box.
4. Select one or more languages in the **Active input methods** list.
5. Select the back arrow.

   When enabling more than one language, a globe key displays next to the comma (,) key on the phone keyboard, which lets you change the active keyboard.
6. Do one of the following:
   - Select and hold the globe key for 1 second to view and choose from a list of enabled languages. The phone uses the default keyboard layout for the language that you choose.
   - Select the globe key to cycle through enabled languages. The space bar displays the current language and keyboard layout.

Enable Pinyin Text on the Phone

Pinyin is the phonetic system used to transcribe spoken Mandarin Chinese into Latin characters.

- Go to Nuance XT9 and download a license key to the phone.

Configure the phone's display name

Configure the phone's name that displays on connected devices.

The default system name displays as *<phone name> <model number>_xxxx* where *xxxx* are the last four digits of the phone's MAC address.

Configure the system name using any of the following parameters:

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

- Default system name

NOTE: This list displays the priority in which the system name is selected from highest priority to lowest priority.

If you set the system name using the `system.name` parameter, the value you set displays for the phone unless you configure a name to display for a specific feature. The system name you set using any of the following feature parameters takes precedence over the name set in `system.name`:

- AirPlay: `content.airplayServer.name`
- Bluetooth: `bluetooth.device.name`
- Wireless Display: `content.wirelessDisplay.name`

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Change the system name.

```
system.name="<system name - maximum 96 characters>"
```

3. **Optional:** Set a name specifically for Bluetooth devices. This setting overrides the setting in `system.name` when searching for the phone from Bluetooth devices.

```
bluetooth.device.name="<UTF-8 encoded string>"
```

4. Set the SIP URI registration/H.323 extension. Replace *x* with the desired line key value.

```
reg.x.address="<SIP URI / H.323 ID>"
```

5. Set the name used in SIP signaling, the H.323 alias, or both. This appears as the caller ID on outgoing calls. Replace *x* with the desired line key value.

```
reg.x.displayname="<UTF-8 encoded string>"
```

6. Set the text label that displays next to the line key for registration *x*. Replace *x* with the desired line key value.

```
reg.x.label="<UTF-8 encoded string>"
```

7. Save the configuration file.

Configuring labels

You can choose to display a phone number, an extension, or a custom label on the *Home* screen below the time and date.

Create a custom Home screen label

Use a configuration file to create and configure a custom message to display on the *Home* screen.

By default, all phones display their phone number in a label on the *Home* screen.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Change the label's type to a custom label and enter the custom message.

   The custom message can be up to 255 characters.

```
homeScreen.labelType="Custom"
homeScreen.customLabel="<Custom message>"
```

3. Save the configuration file.

Configure unique line labels for registration lines

Configure a unique label for a line key on a registered line.

Ensure you enable at least two line keys for a registered line before configuring this feature. If `reg.x.linekeys="1"`, this configuration has no effect.

You must configure multiple line keys for a registration to configure unique line labels. For example, you can set different names to display for the registration *4144* that display on four line keys.

If you configure the line to display on multiple line keys without a unique label assigned to each line, the phone labels the lines automatically in numeric order. For example, if you have four line keys for line *4144* labeled *Poly*, the line keys are labeled as *1_Poly*, *2_Poly*, *3_Poly*, and *4_Poly*. This also applies to lines without labels.

1. Open the configuration file.
2. Enable the phone to use unique labels for line keys for a registered line.

```
up.cfgUniqueLineLabel="1"
```

3. Configure a unique line label for a line key on a registered line. Replace *x* with the registration index number starting from 1. Replace *y* with the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys.

   The default is `Null`. The maximum string length is 255 characters.

```
reg.x.line.y.label="<string>"
```

4. Configure the alignment of the label.

   - `None` (Default)

- `Right`
- `Left`

By default the line label aligns right for alphanumeric strings and it aligns left for numeric strings.

```
up.cfgLabelElide="<value>"
```

5. Save the configuration file.

Time and date display

Configure how the phone displays the time and date or disable the time and date display entirely.

Set the time and date format to display differently when the phone is in certain modes. For example, the display format can change when the phone goes from idle mode to an active call.

The time and date display on phones in PSTN mode in the following conditions:

- An incoming call with a supported caller ID standard
- The phone is connected to Ethernet and you enable the date and time display

Poly recommends synchronizing your phone with an SNTP server to display the most accurate time.

Disable the time and date on the idle display

Prevent the time and date from displaying on the phone's screen when the phone is in idle mode.

1. Open the configuration file.
2. Disable the time and date on the idle display.

```
up.localClockEnabled="0"
```

3. Save the configuration file.

Configure Time and Date Display Settings

Configure how the time and date display on your phone's screen.

1. Open the configuration file.
2. Display time in a 24-hour clock format.

   If the phone language is set to English (Internal) (`lcl.ml.lang=""`), configure the following parameter to display the time in a 24-hour clock format. The default is to display the time in a 12-hour clock format.

   ```
   lcl.datetime.time.24HourClock="1"
   ```

   If the phone language is set to another language, configure the following parameter, where x is the language index. For American English (en-us) and Canadian English (en-ca), the default is 0. For all other languages, the default is 1.

   ```
   lcl.ml.lang.clock.x.24HourClock="1"
   ```

3. Display the time in a 12-hour clock format.

   If the phone language is set to English (Internal) (`lcl.ml.lang=""`), configure the following parameter.

   ```
   lcl.datetime.time.24HourClock="0"
   ```

   If the phone language is set to another language, configure the following parameter, where x is the language index.

```
lcl.ml.lang.clock.x.24HourClock="0"
```

4. Configure the date to appear above the time display. The default displays the time above the date.

   If the phone language is set to English (Internal) (`lcl.ml.lang=""`), configure the following parameter:

   ```
   lcl.datetime.date.dateTop="1"
   ```

   For all other languages, configure the following parameter:

   ```
   lcl.ml.lang.clock.x.dateTop="1"
   ```

5. Save the configuration file.

Change the Date Format

Configure how the date displays on the phone screen.

By default, phones display the day and date as "Thursday, 3 July" with a value of `D,dM`.

The phone uses the following parameters when the language is set to English (Internal):

- Regular format—`lcl.datetime.date.format`
- Long format—`lcl.datetime.date.longformat`

The phone uses the following parameters when the language is set to a different language. *X* is the language index:

- Regular format—`lcl.ml.lang.clock.x.format`
- Long format—`lcl.ml.lang.clock.x.longFormat`

1. Open the configuration file.
2. Configure how the day and date display on the phone with the appropriate value from the following date format table.

   If the language is set to English (Internal), use the following parameter:

   ```
   lcl.datetime.date.format="<date format string>"
   ```

   If the language is set to a different language, use the following parameter, where *x* is the language index:

   ```
   lcl.ml.lang.clock.x.format="<date format string>"
   ```

3. **Optional:** Change the day and month display the long format (Friday/November) instead of the default short format (Fri/Nov).

   If the language is set to English (Internal), use the following parameter:

   ```
   lcl.datetime.date.longFormat="1"
   ```

   If the language is set to a different language, use the following parameter, where *x* is the language index:

```
lcl.ml.lang.clock.x.longFormat="1"
```

NOTE: The following table shows values for Friday, August 20, 2019, as an example.

Table 15-1 Date Format Table

Regular Format	Long Format	Date Displayed on Phone
dM,D	0	20 Aug, Fri
dM,D	1	20 August, Friday
Md,D	0	Aug 20, Fri
Md,D	1	August 20, Friday
D,dM	0	Fri, 20 Aug
D,dM	1	Friday, August 20
DD/MM/YY	N/A	20/08/19
DD/MM/YYYY	N/A	20/08/2019
MM/DD/YY	N/A	08/20/19
MM/DD/YYYY	N/A	08/20/2019
YY/MM/DD	N/A	19/08/20
YYYY/MM/DD	N/A	2019/08/20

4. Save the configuration file.

Contact Support Menu

The **Contact Support** menu displays contact information, such as contact hours, phone numbers, and other support information.

Enable and Configure the Contact Support Menu

Enable the **Contact Support** menu to display contact information, such as contact hours, phone numbers, and other support information.

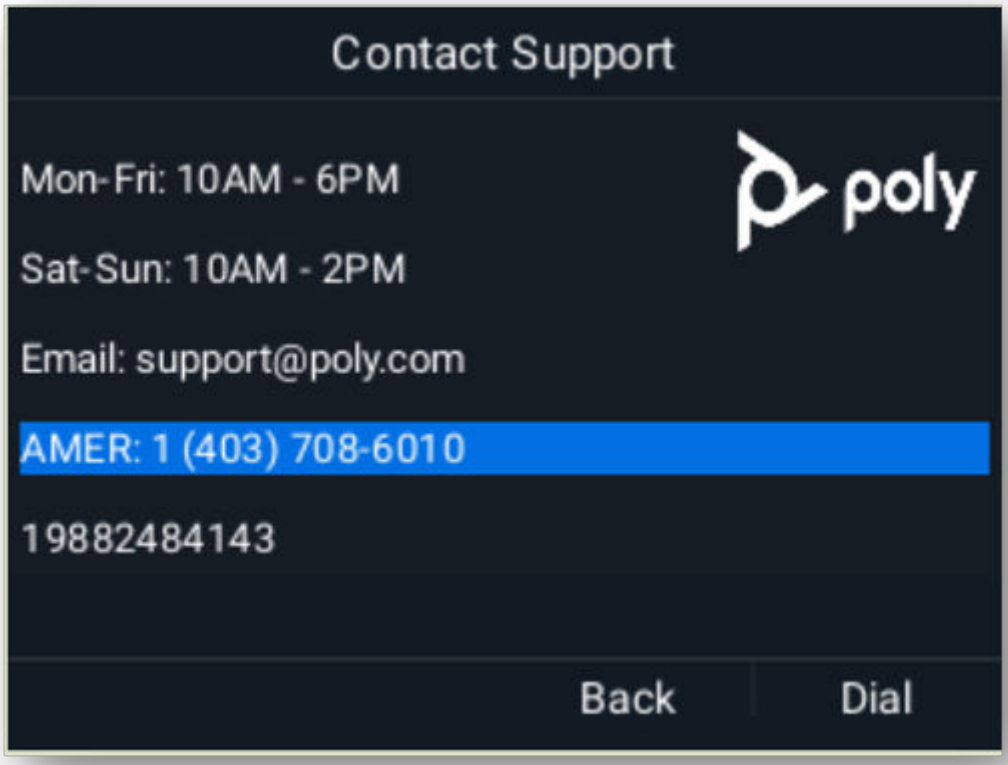
If you want to enable this feature, you must first add information such as contact support hours or phone numbers to display the **Contact Support** menu. See Add Help Desk Contact Information on page 201 and Add Help Desk Hours and Contact Information on page 202.

1. Open the configuration file.
2. Enable the *Contact Support* menu.

```
ui.menu.helpAndSupport.contact.enabled="1"
```

3. Save the configuration file.

Figure 15-1 Example Contact Support Menu



Add Help Desk Contact Information

Add up to three help desk contact numbers, email addresses, or URLs to the **Contact Support** menu.

1. Open the configuration file.
2. Add help desk information. Replace *x* with the desired line key value. The maximum length is 30 characters.

```
ui.menu.helpAndSupport.contact.numbers.x="<Support Information>"
```

NOTE: You can choose to add three phone numbers or two phone numbers and an email address or URL, for example.

3. Save the configuration file.

Add Help Desk Hours and Contact Information

Add help desk hours of operation and contact details to the **Contact Support** menu.

1. Open the configuration file.
2. Add help desk hours of operation and contact details. Replace *x* with the desired line key value. The maximum length is 30 characters.

```
ui.menu.helpAndSupport.contact.hours.x="<Hours of Operation>"
```

NOTE: You can choose to add three lines for hours of operation.

3. Save the configuration file.

Add a Customer Logo to the Contact Support Menu

Customize the **Contact Support** menu by adding a company logo to the page.

You can upload an image (182 x 78 pixels) in the following formats:

- .bmp
- .jpg
- .jpeg
- .jpe
- .jfif
- .png

1. Place the image file on the provisioning server.
2. Open the configuration file.
3. Add a customer logo to the **Contact Support** menu:

```
ui.menu.helpAndSupport.contact.customerLogo="<image filename>"
```

4. Save the configuration file.

Customize the QR Code

By default, the QR code links to overview and explainer videos about Poly Edge E Series phones, but you can customize it to link to other another resource.

1. Open the configuration file.
2. Customize the QR code.

```
ui.menu.helpAndSupport.contact.help.QrCode_URL="URL to help page"
ui.menu.helpAndSupport.contact.help.QrCode_Title="<QR Code Title>"
ui.menu.helpAndSupport.contact.help.QrCode_Description="<QR Code
Description>"
```

3. Save the configuration file.

Set Up a Custom Background

Replace the phone's default background image with a custom image or import multiple images that users can select from.

You can customize the background image for both the main display and, where applicable, the secondary display.

The custom background displays behind the time, date, and line and key labels on the *Home* screen. The phone looks for custom background images from a folder in your network.

Poly Edge E Series phones support the following formats for background images:

- .bmp
- .jpg
- .jpeg
- .jpe
- .jfif
- .png

Refer to the following table for the optimal image size supported for each phone model or series.

Table 15-2 Optimal Background Image Sizes for Edge E Series

Edge E Series	Optimal Background Image Size	Optimal Background Image Size for Secondary Screen
Edge E100	320×240 pixels	N/A
Edge E220	320×240 pixels	N/A
Edge E300 series	320×240 pixels	N/A
Edge E400 series	320×240 pixels	240×320
Edge E500 series	800×480 pixels	N/A

Table 15-2 Optimal Background Image Sizes for Edge E Series (continued)

Edge E Series	Optimal Background Image Size	Optimal Background Image Size for Secondary Screen
Edge E EM	480x854 pixels	N/A

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

For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

This task describes using the configuration file. To use the system web interface instead, go to **General Settings** > **Background**.

1. Open the configuration file.
2. Set the background images location on your network.

   NOTE: If the file is missing or unavailable, a default solid pattern displays.

   ```
   bg.color.bm.1.name="<custom background URL>"
   ```

3. Set the background image location for the EM.

   ```
   bg.color.bm.1.em.name="<custom background URL>"
   ```

4. Set the background image location for the secondary screen (Edge E 400 Series only):

   ```
   bg.color.bm.1.secondary.name="<custom background URL>"
   ```

5. Set the background selection to use the custom background.

   2 refers to custom background, 1 refers to the index of the background parameter file, `bg.color.bm.1.name`.

   ```
   bg.color.selection="2,1"
   ```

Add a Customer Logo to the Home Page

Customize the **Home** page by adding a company logo.

You can upload an image in the following formats:

- .bmp
- .jpg
- .jpeg
- .jpe
- .jfif

- .png

Table 15-3 **Recommended Logo Image Sizes**

Phone Model	Logo Size
Edge E100	60 x 26 pixels
Edge E220	60 x 26 pixels
Edge E300 Series	60 x 26 pixels
Edge E400 Series	60 x 26 pixels
Edge E500 Series	182 x 78 pixels

1. Open the configuration file.
2. Place the image file on the provisioning server.
3. Add a customer logo to the **Home** page:

```
bg.logo="<image filename>"
```

4. Save the configuration file.

Digital Picture Frame

Users can the digital picture frame feature to display a slide show on the phone's idle screen. You can map a different location for the photos, adjust the photo refresh duration, and disable the digital picture frame feature.

For images to display, users must save the images in `.jpg`, `.bmp`, or `.png` format in the root directory of the USB flash drive. The phone can display a maximum image size of 9999 × 9999 pixels and a maximum of 1000 images.

The maximum image size depends on the available memory in the phone.

Users can access the digital picture frame on the web using `PicFrame:// URL`.

Map Digital Picture Frame Location

Configure the digital picture frame feature to use images not stored on the USB flash drive's root directory.

By default, the phone looks for the photos in the USB flash drive's root directory.

1. Open the configuration file.
2. Enter the filepath for the images on the USB flash drive. For example, if you want users to save the images in the `/images/phone` folder on the USB flash drive, configure `images/phone`.

```
up.pictureFrame.folder="<image filepath>"
```

3. Save the configuration file.

Adjust the Digital Picture Frame Refresh Duration

Set how long, in seconds, the phone displays one image before moving to the next one. By default, the phone displays an image for 5 seconds.

1. Open the configuration file.
2. Change how long the phone displays one image before refreshing.

   You can set the duration of the picture frame refresh from 3 to 300 seconds, the default is 5 seconds.

```
up.pictureFrame.timePerImage="<duration>"
```

3. Save the configuration file.

Disable the Digital Picture Frame

Prevent users from displaying images stored on a USB flash drive while idle.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.

2. Disable the digital picture frame feature.

```
feature.pictureFrame.enabled="0"
```

3. Save the configuration file.

Support for REST APIs

Poly phones support REST APIs that enable you to execute certain functions and retrieve information.

The REST API feature is disabled by default. Use parameters to enable REST API on your phone. For more information on phone APIs, review REST API Reference Manual for UC Software.

REST API parameter

Use the following parameter to enable the REST API.

apps.restapi.enabled
0 (default) - Disabled
1 - Enabled

Enhanced Feature Keys

Enhanced feature keys (EFK) enables you to customize the functions of a phone's line, soft, and hard keys to assign frequently used functions to keys or to create menu shortcuts to frequently used phone settings.

Enhanced feature key functionality is implemented using star code sequences like *89 and SIP messaging. Star code sequences that define EFK functions are written as macros that you apply to line and soft keys. The EFK macro language was designed to follow current configuration file standards and to be extensible (see Macro Definitions).

When this feature is enabled, and the user presses Lines soft key, all the lines on the home screen will appear. You can press any line key to initiate the call to that number.

In addition, you can configure an EFK as a line key allowing the users to execute the macro action defined to that line key. When this feature is enabled, all the EFK macros that are configured using `efk.eklist` parameter and has `efk.efklist.x.status=1` will display as a line key. You can enable or disable this feature using configuration parameter or importing the configuration file using the Web Configuration Utility.

For example, configure the phone with the following configuration:

```
feature.enhancedFeatureKeys.enabled="1"

feature.EFKLineKey.enabled="1"

efk.efklist.1.mname="DND"

efk.efklist.1.status="1"

efk.efklist.1.action.string="$FDoNotDisturb$"
```

After you run and update configuration, the DND EFK will display as a line key. When you press the DND line key, Do Not Disturb functionality is executed.

In addition, you can use Flexible Line Keys feature for an EFK and assign to a line key that displays anywhere on the phone's screen. For more information, see Flexible Line Key Assignments.

Some Guidelines for Configuring Enhanced Feature Keys

Use the guidelines in this section to efficiently configure enhanced feature keys (EFKs).

Use the following guidelines to help you to configure enhanced feature keys (EFKs) efficiently:

- Activation of EFK functions requires valid macro construction.
- All failures are logged in the phone's app logs at level 4 (Minor Error).
- If two macros have the same name, the first one is used and the subsequent one is ignored.
- A sequence of characters prefixed with "!" are parsed as a macro name. The exception is the speed dial reference, which starts with "!" and contains digits only.
- A sequence of characters prefixed with "^" is the action string.
- "'!" and "^" macro prefixes cannot be mixed in the same macro line.

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

For more guidance on how to manage

Contact Directory Macros

Because line keys and their functions are linked to fields in the contact directory file, you need to match the contact field (ct) in the directory file to the macro name field (mname) in the configuration file that contains the EFK parameters.

When you enter macro names to the contact field (ct) in the directory file, add the '!' prefix to the macro name. The template directory configuration file is named 000000000000-directory~.xml. To use this file, remove the tilde (~) from the file name.

Special Characters

Macro names and macro labels cannot contain these special characters.

If they do, you may experience unpredictable behavior.

The following special characters are used to implement the enhanced feature key functionality:

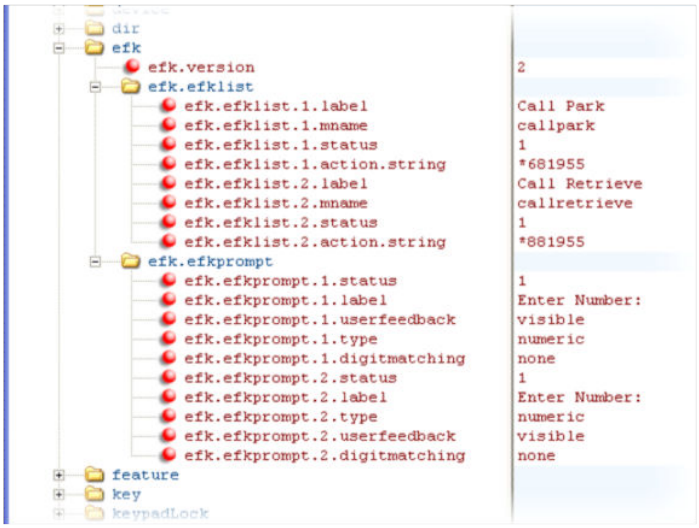
- ! The characters following it are a macro name.
- ' or ASCII (0x27) This character delimits the commands within the macro.
- $ This character delimits the parts of the macro string. This character must exist in pairs, where the $ delimits the characters to be expanded.
- ^ This character indicates that the following characters represent the expanded macro (as in the action string).
- Macro names and macro labels cannot contain these special characters. If they do, you may experience unpredictable behavior.

Enhanced Feature Key Example Configurations

The following configurations shown in the below illustration were set in the features.

cfg file:

- For the `efk.efklist.x.*` parameters, the following configurations were applied:
  - Line key 1 has been assigned a Call Park address (1955) and line key 2 a call retrieve function.
  - The parameter `acton.string` shows the macro definition for these two functions.
  - Status is enabled and a label has been specified to display next to the line key.
  - The entry in the `mname` parameter corresponds to the `contact (ct)` field in the contact directory.
- For the `efk.prompt.*` parameters, the following configurations were applied:
  - `Status` is enabled.
  - The label on the user prompt has been defined as Enter Number: and this prompt displays on the phone screen.
  - The `type` parameter has been set to `numeric` to allow only numbers.
  - `userfeedback` is specified as `visible` , which enables users to see the numbers entered into the prompt.



Mapping Internal Key Functions

A complete list of internal key functions for enhanced feature keys and hard key mappings is shown in the table Key Labels and Internal Functions.

Note the following guidelines:

- The **Function** value is case-sensitive.
- Some functions are dependent on call state. Generally, if the softkey displays on a call screen, the softkey function is executable.
- Some functions depend on the feature being enabled. For example, the BuddyStatus and MyStatus softkeys require the presence feature to be enabled.

- Hard key remappings don't require the enhanced feature key feature to be enabled. This includes the speed dial function on older platforms. On newer platforms, use line key functions.

The table below shows only line1 to line 6 functions.

Table 15-4 Key Labels and Internal Functions

Function	Description
ACDAvailable	Status for Automatic Call Distribution when available.
ACDCallCenterDispositionCode	Attributes applied to a call to identify marketing promotions. Example: cc-disposition-code@example.com;code=123
ACDCustomerOriginatedTrace	Issue a customer-originated trace. Example: customer-originated-trace@example.com; trace=call trace for an obsence, harassing, threating or answered call.
ACDEmergencyEscalation	Emergency escalate a call to an available supervisor number. Example: emergency-escalation@example.com;supervisor=2405555280
ACDLogin	Log in to Automatic Call Distribution.
ACDLogout	Log out from Automatic Call Distribution.
ACDUnavailable	Status for Automatic Call Distribution when unavailable.
Answer	Answer an incoming call. This function applies to call screen only.
Applications	Main Browser
ArrowDown	Move arrow down.
ArrowLeft	Move arrow left.
ArrowRight	Move arrow right.
ArrowUp	Move arrow up.
BargeIn	Barge In to show appearances, Barge In This function applies to call screen only.
BuddyStatus	Status of the contacts added to Buddy list.
Calendar	Displays the calendar screen.
Callers	Displays the list of callers.
CallList	Displays the call logs.
CallPark	Park an active call. This function applies to call screen only.
CallPickup	Call pick-up on the phone. This function applies to call screen only.
Conference	Begin a conference call. This function applies to call screen only.
Diagnostic	Displays the diagnostic screen.

Table 15-4 Key Labels and Internal Functions (continued)

Function	Description
Delete	Delete the selected item.
Dialpad0	Dialpad 0
Dialpad1	Dialpad 1
Dialpad2	Dialpad 2
Dialpad3	Dialpad 3
Dialpad4	Dialpad 4
Dialpad5	Dialpad 5
Dialpad6	Dialpad 6
Dialpad7	Dialpad 7
Dialpad8	Dialpad 8
Dialpad9	Dialpad 9
DialpadPound	Dialpad pound sign
DialpadStar	Dialpad star sign
DialpadURL	Go to a specific address or location. This function applies to call screen only.
DirectedPickup	Directed call pick-up on the phone. This function applies to call screen only.
Directories	Displays the directory items.
Divert	Forward a call.
DoNotDisturb	Don't Disturb menu.
EnterRecord	Enter a call record. This function applies to call screen only.
Exit	Exit existing menu. This function applies to Menu only.
Favorites	Displays the favorites list.
GAB	Displays Ribbon communications Global Address Book.
GroupPickup	Group call pick-up on the phone.
Handsfree	Use handsfree
Headset	Use headset This function applies to Desktop phones only.
Hold	Toggle hold
Join	Joins a call to an active call to make a conference. This function applies to call screen only.
LdapCorpDir	Displays the corporate directory menu screen.

Table 15-4 Key Labels and Internal Functions (continued)

Function	Description
LCR	Last Call Return
Line1	Line Key 1
Line2	Line Key 2
Line3	Line Key 3
Line4	Line Key 4
Line5	Line Key 5
Line6	Line Key 6
ListenMode	Turn on speaker to listen only.
LockPhone	Lock the phone.
MediaStat	Displays the media statistics screen.
Menu	Displays the main menu.
Messages	Messages menu
MicMute	Mute the microphone.
MyStatus	View my status.
NewCall	Place a new call. This function applies to call screen only.
Null	Do nothing
Offline	Offline for presence
PAB	Displays Ribbon communications personal address book.
Page	Group Paging
PageGroup	Initiates paging. Example: 5$APageGroup$ - It initiates the paging from default page group5. Admin must enable the input page channel.
ParkedPickup	Specifies how the phone performs a parked call pick-up. This function applies to call screen only.
Preferences	Displays the preference menu screen.
QuickSetup	Quick setup feature. This function applies to call screen only.
Redial	Redial the last dialed number. This function applies to call screen only.
Select	Select an item.
ServerACDAgentAvailable	Status for server-based Automatic Call Distribution agent when available.

Table 15-4 Key Labels and Internal Functions (continued)

Function	Description
ServerACDAgentUnavailable	Set the unavailable status for server-based Automatic Call Distribution agent. This macro functionality is extended to set the unavailable status with a mentioned reason code. Example: softkey.1.action="$FServerACDAgentUnavailable$ $R10001$"
ServerACDAgentAfterCallWork	Set the status after-call work for server-based Automatic Call Distribution agent. Example: softkey.1.action="$FServerACDAgentAfterCallWork$"
ServerACDSignIn	Log in to a server-based Automatic Call Distribution.
ServerACDSignOut	Log out from a server-based Automatic Call Distribution.
Setup	Settings menu
Silence	Silence the call ringer. This function applies to call screen only.
SoftKey1	Softkey 1
SoftKey2	Softkey 2
SoftKey3	Softkey 3
SoftKey4	Softkey 4
Softkey5	Softkey 5
SpeedDial	Place a call to a number assigned to the SpeedDial.
Split	Split a conference call. This function applies to call screen only.
Talk	Push-to-Talk
Transfer	Transfer a call. This function applies to call screen only.
UCOneDir	Displays the UCOne directory.
Video	Enables the video in a call. This function applies to Polycom VVX 501 and 601 business media phones.
VoiceMail	Displays voicemail messages for a registration line. This function must have a prefixed line index.
VolDown	Set volume down
VolUp	Set volume up

Macro Definitions

The `efk.efklist.x.action.string` can be defined by macro actions, prompt macro substitution or an expanded macro.

Macro Actions

The action string is executed in the order it displays.

User input is collected before any action is taken. The action string can contain the fields shown in the following table.

Table 15-5 Macro Actions

Action String	Description
$L<label>$	This is the label for the entire operation. The value can be any string including the null string (in this case, no label displays). This label is used if no other operation label collection method worked (up to the point where this field is introduced). Make this the first entry in the action string to be sure that this label is used; otherwise another label may be used and this one ignored.
digits	The digits to be sent. The appearance of this parameter depends on the action string.
$C<command>$	This is the command. It can appear anywhere in the action string. Supported commands (or shortcuts) include: hangup (`hu`) hold (`h`) waitconnect (`wc`) pause <number of seconds> (`p` <*num sec*>) where the maximum value is 10
$Tconsult$	An administrator uses this macro to execute a consultative transfer irrespective of the default transfer type. The input to this macro is given using star code sequences or prompt macro substitution. For example, Call Park - *68<Number>$Tconsult$ Consultative Transfer using direct number - <Number>$Tconsult$ Consultative Transfer using prompt - $P1N10$$Tconsult$
$T<type>$	The embedded action type. Multiple actions can be defined. Supported action types include: `invite dtmf refer intercom` Poly recommends that you always define this field. If it isn't defined, the supplied digits are dialed using INVITE (if no active call) or DTMF (if an active call). The use of refer method is call server dependent and may require the addition of star codes.
$M<macro>$	The embedded macro. The <macro> string must begin with a letter. If the macro name isn't defined, the execution of the action string fails.
$P<prompt num>N<num digits>$	The user input prompt string.
$S<speed dial index>$	The speed dial index. Only digits are valid. The action is found in the contact field of the local directory entry pointed to by the index.
$F<internal function>$	An internal key function. Mapping Internal Key Functions on page 211
$A<internal function>$	The internal key function. If you need to add a value to the macro use a parameter value before the macro definition. For example, 1$AVoiceMail$ - Voice mail is an internal function, which uses "1" as an input for the parameter.
URL	A URL. Only one per action string is supported.

Prompt Macro Substitution

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

Macros are case sensitive.

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

For example, the `efk.efklist.x.action.string` can be defined by a macro substitution string, PnNn, where the following applies:

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

Expanded Macros

Expanded macros are prefixed with the "^" character and are inserted directly into the local directory contact (ct) field.

Example Macros

This section provides examples of macros that you can use for line keys.

The action string `$Changup$*444*$P1N4$$Tinvite$$Cwaitconnect$$P2N3$$Cpause2$$Tdtmf$$Changup$` is executed in order as follows:

1. The user is prompted for 4 digits. For example, 1234.
2. The user is prompted for 3 digits. For example, 567.
3. The user's active call is disconnected.
4. The string *444*1234 is sent using the INVITE method.
5. After connection, there is a two second pause, and then the string 567 is sent using DTMF dialing on the active call.
6. The active call is disconnected.

Because line keys and their functions are linked to fields in the directory file, the macro name you enter in `efk.list.x.mname` must match the name you enter to the `contact (ct)` field in the directory file. The macro name you enter in the `(ct)` field of the directory file must begin with the '!' prefix.

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.

For more LED pattern configurations, see the *Poly Edge E Series Phones Parameter Reference Guide*

LED indicator pattern types

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

Table 15-6 LED Indicator Pattern Type

Pattern Type	Function
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.

LED Pattern Parameters

The LED pattern parameters 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 and a permitted value:

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

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

`ind.pattern.<pattern type>.step.x.state`
Specify whether the LED is on (1) or off (0) for the step.
The default value varies for different steps and pattern types.

0 - Turn off the LED indicator.

1 - Turn on the LED indicator.

`ind.pattern.<pattern type>.step.x.duration`
Specify the duration that the LED is on or off for the step.
The default value varies for different steps and pattern types.

Min - 0

Max - 32767

`ind.pattern.<pattern type>.step.x.color`
Specify the color that the LED uses for the step.
Depending on the pattern type, the default value varies.

Null

Red

Green

Yellow

Set an LED Pattern for Active Calls

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

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`. Alternatively, using RGB values in hex format is also permitted, for example, "#0000FF". 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) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

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 locally held calls

By default, the phone's LED blinks red for held calls. Configure the LED to blink red and green for locally held calls and to blink only red for held calls on shared lines.

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 Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable alternating red/green LED behavior for locally held calls.

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

3. Save the configuration file.

Configuring Line Key LEDs

Configure the appearance and behavior of line key LEDs.

Disable the Headset Key LED in Headset Memory Mode

Disable the flash pattern for the **Headset** key in Headset Memory Mode.

The **Headset** key flashes green for headsets by default while in headset memory mode. Disable the key flashes if the user finds it distracting or bothersome.

1. Open the configuration file.
2. Disable the **Headset** key LED flashing in headset memory mode.

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

3. Save the configuration file.

Surround Lighting Bar

Configure the appearance and behavior of the surround lighting bar.

Surround lighting bar pattern types

Use the values from the following table to indicate the surround lighting bar pattern type.

Table 15-7 LED indicator pattern type

Pattern type	Function
haloBluetoothScan	Sets the surround lighting bar behavior when scanning for Bluetooth devices.
haloCallConnected	Sets the surround lighting bar behavior when on a call.
haloCallConnectedDigitalHeadset	Sets the surround lighting bar behavior when on a call and a digital headset are connected.
haloCallOffering	Sets the surround lighting bar behavior when the phone is ringing.
haloCallHold	Sets the surround lighting bar behavior when the phone puts a call on hold.
haloDND	Sets the surround lighting bar behavior for Do not Disturb.
haloMute	Sets the surround lighting bar behavior when the phone is muted.
haloVoicemail	Sets the surround lighting bar behavior when there's a voicemail.
powerSaving	Sets the surround lighting bar behavior when the phone is in power saving mode.

Surround LED Lighting Bar Pattern Parameters

The surround lighting bar pattern parameters configure the pattern state, effect, color, and duration of the LED indicators.

NOTE: To activate a pattern, you must configure all parameters for a step.

For each parameter, specify the pattern type and a permitted value.

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

`ind.pattern.<pattern type>.step.1.state`
Specify whether the surround lighting bar is on (1) or off (0) for the step.
0 - Turn off the LED indicator.

1 - Turn on the LED indicator (default).

`ind.pattern.<pattern type>.step.1.duration`
Specify the duration that the surround lighting bar is on or off for the step, in milliseconds.
Depending on the pattern type, the default value varies.

Min - 0

Max - 32767

`ind.pattern.<pattern type>.step.1.color`
Depending on the pattern type, the default value varies. Express the values in plain English, in RGB hex format (*#RRGGBB*), or in RGB decimal string format (*RRR.GGG.BBB*).
Red

Green

Blue

Yellow

`ind.pattern.<pattern type>.step.1.effect`
Specify the effect that the surround lighting bar uses. Depending on the pattern type, the default value varies.
None: Solid color

DimmedBreathe: Intensity decreases from 50% to 0% and then back to 50%.

Breathe: Intensity decreases from 100% to 50% and then back to 100%.

BreatheBottom: On the bottom part of the display, intensity decreases from 100% to 50% and then back to 100% in one cycle.

Chase: Color rotates around the display (E300, E400 , and E500 Series) or back and forth on the LED bar (E100 and E220).

ChaseOnWhite: The same as Chase, but with the unlit LEDs set to white.

ChaseOnBlack: The same as Chase, but with the unlit LEDs set to black.

Activate Surround Lighting Bar Patterns

Activate surround lighting bar patterns to indicate various phone states.

To activate a surround lighting bar pattern, you must configure all parameters for the step.

1. Open the configuration file.
2. Specify the duration that the surround lighting bar is on or off for the step from 0 to 32767 milliseconds. The default varies depending on the type.

```
ind.pattern.<pattern type>.step.1.duration="<Duration>"
```

3. Specify the color for the LED pattern step. The default varies depending on the LED indicator pattern type.

   Express the values as color names, in RGB hex format (*#RRGGBB*), or in RGB decimal string format (*RRR.GGG.BBB*).

```
ind.pattern.<patterntype>.step.1.color="<Color>"
```

4. Specify the effect for the LED pattern step.

   For more information, see Surround LED Lighting Bar Pattern Parameters on page 223.

```
ind.pattern.<patterntype>.step.1.effect="<Effect>"
```

5. Save the configuration file.

Enable Mute Indication on the Surround Lighting Bar

Enable the mute indication surround lighting bar effect when the phone is in a call and muted.

1. Open the configuration file.
2. Enable the mute indication effect.

```
ind.led.alert.indicateMute="1"
```

3. Save the configuration file.

Enable Digital Headset Indication on the Surround Lighting Bar

Enable the headset indication surround lighting bar effect when the phone is in a call and a digital headset is connected.

1. Open the configuration file.
2. Enable the digital headset indication effect.

```
ind.led.alert.indicateDigitalHeadset="1"
```

3. Save the configuration file.

Disable Surround Lighting Bar in Power Saving Mode

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

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Disable the surround lighting bar in power saving mode.

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

3. Save the configuration file.

Disable halo when DnD is active

Disable the surround lighting bar while the phone is in Do Not Disturb mode

1. Open the configuration file.
2. Disable the surrounding lighting bar in power saving mode.

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

3. Save the configuration file.

Disable surround lighting bar when DnD is active

Disable the surround lighting bar while the phone is in Do Not Disturb (DND) mode.

1. Open the configuration file.

2. Disable the surround lighting bar in power saving mode.

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

3. Open the configuration file.

Flexible Line Key Assignment

By default, functions are assigned to line keys in the order in which the line key displays on the phone. The flexible line key feature enables you to break that ordering and assign a line key function to a line key that displays anywhere on the phone's screen.

You can apply this feature to any line key function, including a line appearance, speed dial, busy lamp field (BLF), presence, and Enhanced Feature Keys.

Line Key Registration Assignments

The number of line key assignments that a phone has depends on the number of physical line keys and whether an EM is connected.

Table 15-8 Poly Edge E Series Line Key Registration Assignments

Model	Physical Line Keys	Configurable Line Keys Without EM (primary screen)	Configurable Line Keys (secondary screen)
Edge E100	2	8	–
Edge E220	4	16	–
Edge E300 Series	8	32	–
Edge E400 Series	8 (primary) + 6 (secondary)	32	12
Edge E500 Series	12	48	–

Line Key Numbering

Line keys on Poly phones and expansion modules (EM) are numbered sequentially, and the line key numbering on expansion modules depend on how many lines the phone supports.

For example, an Edge E500 phone supports 12 lines, numbered 1 to 12. Therefore, the first line on an expansion module connected to an Edge E500 phone is line 13.

Table 15-9 Line Key Numbering on Poly Edge E Series Phones

Phone Model or Series	Supported Line Keys	Page Number
E100	1 to 2	1
	3 to 4	2
	5 to 6	3
	7 to 8	4
E220	1 to 4	1
	5 to 8	2
	9 to 12	3
	13 to 16	4

Table 15-9 Line Key Numbering on Poly Edge E Series Phones (continued)

Phone Model or Series	Supported Line Keys	Page Number
E300 Series	1 to 8	1
	9 to 16	2
	17 to 24	3
	25 to 32	4
E400 Series (without EM)	1 to 8	Primary screen, page 1
	9 to 14	Secondary screen, page 1
	15 to 20	Secondary screen, page 2
	21 to 28	Primary screen, page 2
	29 to 36	Primary screen, page 3
	37 to 44	Primary screen, page 4
E400 Series (with EM)	1 to 8	Primary screen, page 1
	9 to 14	Secondary screen, page 1
	15 to 20	Secondary screen, page 2
	21 to 86	EM, pages 1 to 3
E500 Series (without EM)	1 to 12	1
	13 to 24	2
	25 to 36	3
	37 to 48	4
E500 Series (with EMs)	1 to 12	Primary screen, page 1
	13 to 78	EM 1, pages 1 to 3
	79 to 144	EM 2, pages 1 to 3

Configure Flexible Line Keys

Configure flexible line key assignments and enable users to assign a line key function to any line key on their phone.

Line keys that you configure using this feature override the default line key assignments and any custom line key configurations you may have made.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable flexible line key reassignment.

```
lineKey.reassignment.enabled="1"
```

3. Assign a category to each line key.

```
lineKey.x.category="<value>"
```

Supported categories include:

- Any (default)
- Unassigned
- Line
- BLF
- EFK
- SpeedDial
- Presence

4. Specify an index number that corresponds with the category set for the key. For more information, see Flexible Line Key Assignment Categories and Index on page 229.

```
lineKey.x.index="<value>"
```

NOTE: When you set `lineKey.x.category="Any"`, the phone ignores the value set for `lineKey.x.index` .

5. Save the configuration file.

Flexible Line Key Assignment Categories and Index

The FLK category specifies the function of the line key. The index specifies the order in which the line keys display on the phone screen.

Use the following table to assign a category and an index to the line keys on your phone.

Table 15-10 Flexible Line Key Assignment Categories and Index

Category	Index
Unassigned	Null
Line	The Line index number.
BLF	Static BLF index number if `up.staticBLF.FLKIndexRequired="1"`; otherwise, use 0 for automatic ordering.
Speed Dial	The favorite index from someone in your directory.
EFK	EFK index number if `up.EFK.FLKIndexRequired="1"`; otherwise, use 0 for automatic ordering.
Presence	0
Any	Null.

Using the Any Category

Any keys configured with the "Any" category are assigned the remaining functions that weren't assigned to any other keys.

When the parameter `lineKey.x.category` is set to "Any", the phone assigns the functions in the following order:

1. Registrations
2. EFK
3. BLF
4. Presence
5. SpeedDial

Assigning Busy Lamp Field (BLF) and Presence to Line Keys

BLF and presence line keys are self-ordering. If you have these features assigned to multiple line keys, you can specify the location of the BLF or presence line key but not the order in which they display.

For example, you can assign a BLF line key to index 1, 3, and 5 but you cannot specify how the contacts are ordered or which BLF contacts display on line keys 1, 3, and 5.

BLFs can be ordered by index when up.staticBLF.FLKIndexRequired="1", but presence can't.

Assign BLF to a Line Key

Configure line keys for busy lamp field (BLF) to enable users to monitor multiple contacts.

Before assigning BLF to a line key, configure the feature for the phones. See Configure a Busy Lamp Field Resource in the Configuration File on page 137 and Subscribe to a Busy Lamp Field Resource List on a Call Server on page 136.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable flexible line key reassignment.

```
lineKey.reassignment.enabled="1"
```

3. Assign the category BLF to each line key.

```
lineKey.x.category="BLF"
```

4. If the customer wants the line index to be ordered automatically, set the line index for automatic ordering.

```
lineKey.x.index="0"
```

5. If the customer wants to specify the BLF index, do the following:

a. Enable the `up.staticBLF.FLKIndexRequired` parameter.

```
up.staticBLF.FLKIndexRequired="1"
```

b. Set the line index to use the BLF index.

```
lineKey.x.index="<BLFIndex>"
```

6. Save the configuration file.

Assign Presence to Line Keys

Configure line keys for presence to enable users to monitor multiple contacts.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable flexible line key reassignment.

```
lineKey.reassignment.enabled="1"
```

3. Assign the `Presence` category to each line key.

```
lineKey.x.category="Presence"
```

4. Set the line index for automatic ordering.

```
lineKey.x.index="0"
```

5. Save the configuration file.

Poly Edge E400 Series Secondary Screen

Poly Edge E400 Series phones have a secondary screen for viewing and managing lines, BLFs, EFKs, and speed dial favorites.

Specifying the Location of Lines, BLFs, EFKs, and Speed Dial Favorites

On an Edge E400 Series phone, you can specify registered lines, BLF resource lists, BLF resources, EFKs, and speed dial favorites to display on the primary screen, the secondary screen, or both.

Specify the Location of a Registered Line

On an Edge E400 series phone, you can configure a registered line to display on the primary screen, the secondary screen, or both.

NOTE: When line key reassignment is enabled (`linekey.reassignment.enabled="1"`), this feature has no effect. BLFs, EFKs, and speed dials are placed on the screen according to their LKR configuration.

1. Open the configuration file.
2. Specify the location of a registered line with one of the following values. The default value is Primary. Replace X with the registered line key number.
   - `Primary`
   - `Secondary`
   - `PrimaryandSecondary`

```
reg.X.location="<value>"
```

3. Save the configuration file.

Specify the Location of a BLF Resource List

On an Edge E400 Series phone, you can configure a BLF resource list to display on the primary screen, the secondary screen, or both.

NOTE: When line key reassignment is enabled (`linekey.reassignment.enabled="1"`), this feature has no effect. BLFs, EFKs, and speed dials are placed on the screen according to their LKR configuration.

1. Open the configuration file.
2. Specify the location of the BLF resource list with one of the following values. The default value is Primary.
   - `Primary`
   - `Secondary`
   - `PrimaryandSecondary`

```
attendant.uri.location="<value>"
```

3. Save the configuration file.

Specify the Location of a BLF Resource

On an Edge E400 Series phone, you can configure a BLF resource to display on the primary screen, the secondary screen, or both.

NOTE: When line key reassignment is enabled (`linekey.reassignment.enabled="1"`), this feature has no effect. BLFs, EFKs, and speed dials are placed on the screen according to their LKR configuration.

1. Open the configuration file.
2. Specify the location of the BLF resource with one of the following values. The default value is Primary. Replace X with the resource's BLF index number.
   - `Primary`
   - `Secondary`
   - `PrimaryandSecondary`

```
attendant.resourceList.X.location=”<value>”
```

3. Save the configuration file.

Specify the Location of an EFK

On an Edge E400 Series phone, you can configure an EFK to display on the primary screen, the secondary screen, or both.

NOTE: When line key reassignment is enabled (`linekey.reassignment.enabled="1"`), this feature has no effect. BLFs, EFKs, and speed dials are placed on the screen according to their LKR configuration.

1. Open the configuration file.
2. Specify the location of the EFK with one of the following values. The default value is Primary.
   - `Primary`
   - `Secondary`
   - `PrimaryandSecondary`

```
efk.efklist.X.location="<value>"
```

3. Save the configuration file.

Specify the Location of a Speed Dial Favorite

On an Edge E400 Series phone, you can configure speed dial favorites to display on the primary screen or the secondary screen.

NOTE: When line key reassignment is enabled (`linekey.reassignment.enabled="1"`), this feature has no effect. BLFs, EFKs, and speed dials are placed on the screen according to their LKR configuration.

1. Open the directory file for the phone.
2. Add and set the `<loc></loc>` element for the speed dial favorite with one of the following values. The default value is 0 (Primary).
   - 0 (Primary)
   - 1 (Secondary)

```
<loc>1</loc>
```

3. Save the directory file.

16 Phone Maintenance

Perform system management and maintenance tasks on your phone and upgrade the software.

Cloud-Based Configuration and Management Methods

Use Poly Device Management Service for Service Providers (PDMS-SP) or Poly Lens to configure and manage phones.

Enable PDMS-SP Onboarding

1. Obtain the Onboarding Service Tag from the PDMS-SP ITSP portal.
   a. Log in to the PDMS-SP portal.
   b. Click **Service API**.
   c. Copy the **Onboarding Service Tag** value.
2. **Optional:** Obtain a PDMS-SP onboarding service tag for a specific organization.

   If you've created a hierarchy of multiple organizations under your top level Tenant, each organization has a unique Onboarding Service Tag that enables you to immediately link devices with that specific organization.
   a. Click **Manage Organizations**.
   b. Click the organization name.
   c. Click **Service API**.
   d. Copy the **Onboarding Service Tag** value for the organization.
3. Open the configuration file.
4. Enable onboarding for PDMS-SP.

```
feature.da.enabled="1"
feature.obitalk.enabled="1"
obitalk.accountCode="<Onboarding_Service_Tag>"
```

5. **Optional:** Enable packet capture so the phone can upload packet captures to PDMS-SP.

```
diags.pcap.enabled="1"
```

6. **Optional:** Set the self-note value that the phone sends to PDMS-SP. The maximum string length is 512 characters.

```
deviceAnalytics.note="<self_note_value>"
```

7. **Optional:** Specify the list of device analytics services to enable. Separate items with a comma.

   The maximum length is 2048 characters. The default value is `all`, which enables all device analytic services.

```
da.supported.services="<Service1,Service2,Service3>"
```

8. Save the configuration file.

Poly Lens

Poly Lens lets you monitor and manage device health with actionable insights, including device status and usage for phones on the network.

For information about Poly Lens, including onboarding your phone, see the Poly Lens Documentation.

Poly phones send the following device 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
- Device details are updated or changed

Analytics support for Poly Cloud Services

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

NOTE: Device analytics is not enabled by default on CCX phones. To enable device analytics, include the following parameter in the configuration file: `feature.da.enabled="1"`.

Poly phones send the following details to the cloud:

- Device Asset
- Device Network
- Device Diagnostics

Poly phones send the device details to the cloud when the following occurs:

- Phone restarts or reboots
- On-demand request from the cloud
- Device details are updated or changed

Importing and exporting configurations

Enable device analytics to export and import device configurations to and from the cloud.

When you enable device analytics and set the `da.supported.services` value to `all` or `config`, you can configure the following device options:

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

Busy Lamp Field Analytics

When you enable Device Analytics and set `da.supported.services` to `all` or `blf`, the phone sends certain BLF details to the cloud.

The phone sends the following details to the cloud:

- The total number of configured Busy Lamp Field (BLF) lines.
- The total number of dropped BLF line notification.
- The total number of actions/pickup on BLF line.
- The phone increments the BLF's line notification for every new notification for each BLF configured line.

Shared Call Appearance Analytics

When you enable Device Analytics and set `da.supported.services` to `all` or `sca`, the phone sends certain information to the cloud.

The phone sends the following details are sent to the cloud:

- The total number of registered Shared Call Appearance (SCA) lines.
- The total number of action or resume/barge-in on SCA line.
- The phone increments the SCA line notification for every new notification of call-info, line-seize, and dialog for each SCA configured line.

User Interface Analytics

User Interface analytics enables you to upload phone activity to the cloud when you set `da.supported.services` to `all` or `uianalytics`.

Key-Press Analytics

Key-press analytics enables you to track and maintain hard and soft key press count on the phone for each key.

You can upload key-press counts at intervals you configure. Counters per key are reset after each upload. You cannot record the sequence of the key presses on the phone.

Feature Access Analytics

Feature access analytics enables you to track and maintain features that users access on the phone.

When a user accesses a feature, the corresponding feature counter is incremented. You can upload feature counts at an interval you configure. Feature counters are reset after each upload.

Uptime Analytics

The phone keeps track of various services and uploads the active status to cloud periodically when `da.supported.services` value is set as `all` or `uptimeanalytics`.

The phone monitors and sends the following services details to the cloud:

- Exchange Services (Calendar, Call logs, and Contacts)
- Provisioning Server
- Cisco BroadWorks Directory
- Corporate Directory
- Ribbon Communications PAB-GAB Directory

The phone immediately sends the change in service connectivity status to the cloud. For example, if the Microsoft Exchange server gets an authentication failure, the failed authentication details are sent to cloud immediately.

If there's no change in the service connectivity status, the phone periodically sends the status to the cloud based on the configured interval. The phone also sends the last access time of the service to the server along with response codes and failure reason if any.

Hardware Analytics

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

Poly phones send and upload the following hardware analytics and information to the cloud:

- **CPU Monitoring Service** – Sends CPU details for software processes along with total CPU consumed, Timestamp, and Monotonic time. You can set the values for trigger points such as `UpperCPUValue` and `LowerCPUValue` in percentage from the cloud. The following actions trigger the phone to send CPU details to the cloud:
  - The CPU usage value equals or goes above the `UpperCPUValue`.
  - The CPU usage value equals or goes below the `LowerCPUValue`.
  - The `UpperCPUValue` and `LowerCPUValue` are 0.

    The phone collects the records at every defined time interval. On receiving a stop command from the cloud or after timeout, the phone sends the collected records to the cloud. However, if the number of records crosses the limit of 100, the records are sent to the cloud and the counter is reset.
- **Packet Loss Service** – Uploads L2 layer network statistics (received) to the cloud through Packet Loss Service. This service has the following Rx L2 parameters:
  - `rxDiscard`
  - `rxUnicastPkts`
  - `rxBroadcastPkts`
  - `rxMulticastPkts`

  This service has the following fields:
  - `eventMonotonicTime` – Time since DUT is up.
  - `uploadTime` – Time at which DUT sends the packet to the cloud.
  - `versionInfo` – Every INLINE message sent to cloud contains the `versionInfo` parameter to indicate version of that message. Minor or major version change depends on type of change with respect to particular message in subsequent releases.

  The following action triggers the phone to send packet loss details to the cloud:
  - Timeout
  - Manually stopping service by issuing stop request

  This service is applicable only for Ethernet.
- **Memory Monitoring Service** – Sends memory monitoring details for software processes along with total used, cached, and free memory to the cloud.

  Memory metrics is controlled through two parameters: `UpperMemoryValue` and `LowerMemoryValue`. The following actions trigger the phone to send memory monitoring details to the cloud:
  - Free memory is equal to and below `LowerMemoryValue` (Normal to Low memory)
  - Free memory is equal to and above `UpperMemoryValue` (Low to Normal memory)

When you define `LowerMemoryValue` and `UpperMemoryValue`as 0, memory information is shared with the cloud periodically.

Device Details Sent to the Cloud

When you enable device analytics, the phones can send various details regarding the device to the cloud service.

Device Asset Details

Device asset details include details for a primary device and SIP service. A primary device consists of Poly phones, and a secondary device consists of Bluetooth or USB headsets, expansion modules (if supported), connected cameras, and a PC port.

When you enable device analytics, the phone sends the following primary device details to the cloud:

- Manufacturer
- Product Family
- Power Source
- MAC Address
- PCS Number
- PCS Account Code
- Region Code
- Version Information
- Hardware Model
- Hardware Revision
- Hardware Part number
- Serial Number
- OBi Number
- Offset GMT
- Reboot Type
- Mac Address
- Software Release
- Upload Time
- Updater Version

Secondary Device Details

When you connect a secondary device to a Poly phone and enable device analytics with the parameter `da.supported.services` value set as `all` or `sdi`, the secondary device details are sent to the cloud.

The following table lists supported secondary devices and the device details that they send to the cloud:

Table 16-1 Secondary Device Details

Bluetooth Headset	USB Headset	Expansion Module	PC Port
• Connection Type • Peripheral Type • Display Name • Bluetooth Address	• Display Name • Connection Type • Peripheral Type • Power Source	• Display Name • Connection Type • Serial Number • Peripheral Type	• Mac Address • Display Name • PC Port Status • PC Port Speed • PC Port Mode • Connection Type • Peripheral Type • Serial Number

Service Details

When you enable device analytics and set the `da.supported.services` parameter value to `all` or `service`, the phone sends certain information to the cloud.

The phone sends the following SIP service details to the cloud:

- Registration Type
- SIP Server Address
- SIP User Registration Address
- SIP User ID
- Transport Protocol
- SIP Port
- Outbound Proxy Address
- Outbound Proxy Transport Protocol
- Outbound Proxy Port
- Line Type
- Display Name
- Registration Status
- Registration Refresh Time
- Registration Failure Reason
- Server Platform
- Registration Line Index

Device Network Details

When the phone's network boots up or when there's a change in network parameters. the phone sends device network details to Polycom Cloud Services.

Poly phones send network information for the Ethernet to the cloud when the phone is idle and send Wi-Fi information to the cloud at any time.

When you enable device analytics and set the `da.supported.services` parameter value to `all` or `ni`, the phone sends the following device network details for Ethernet to the cloud:

- Connection Type
- IPv4 Address
- IPv4 Subnet
- IPv4 Gateway
- VLAN
- IPv4 Address Source
- Interface Name
- DNS Primary Address
- DNS Alternative Address
- DNS Domain
- Connection Speed
- PC Port Status
- LLDP Status
- LLDP Neighbors
- LLDP Location Information
- CDP Status
- 802.1x Status
- NTP Server
- EAP Method
- Provisioning Protocol
- Connection Mode

When Poly phones are connected to a wireless network, the phones send the following network details for the wireless network to the cloud:

- IPv4 Subnet
- Upload Time
- Version Information

- Wi-Fi Channel
- Connection Type
- Regulatory Domain
- IPv4 Address
- IPv4 Gateway
- DNS Primary Address
- DNS Alternative Address
- Interface Name
- IPv4 Address Source
- DNS Domain
- EAP Method
- Provisioning Protocol
- MIC Error Count
- EAP Error Count
- NTP Server

Monitoring the phone's memory usage

If you're using a range of phone features, customized configurations, or advanced features, you might need to manage phone memory resources.

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

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

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

Phone memory resources

If you need to free up memory on your phone, review the following table for the amount of memory each customizable feature uses. You can then reduce the amount of memory you need the feature to use.

Table 16-2 Phone Memory Resources

Feature	Typical Memory Size	Description
Custom idle display image	15 KB	The average size of the display image is 15 KB. Custom idle display image files should also be no more than 15 KB.
Local contact directory	42.5 KB	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: • 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	The system web interface (Web Configuration Utility) runs on a web browser.

Check memory usage from the local interface

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

Before you check the memory usage, load and configure the features and files you want to make available on the phone's local interface.

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

Configure a phone memory alert

Configure the alert when the phone's available memory falls below a percentage threshold.

If the phone's free memory falls below this threshold, the phone displays a warning message. The default setting is 20%. You can also configure the interval, in minutes, that the phone checks its available memory.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Adjust the available memory threshold percentage.

   The default is `20`. The value range is 20 to 40.

   ```
   up.sysFreeMemThresholdPercent="<value>"
   ```

3. Set the interval, in minutes, that the phone checks its available memory.

   The default is `0`. The value range is 0 to 1440.

   ```
   up.lowSysMemWarn.timeInMins="<value>"
   ```

4. Save the configuration file.

Memory usage errors in the application log

Each time the phone's minimum free memory goes below about 5%, the phone displays a message in the application log that the minimum free memory has been reached.

The application log file is enabled by default. The file is uploaded to the provisioning server directory on a configurable schedule. You can also upload a log file manually.

Capturing the Phone's Screen

Capture the phone's current screen as a saved image on your computer.

This can be helpful when explaining a problem or providing instructions.

Enable Screen Capture

Before screen capture is available, you must enable it either through configuration or the system web interface.

1. Find your phone's IP address by pressing the checkmark button in the center of the phone's navigation circle.
2. To log in to your phone's web interface, enter the phone's IP address into a web browser and then enter the administrator password.
3. Select **Diagnostics** > **Screen Capture**.
4. Toggle **Enable Screen Capture** to **On**.

   Screen capture is available for the main display as well for expansion module displays.

Capture the Phone's Screen

Capture and save a screenshot of the phone's display.

1. Set the phone to the screen you want to capture.
2. In the system web interface, go to **Diagnostics** > **Screen Capture**.
3. Enter the username `Polycom` and the phone's current administrator password.

   The web browser displays an image showing the phone's current screen. You can save the image as a `.bmp` file.

Rebooting the Phone

Reboot the phone when you want to send configuration changes that require a phone reboot.

Configure your phone to reboot in the following scenarios:

- At a scheduled time
- When paired to a network device

Reboot the Phone

Reboot the phone from the local interface when you want to send configuration changes that require a phone reboot.

Parameters that require a reboot are marked in this guide. If a configuration change doesn't require a reboot, you can update the configuration.

- Do one of the following:
  - Go to **Settings** > **Advanced** > **Reboot Phone**.
  - Go to **Settings** > **Basic** > **Update Configuration**.

If new software is available on the provisioning server, the phone downloads the software and immediately reboots.

Reboot the phone at a scheduled time

Configure your phones to reboot at a scheduled time, time period, or day.

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

   For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

   Open the configuration file.

2. Enable scheduled reboot on the phone.

```
prov.scheduledReboot.enabled="1"
```

3. Specify the time, in days, between scheduled reboots.

   The default is `1`. The value range is 1 to 365.

```
prov.scheduledReboot.periodDays="<value>"
```

4. Specify a time to reboot the phone. Use 24-hour time format (hh:mm).

   The default is `03:00`.

```
prov.scheduledReboot.time="<value>"
```

5. **Optional:** Set to a specific time to randomize the scheduled reboot between the time you set for `prov.scheduledReboot.time` and this parameter. Use 24-hour time format (hh:mm).

   The default is `Null`.

```
prov.scheduledReboot.timeRandomEnd="<value>"
```

6. Save the configuration file.

Disable the phone boot status message

By default, the phone displays its status IP address, VLAN ID, provisioning status, and SNTP status in a dialog every time it reboots. Prevent the message from displaying.

NOTE: Reboot status may not be in sync or as expected due to limitation on network activity.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Disable the phone's boot status dialog.

```
up.phoneBootStatusPopupEnabled="0"
```

3. Save the configuration file.

Upgrading the Software

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

New software versions may offer only small enhancements to improve the user experience, or they may be large software upgrades that offer new features.

Important update information for PVOS 9.0.0

For all this PVOS software release includes a major Android platform update.

Note the following important information before updating to PVOS 9.0.0:

- Don't turn off the power during the upgrade process.
- After you upgrade your or phone to PVOS 9.0.0, PVOS 9.0.0 becomes the new minimum software version. Returning to PVOS software versions earlier than PVOS 9.0.0 requires the use of a one-time downgrade utility.
- You can upgrade to PVOS 9.0.0 from any earlier PVOS or UC Software version.
- The PVOS 9.0.0 software package contains several upgrade components and is larger than a typical PVOS release. The total duration of the file download, installation, and update can take 30 to 60 minutes or longer, depending on the speed of your network. Most of the upgrade duration is the software download, which occurs as a background service so you can use your phone as normal.
- Your device may restart several times during the upgrade.
  - Upgrading to PVOS 9.0.0 from versions earlier than PVOS 8.1.4 automatically installs PVOS 8.1.4 first, as it contains resources necessary to upgrade the OS to Android 12.
  - Phones already running PVOS 8.1.4 or later skip the interim step and upgrade directly to PVOS 9.0.0.



NOTE: Your phone doesn't restart during an active call. If a call is active when the phone completes the download of an installation stage, the restart occurs immediately after the call ends.

- Applicable if upgrading from 8.1.3 or earlier: If a software provisioning server becomes unreachable after the installation of the first component of the software package, the phone remains on the interim software package until the server becomes reachable again. The update attempts to continue after a restart, a check-sync, or at the next scheduled configuration polling time.

Downgrading PVOS 9.X.X to earlier software versions

After you update your phone to PVOS 9.X.X, a downgrade to earlier software versions requires the use of a one-time downgrade software package that allows transition from the Android™ 12 OS to the Android 9 OS.

The downgrade package contains two software updates within a single file that are installed in sequence as follows:

- Your phone downloads the downgrade package and restarts to install an interim software version that downgrades the Android OS from Android 12 to Android 9.

- After you install the interim software, your device downloads the second component of the downgrade package and restarts to complete the installation of the PVOS 8.1.5 generally available release.

If you want to use a software version other than PVOS 8.1.5, you can now install that version in the same way that you would install any other PVOS version.

Information removed and retained after downgrading

The downgrade process includes a file system format that removes user data and most configurations.

Information removed when downgrading

- Microsoft Teams sign-in information
-
- Poly Studio X Series video bar pairing
- Paired Bluetooth devices
- Configuration changes made or imported from the system web interface that are not listed in the retained information list
- Basic configuration settings such as ring tones, power saving, and OpenSIP speed dials
- SCEP server and client configuration (certificates installed using SCEP are retained)
- Web proxy information

Information retained when downgrading

- DHCP, DNS, SNTP, IP, Ethernet, and Wi-Fi settings
- LLDP, CDP, and custom VLAN settings
- Syslog settings
- 802.1X settings, Custom CA certificates, device certificates and keys, and TLS profile settings
- Provisioning server address
- Base profile
- Admin and user passwords
- Settings hosted on your service provider's provisioning service or the Poly Lens device management service (recovered once your phone reconnects after the downgrade)

Configure software rollback prevention

This optional configuration parameter enables you to restrict software downgrades.

Make sure your configuration file includes `device.set="1"`.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Set the following parameter to prevent the phone from loading previous versions of the software.

```
device.set="1"
device.prov.rollbackProtection.set="1"
device.prov.rollbackProtection="Enabled"
```

3. Save the configuration file.

Downgrade restriction parameters

These parameters enable stricter software management policies for your phone deployment.

device.prov.rollbackProtection
Values: Auto, Enabled, Disabled
Default: Auto
The default value of "Auto" means that for phones running the Microsoft Teams base profile, rollback protection is enabled by default. However, for all other base profiles, rollback protection is disabled by default.
Enabled: The phone doesn't permit downgrade to any earlier release regardless of the current base profile.
Disabled: Any compatible software release can be installed.

Upgrading the software on a single phone

Use the **Software Upgrade** tool in the system web interface to update the software version on a single phone.

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

Configuration changes made to individual phones using the system web interface override configuration settings made using central provisioning.

Configure user-controlled software updates and polling

Upgrade software with the user-controlled software upgrade feature.

Set a polling policy and polling time period at which the phone polls the server for software updates and displays a notification on the phone to update software. For example, if you set the polling policy to poll every four hours, the phone polls the server for new software every four hours and displays a notification that says a software update is available. Users can choose to update the software right then, or they can postpone it a maximum of three times for up to six hours. The phone automatically updates the software after three postponements or after six hours, whichever comes first.

If a user postpones a software update, configuration changes and software version updates from both the server and the system web interface postpone as well. The server and system web interface send their configuration and software version changes to the phone when the user chooses to update.

You can send earlier or later versions of the software to your users' phones. User-controlled updates apply to configuration changes and software updates you make on the server and the system web interface.

This feature doesn't work if you enable ZTP.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Display the **Ignore** and **Ignore until next Reboot/Sync** options during a software upgrade alert. This gives users the option to completely ignore software updates or defer them until the next reboot or sync event.

```
prov.usercontrol.optionToIgnore="1"
```

3. **Optional:** Adjust the postponement duration using the HH:MM format.

   The default is `02:00` (2 hours).

```
prov.usercontrol.postponeTime="<HH:MM>"
```

4. Save the configuration file.

Update PVOS using a USB flash drive

Use a USB flash drive to update the software on your phone.

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

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 PVOS from Poly Lens.
3. Copy the configuration files that you want to use to the root of the USB flash drive.

   You must copy at least the primary configuration file (`000000000000.cfg`) and the product-specific configuration files to the USB flash drive:
4. Insert the USB flash drive into the USB port.

   The phone detects the flash drive automatically.
5. Enter the administrator password.

   The phone starts the update within 30 seconds of entering the correct administrator password.

   The system may reboot several times during the update. The update is complete when the indicator lights stop blinking and the *Home* screen displays.

Resetting a Phone to Factory Defaults

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

Reset the Phone and Configuration

When you reset your phone, you can choose a complete configuration reset or choose partial reset options.

1. Go to **Settings** > **Advanced** > **Administration Settings**.
2. Select **Reset to Defaults** and choose a reset option:
   - **Reset Local Configuration**: Clears the override file generated when you make changes using the phone's local interface.
   - **Reset Web Configuration**: Clears the override file generated by changes made using the system web interface.
   - **Reset Cloud Configuration**: Clears any configuration received from the configuration source identified by `cfgParamSourceCloud`.
   - **Reset Device Settings**: Resets the phone's flash file system settings not stored in an override file. These settings are your network and provisioning server settings and include custom certificates and encryption keys. Local, web, and other configuration files remain intact.
   - **Format File System**: Formats the phone's flash file system and deletes the software application, log, configuration, and override files. Note that if the override file is stored on the provisioning server, the phone redownloads the override file when you provision the phone again. Formatting the phone's file system doesn't delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the phone.
   - **Reset to Factory**: Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the PVOS 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 PVOS 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.

Enable Users to Reset the Phone to Factory

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

Make sure your configuration file includes `device.set="1"`.



NOTE: For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the phone to write the parameter to the phone's flash.

1. Open the configuration file.
2. Display the **Reset to Factory** option under the **Basic** settings.

```
up.basicSettings.factoryResetEnabled="1"
```

3. **Optional:** Adjust which settings the phone resets when a user performs a factory reset. You can preserve just the administrator password or the administrator password and the provisioning settings.

   Enable device.set for `device.system.recoveryType`:

   ```
   device.system.recoveryType.set="1"
   ```

   To preserve just the administrator password, set the following parameter:

   ```
   device.system.recoveryType="PreserveAdmin"
   ```

   To preserve the administrator password and the provisioning settings, set the following parameters:

   ```
   device.system.recoveryType="CloudProv"
   ```

4. Save the configuration file.

17 Third-Party Servers

This section explains certain features you can configure 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.

Features that Require Cisco BroadWorks XSP Authentication

A small set of Cisco BroadWorks features require you to authenticate Poly phones with the Cisco BroadWorks XSP service interface before configuring the features on your phones.

The following Cisco BroadWorks features require XSP authentication:

- Enhanced call park
- Executive-Assistant
- UC-One integration and features

Authenticate phones using SIP credentials

If your server is running Cisco BroadWorks R19 Service Pack 1 or later, authenticate the phones on the BroadWorks server using the same SIP credentials you use to register the phone lines.

1. Open the configuration file.
2. Configure the server address for your BroadWorks XSP directory. Replace *x* with the registered line number.

```
dir.broadsoft.xsp.address="<server address>"
```

3. Enter the BroadWorks XSP user ID. Replace *x* with the registered line number.

```
reg.x.broadsoft.userId="<XSP user ID>"
```

4. Enter the SIP user ID. Replace *x* with the registered line number.

```
reg.x.auth.userId="<user ID>"
```

5. Enter the SIP password. Replace *x* with the registered line number.

```
reg.x.auth.password="<password>"
```

6. Save the configuration file.

Authenticate phones using Cisco BroadWorks XSP credentials

If your server is running BroadWorks R19 or earlier, authenticate your phone using Cisco BroadWorks XSP credentials.

1. Open the configuration file.
2. Configure the server address for your BroadWorks XSP directory.

```
dir.broadsoft.xsp.address="<server address>"
```

3. Require the phone to use BroadWorks XSP credentials. Replace *x* with the registered line number.

```
reg.x.broadsoft.useXspCredentials="1"
```

4. Configure the user ID for BroadWorks XSP services. Replace *x* with the registered line number.

```
reg.x.broadsoft.userId="<user ID>"
```

5. Configure the password for BroadWorks XSP services. Replace *x* with the registered line number.

```
reg.x.broadsoft.xsp.password="<password>"
```

6. Save the configuration file.

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

Features Supported with the UC-One Integration

When you integrate Poly phones with UC-One, users can access and use BroadWorks directory, favorites, and presence features.

The following features are available on Poly phones with integrated with UC-One:

- **BroadWorks Directory**: Displays information for all users in the enterprise. For example, work and mobile phone numbers.
- **BroadWorks Self-Presence**: Displays the user's aggregated presence received from the Cisco BroadWorks Messaging Server on the phone.

- **BroadCloud Presence**: Enables users to share presence information with the BroadTouch Business Communicator (BTBC) client application.
- **BroadCloud Favorites**: Enables users to mark contacts as favorites with the BroadTouch Business Communicator (BTBC) client application.

Required Cisco BroadWorks Platform

UC-One features require support from the Cisco BroadWorks R18 SP1 platform with the latest patches and Cisco BroadCloud services.

Enable UC-One integration

Configure your phones to integrate with UC-One.

Before configuring this feature, authenticate your Poly phones with the Cisco BroadWorks XSP service interface. For more information, see .Authentication with CISCO BroadWorks XSP Service Interface.

IMPORTANT: Configuring the following parameter(s) may cause the phone to reboot. Dependencies and overrides may affect other parameters.

For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the UC-One feature.

```
feature.broadsoftUcOne.enabled="1"
```

3. Enable the QML viewer on the phone. This is required for the UC-One directory user interface.

```
feature.qml.enabled="1"
```

4. Enable simple search for Enterprise Directories.

```
feature.broadsoftdir.enabled="1"
```

5. Enable the presence feature, which includes buddy management and user status.

```
feature.presence.enabled="1"
```

6. Save the configuration file.

Cisco BroadWorks Directory Support

After you enable Poly phones to integrate with UC-One, configure access to any of the Cisco BroadWorks directories on Poly phones.

Types of Cisco BroadWorks Directories

When you integrate Cisco BroadWorks directories with Poly phones, users can access the different types of directories and search for contacts.

There are five types of Cisco BroadWorks directories:

- **Enterprise Directory**: This directory enables users to search and view an enterprise Active Directory. Users can query by first name, last name, phone number, extension and mobile number, and access contact information.
- **Group Directory**: This directory enables users to view the contact details of contacts within a group. Users can place a call to anyone in the user group.
- **Group Common Directory**: This directory enables users to view the contact details of common contacts listed in the Group Common Directory.
- **Enterprise Common Directory**: This directory enables users to view the contact details such as names and phone numbers of common contacts listed in the Enterprise Common Directory.
- **Personal Directory**: This directory enables users to view the contact details of the contacts in the user's personal directory stored on the server. You must enable this feature to enable users to add, delete, or edit the contacts in the Cisco BroadWorks Personal Directory.

Enable Cisco BroadWorks Directories

Enable Cisco BroadWorks directories on Poly phones to enable users to search and view their personal, group, or enterprise contacts.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

1. Open the configuration file.
2. Enable the Cisco BroadWorks Enterprise and Enterprise Common Directories.

```
feature.broadsoftdir.enabled="1"
```

3. Enable the Group and Group Common Directories.

```
feature.broadsoftGroupDir.enabled="1"
```

4. Enable the Personal Directory and enable users to manage them on the phone's local interface.

```
feature.broadsoftPersonalDir.enabled="1"
```

5. Save the configuration file.

Configure the UC-One directory

For the Cisco BroadWorks R20 server or later, configure the UC-One phone directory.

Before configuring this feature, authenticate your Poly phones with the Cisco BroadWorks XSP service interface. For more information, see .Authentication with CISCO BroadWorks XSP Service Interface.

1. Open the configuration file.
2. Prevent the phone from using the Cisco BroadWorks XSP credentials.

```
dir.broadsoft.useXspCredentials="0"
```

3. Enter the SIP credentials to retrieve the UC-One directory.

```
dir.broadsoft.regMap="<SIP credentials>"
```

4. Save the configuration file.

Enable the Default Search View for the Enterprise Directory

Enable users to view an initial list of contacts before entering a name in the search field of the directory.

1. Open the configuration file.
2. Enable the phone to display an initial list of contacts for an empty search field.

```
feature.broadsoftdir.showDefaultSearch="1"
```

3. Save the configuration file.

UC-One Call Control Features

Poly phones support UC-One calling and management features that you can configure on the phones.

Poly phones support the following UC-One features:

- Anonymous call rejection
- Simultaneous ring
- Line ID blocking
- BroadWorks Anywhere
- Remote office

Enable UC-One on Poly Phones

Enable UC-One to enable users to use Cisco BroadWorks features, such as BroadWorks Anywhere, on their Poly phone.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable the UC-One feature.

```
feature.broadsoftUcOne.enabled="1"
```

3. Save the configuration file.

Enable Users to Log In Using UC-One Credentials

Enable users to log in to Poly phones using their UC-One credentials.

Before you configure this feature, see Enable UC-One on Poly Phones.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable users to enter their BroadWorks XSP credentials on the phone.

```
reg.x.broadsoft.useXspCredentials="1"
```

3. Save the configuration file.

Enable anonymous call rejection

Enable users to automatically reject incoming calls from anonymous parties with restricted caller identification.

Before you configure this feature, see Enable UC-One on Poly Phones.

1. Open the configuration file.
2. Enable the **Anonymous Call Rejection** menu to display on the phone.

```
feature.broadsoft.xsi.AnonymousCallReject.enabled="1"
```

3. Save the configuration file.

Enable simultaneous ring

Enable users to add phone numbers to a list of contacts whose phones ring simultaneously when they receive an incoming call. Users can turn the feature on or off from the phone and define which numbers to include in the simultaneous ring group.

Before you configure this feature, see Enable UC-One on Poly Phones.

1. Open the configuration file.
2. Configure the **Simultaneous Ring** menu to display on the phone menu.

```
feature.broadsoft.xsi.SimultaneousRing.enabled="1"
```

3. Save the configuration file.

Enable line ID blocking

Enable users to conceal their phone number when making calls.

Before you configure this feature, see Enable UC-One on Poly Phones.

1. Open the configuration file.
2. Configure the **Line ID Blocking** menu to display on the phone.

```
feature.broadsoft.xsi.LineIdblock.enabled="1"
```

3. Save the configuration file.

Enable Remote Office

Enable users to set up a phone number on their office phone to forward incoming calls to a mobile device or home office number. Calls placed from the other phone display the office phone number on the far end.

Before you configure this feature, see Enable UC-One on Poly Phones.

1. Open the configuration file.
2. Configure the **Remote Office** menu to display on the phone.

```
feature.broadsoft.xsi.RemoteOffice.enabled="1"
```

3. Save the configuration file.

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.

Enable BroadWorks anywhere

Enable users to use one phone number on multiple phones, such as their desk phone, mobile phone, and home office phone. Users can then turn the feature on or off and add BroadWorks Anywhere locations, which enable users to move calls between phones and perform phone functions from any phone.

Before you configure this feature, see Enable UC-One on Poly Phones.

1. Open the configuration file.
2. Configure the **BroadWorks Anywhere** menu to display on the phone.

```
feature.broadsoft.xsi.BroadWorksAnywhere.enabled="1"
```

3. Save the configuration file.

Create an EFK for BroadWorks Anywhere

Configure an enhanced feature key (EFK) for the BroadWorks Anywhere feature that enables users to navigate directly to the feature menu using a softkey.

For more information, see Enhanced Feature Keys on page 209.

1. Open the configuration file.
2. Enable the enhanced feature keys feature.

```
feature.enhancedFeatureKeys.enabled="1"
```

3. Enter the name for the EFK.

```
efk.efklist.x.mname="<string>"
```

4. Enable EFK as a softkey.

```
efk.efklist.x.status="1"
```

5. Define `BroadWorks Anywhere` as the action for the key.

```
efk.efklist.1.action.string="$FBWSAnyWhere$"
```

6. Save the configuration file.

Hide the UC-One Settings icon on the Home screen

Disable the **UC-One Settings** icon on the phone's *Home* screen to prevent unauthorized access to the settings.

1. Open the configuration file.
2. Hide the **UC-One Settings** icon on the *Home* screen.

```
homeScreen.UCOne.enable="0"
```

3. Save the configuration file.

BroadWorks Call Decline

By default, users can't reject calls to a shared line on Poly phones. The BroadWorks call decline feature enables a user to reject a call to a shared line, which rejects it on all phones registered with the same shared line.

Enable the Reject Softkey for Shared Lines

Enable the **Reject** softkey to enable users to reject calls to a shared line in a Cisco BroadWorks environment.

When enabled, a user can reject an incoming call on the shared line and prevent the call from ringing on all phones registered with the shared line.

1. Open the configuration file.
2. Enable the **Reject** softkey to display on the phone.

```
call.shared.reject="1"
```

3. Save the configuration file.

Flexible Seating

Flexible seating enables a user with an assigned primary phone to access a registered line as a guest on an alternate host phone.

The user's primary registration is simultaneously active on the primary and host phones. Users can access the UC-One contact directory and favorites on the host phone, but not the Poly contact directory and favorites.

NOTE: Flexible seating is different from hoteling because it provides only the primary registration's label on the host phone without synchronizing features or settings.

Feature Conditions with Flexible Seating

There are some conditions that apply to the primary and host phones when you enable flexible seating.

The following conditions apply to phones with flexible seating:

- The primary phone and host phone don't sync automatically, but you can manually sync the phones on the BroadWorks server.
- The phone configured for the host user can't accept incoming calls.
- The host user can make only emergency outgoing calls that are defined by the BroadWorks server.
- If you enable the phone lock feature, numbers defined in the authorized call list aren't allowed to make outgoing calls except for the emergency numbers set on the BroadWorks server.
- The host user account is a placeholder account that supports guest users and isn't intended to be assigned to an actual phone user.
- The guest user can't change the user password when you enable flexible seating on the phone. You can change the host phone's user password from the system web interface at any time. You can change the host phone's user password from the phone screen only when the guest user isn't logged in.
- On the BroadWorks server, you can set a period of time when the server automatically logs a user out from a phone in case a user doesn't log out.

Flexible Seating Feature Limitations

When you enable flexible seating, there are some limitations that prevent you from configuring other features on the phone.

Flexible seating isn't compatible with the following features:

- Hoteling
- Visitor desk phone (VDP)
- User profile
- Local call forwarding
- Local do not disturb

Configure Flexible Seating

Before you configure a host phone to support the primary phone's line registration, you must configure a host user profile, a guest user profile, and a guest profile PIN on the Cisco BroadWorks server.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Specify the phone line on the host phone that hosts the guest line.

```
hoteling.reg="<line key value>"
```

3. Enable flexible seating on the phone and put it into a state where a guest isn't logged in.

```
hotelingMode.type="2"
```

NOTE: This parameter overrides `voIpProt.SIP.specialEvent.checkSync.downloadDirectory`.

4. Save the configuration file.

After you configure flexible seating on the Poly phones, map these parameters to the corresponding BroadWorks configuration tags on the Cisco BroadWorks server. See BroadWorks Configuration Tags for Flexible Seating.

BroadWorks Configuration Tags for Flexible Seating

To use flexible seating on Poly phones, you must map the Poly parameters to the corresponding configuration tags on the Cisco BroadWorks server.

The following table includes the Poly parameters and corresponding BroadWorks tags.

Table 17-1 Broadworks Tags for Flexible Seating

Poly Configuration Parameter	BroadWorks Tag
`hoteling.reg`	`%BWHOTELINGLINE-x%`
`hotelingMode.type`	`%BWHOTELINGMODE-x%`

Executive and Assistant Lines

The BroadWorks Executive-Assistant feature enables you to assign lines as an executive or an assistant on lines registered with the Cisco BroadWorks R20 or later server.

Configure a Phone for Executive or Assistant Lines

Enable the BroadWorks Executive-Assistant feature and designate registered lines as an executive or an assistant line.

Before configuring this feature, authenticate your Poly phones with the Cisco BroadWorks XSP service interface. For more information, see .Authentication with CISCO BroadWorks XSP Service Interface. Also enable the Executive Service for private and shared executive lines and the Executive-Assistant Service for private and shared assistant lines in the BroadWorks web portal.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable the Executive-Assistant feature.

```
feature.BSExecutiveAssistant.enabled="1"
```

3. Designate the registered line assigned to the executive or assistant.

```
feature.BSExecutiveAssistant.regIndex="line registration index"
```

4. Assign the executive or assistant role to each registered line. Phones default to the executive role.

```
feature.BSExecutiveAssistant.userRole="<role>"
```

Supported parameter values:

- `ExecutiveRole`
- `AssistantRole`

5. Save the configuration file.

Depending on the role you assign the user, the **Executive** or **Assistant** icon displays on the *Home* screen of the phone.

Disable the Pick Call and Barge-in Softkeys

By default, the **Pick Call** and **Barge-in** softkeys display on phones assigned as Executives and Assistants. Disable the softkeys if you don't want them to display on the phones.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Disable the softkeys for lines assigned as Assistant.

```
feature.BSExecutiveAssistant.SimplifiedAssistant.enabled="1"
```

3. Disable the softkeys for lines assigned as Executive.

```
feature.BSExecutiveAssistant.SimplifiedExec.enabled="1"
```

4. Save the configuration file.

Create EFKs for the Executive and Assistant Menus

Create enhanced feature keys (EFK) to enable users to quickly access the *Overview Executives* menu for assistants or the *Executive Settings* menu for executives from a line or softkey.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

For more information, see Enhanced Feature Keys on page 209.

1. Open the configuration file.
2. Enable the enhanced feature keys feature.

```
feature.enhancedFeatureKeys.enabled="1"
```

3. Enter the name for the EFK.

```
efk.efklist.1.mname="<string>"
```

4. Do one of the following:

   - Enable the EFK as a softkey.

     ```
     efk.efklist.<x>.status="1"
     ```

   - Enable the EFK as a line key.

     ```
     feature.EFKLineKey.enabled="1"
     ```

5. Define the action for the key.

   ```
   efk.efklist.1.action.string="<macro>"
   ```

   Executive-Assistant macros:

   - `$FAssistantMenu$`
   - `$FExecutiveMenu$`

6. Save the configuration file.

Enhanced Call Park

Configure Cisco BroadWorks enhanced call park per registered line, set the retrieval star code, and enable audio notifications for parked calls..

Configure Enhanced Call Park

Enhanced call park enables softkeys on the phone to park a call and retrieve a parked call in a Cisco BroadWorks environment.

Before configuring this feature, authenticate your Poly phones with the Cisco BroadWorks XSP service interface. For more information, see .Authentication with CISCO BroadWorks XSP Service Interface.

1. Open the configuration file.
2. Enable BroadWorks enhanced call park on a registered or shared line. Replace *x* with the registered line number.

   ```
   reg.x.enhancedCallPark.enabled="1"
   ```

3. **Optional:** If you're configuring a shared line, enter the line extension. Replace *x* with the registered line number.

   ```
   reg.x.lineAddress="<extension>"
   ```

4. Save the configuration file.

Default Retrieval Star Code

The default star code for Enhanced Call Park is set to *88.

See Configure Retrieval Star Code for Parked Calls on page 269 to change the star code.

Configure Retrieval Star Code for Parked Calls

Configure the star code that users can enter retrieve parked calls.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enter the star code used for retrieving parked calls.

```
call.parkedCallRetrieveString="<star code>"
```

3. Save the configuration file.

Enable Audio Notifications for Parked Calls

Configure Poly phones to play an audio notification for calls parked on a shared or private line.

Don't configure the call park notification for monitored BLF lines.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable call park audio notifications.

```
feature.enhancedCallPark.allowAudioNotification="1"
```

3. Save the configuration file.

Enable Cisco BroadWorks Server-Based Call Features

Configure Poly phones to use server-based call features, such as call waiting, redial, and call lists in place of the phone's default features.

1. Open the configuration file.
2. Enable users to view call logs retrieved from the BroadWorks server.

```
feature.broadsoft.callLogs="1"
```

3. Display the **Redial** softkey and enable users to redial the last dialed number.

```
feature.broadsoft.basicCallLogs.redial.enabled="1"
```

4. Enable the BroadWorks server to manage incoming calls and call waiting for the phone.

```
feature.broadsoft.xsi.callWaiting.enabled="1"
```

5. Save the configuration file.

Enable Cisco BroadWorks Server-Based Call Forwarding

Enable Cisco BroadWorks server-based call forwarding on a Poly registered phone. If you enable server-based call forwarding on one registration, other registrations aren't 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.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable server-based call forwarding.

```
reg.x.serverFeatureControl.cf="1"
```

3. Save the configuration file.

Hoteling

The hoteling feature enables users to use any available shared phone by logging in to a guest profile. After logging in, users can access their own guest profiles and settings on the shared phone.

Limitations with Hoteling and Feature-Synchronized ACD

You can't use hoteling in conjunction with the feature-synchronized ACD feature, and you must disable all ACD parameters to use the hoteling feature.

If you enable both features at the same time, ACD takes precedence. The hoteling **GuestIn** and **GuestOut** softkeys don't display.

Enable and Configure Hoteling

Enable hoteling to enable users to log in to a guest profile on any available shared phone in the Cisco BroadWorks environment.

NOTE: For additional details on configuring the hoteling feature, see *Using Hoteling on Poly Phones (FP 76554)* at Poly Engineering Advisories and Technical Notifications.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable hoteling, and configure the hoteling line key value.

```
feature.hoteling.enabled="1"
hoteling.reg="<line key value>"
```

3. Save the configuration file.

The **Guest In** softkey displays for users to log in to the phone. After logging in, users have access to their own guest profile and settings on the shared phone.

Feature-Synchronized ACD

Feature-synchronized automatic call distribution (ACD) assists organizations in handling a large number of incoming phone calls to a call center with users in agent and supervisor roles. Feature-synchronized ACD is distinct from and provides more advanced ACD functions than the hoteling feature.

Feature-Synchronized ACD Services

Feature-synchronized ACD is available in standard and premium services.

- **Standard**: Standard service enables call center agents to sign in to a shared phone. After agents sign in, the phone displays their availability to take new calls.
- **Premium**: Premium service offers two additional features to the Standard service: hoteling and queue status notification.
  - Hoteling enables agents to use their agent credentials to log in to any available phone.
  - Queue status notification enables agents to view the queue status of a call center so that agents can adjust their call response.

For more information on standard and premium services as well as the hoteling and queue status notification enhancements, see *Feature Profile 76179: Using Premium Automatic Call Distribution for Call Centers - Hoteling and Queue Status* at Poly Support.

Enable Feature-Synchronized ACD

Feature-synchronized ACD helps organizations handle a large number of incoming phone calls, such as a call center with users in agent and supervisor roles.

1. Open the configuration file.
2. Enable feature-synchronized ACD on the phone.

```
feature.acdAgentAvailable.enabled="1"
```

3. Enable the ability for agents to log in and out of their phones.

```
feature.acdLoginLogout.enabled="1"
```

4. **Optional:** If you have the Premium service, enable the Premium Unavailability feature.

```
feature.acdPremiumUnavailability.enabled="1"
```

5. Enable the phone to display the **Trace**, **Emergency**, and **Disp Code** softkeys.

```
feature.acdServiceControlUri.enabled="1"
feature.enhancedFeatureKeys.enabled="1"
```

6. Save the configuration file.

SIP Call Server for Feature-Synchronized ACD

The capabilities of feature-synchronized ACD vary with the SIP call server. Consult your call server provider for information and for documentation.

You can find information on the SIP signaling used for this implementation in the Cisco BroadWorks document *Device Key Synchronization Requirements Document*, Release R14 SP2; version 1.6.

Centralized Call Recording

Centralized call recording enables users to record audio and video calls and control call recording directly from phones registered with Cisco BroadWorks R20 server.

Users can manage recorded audio and video files on a third-party call recording server connected to their BroadWorks server account.

Centralized Recording or Local Call Recording

You can record calls using centralized recording or local call recording. You can't use both at the same time. By default, both features are disabled, so if you enable one call recording feature, make sure to disable the other feature.

Call Recording Alerts

By default, far-side participants don't receive an alert when the near side records a call. However, administrators can enable an announcement on the BroadWorks R20 server, which sounds at the beginning of a call when a recording begins.

Enable Centralized Call Recording

Enable phones to support Cisco BroadWorks centralized call recording.

You must also enable this feature on the Cisco BroadWorks R20 server.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable centralized call recording on the phone.

```
voIpProt.SIP.serverFeatureControl.callRecording="1"
```

3. Save the configuration file.

Block Call Recording on a Registered Line

Prevent users from using centralized call recording on specific registered lines.

1. Open the configuration file.
2. Specify the lines that you want to block centralized call recording on. Replace *x* with the desired line key value.

```
reg.x.serverFeatureControl.callRecording="0"
```

3. Save the configuration file.

Call Recording Modes

The Cisco BroadWorks R20 server has call recording modes that users can use to control call recording options on Poly phones.

The following table includes call recording modes are available on the BroadWorks server.

Table 17-2 **Centralized Call Recording Modes**

Mode	Description
Never Mode	Call recording never initiates, and the phone never displays call recording softkeys.
Always Mode	The server records all incoming and outgoing calls without user initiation. Users have no call recording control options. During active calls, the phone display indicates the status of the call recording state. Call recording stops when the call ends, and the server stores the recording.
Always with Pause/Resume Support Mode	Call recording starts automatically when the call connects, and the **Pause** and **Resume** softkeys display on the phone. The phone display indicates the status of the call recording state. Call recording stops when the call ends, and the server stores the recording.
On Demand Mode	Call recording starts on the server when the call connects, but the recorded file saves only if the user initiates the recording. When the user presses the **Start** softkey, the recording saves to the server, and the phone displays the **Pause** and **Resume** softkeys.
On Demand Mode with User-Initiated Start Mode	Call recording doesn't begin automatically, and the **Record** softkey displays on the phone. If users want to record an active call, they must select **Record** > **Start** to start recording and save it to the server. While recording, the phone displays the **Pause**, **Resume**, and **Stop** softkeys.
Recording two separate calls and creating a conference	This mode enables users to record two participants as separate call sessions when connected in a conference call. The server stores the conference call as two separate recording sessions.

Visual Security Classification for Cisco BroadWorks Calls

Poly phones registered with the Cisco BroadWorks R20 server or later support visual security classifications for SIP calls.

When you enable this feature, a visual security classification notification displays during a call to make participants aware of the maximum level of classified information they can safely exchange in a conversation. The participant with the lowest security classification determines the security classification for a call.

Users can choose to override a call's security classification and assign a lower security classification level, but they can't raise it higher than the default setting. The classification level resets after the call ends.

Enable phones to display the security classification

Enable phones registered with the Cisco BroadWorks R20 server or later to display the security classifications for all lines or for specific phone lines.

Before enabling this feature, enable security classification, set the priority for each classification, and set the default security classification level on the Cisco BroadWorks server. The default security classification **Unclassified** displays on the phone until you set the classifications on the server.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

1. Open the configuration file.
2. Enable visual security classifications.
   - For all lines:

     ```
     voIpProt.SIP.serverFeatureControl.securityClassification="1"
     ```

   - For specific lines: Replace *x* with the registered line number.:

     ```
     reg.x.serverFeatureControl.securityClassification="1"
     ```

3. Save the configuration file.

Configure Key System Emulation

Key system emulation (KSE) enables one-touch call park and call retrieve from any phone within the user group.

You must enable busy lamp field (BLF) and enhanced call park features on the phone for KSE to work seamlessly.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

BLF and KSE are mutually exclusive. If you enable KSE, BLF is no longer available to monitor calls.

Key system emulation includes the following behavior:

- An audio notification plays on the phones in the user group when someone parks a call.
- A reminder tone continuously plays after a designated time interval if no one answers the call.
- There are no audio and reminder notifications for a self-parked call.
- The LED patterns and the line icons for a self-parked call are different from a call parked by other users in the group. This helps to differentiate between a self-parked call and a remote-parked call.
- The LED indicator turns solid red for a self-parked call and turns blinking red for a remote-parked call.

NOTE: Key system emulation is applicable to only the Cisco BroadWorks call control platform.

1. Open the configuration file.
2. Enable KSE.

   ```
   attendant.keylineEmulation.enabled="1"
   ```

3. Enter the address for the registered line. Replace *x* with the desired line key value.

   ```
   reg.x.address="<line registration>"
   ```

4. Enter the address for the SIP server accepting registrations. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

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

5. Enter the SIP URI for your attendant call server.

```
attendant.uri="<attendant SIP URI>"
```

6. Specify the line registration to use to subscribe to the BLF resource list.. Permitted values for the line registration index are 1 to 34. The default index is `1`.

```
attendant.reg="<index number>"
```

7. Set the call action behavior for an active call to `Park`.

```
attendant.CallAction="Park"
```

8. Set the call action behavior for an active call to `Park`.

```
attendant.CallAction="Park"
```

9. **Optional:** Enable the phone to display **Attendant Call Action** on the phone when you configure dynamic BLF on the phone.

   Setting this parameter adds a menu item in the **Basic** > **Preferences** menu to allow the user to select the behavior when selecting an attendant line key.

```
attendant.callActionMenu.enabled="1"
```

10. Enable an audible call park notification for BLF-monitored lines.

```
feature.enhancedCallPark.allowBLFAudioNotification="1"
```

11. Configure a delay, in seconds, before the first call park notification plays, and then the delay, in seconds, that subsequent notifications play.

```
attendant.callParkBLFReminder.StartDelay="<delay in seconds>"
attendant.callParkBLFReminder.RepeatTime="<delay in seconds>"
```

12. **Optional:** Configure the call park notification ringtone. Replace *x* with the appropriate tone instruction step index.

    The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFReminderTone.inst.1.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.1.value="cs3"
se.pat.misc.callParkBLFReminderTone.inst.2.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.2.value="cs4"
se.pat.misc.callParkBLFReminderTone.inst.3.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.3.value="cs6"
se.pat.misc.callParkBLFReminderTone.inst.4.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.4.value="cs4"
```

13. **Optional:** Configure the call park notification ringtone. Replace *x* with the appropriate tone instruction step index.

    The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFAudioNotification.inst.1.type="chord"
se.pat.misc.callParkBLFAudioNotification.inst.1.value="cs7"
se.pat.misc.callParkBLFAudioNotification.inst.2.type="chord"
se.pat.misc.callParkBLFAudioNotification.inst.2.value="cs4"
se.pat.misc.callParkBLFAudioNotification.inst.3.type="chord"
se.pat.misc.callParkBLFAudioNotification.inst.3.value="cs7"
```

14. Save the configuration file.

Ribbon Communications Server

Ribbon Communications application server, also called EXPERiUS™ A2, provides full-featured, IP-based multimedia communications applications for businesses and consumers.

You can deploy EXPERiUS A2 as a standalone server or in combination with a Ribbon Communications CONTiNUUM™ C20 server; features vary depending on your deployment.

Features Available with Ribbon Communications

The following features are available for phones registered with the Ribbon Communications servers:

- MADN-SCA—A shared group feature that provides support for conference barge in, privacy, and remote call appearance. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 server.
- Global Address Book—The global address book (GAB) feature is a corporate directory application managed by the Ribbon Communications server.
- Personal Address Book—The personal address book (PAB) feature is managed by the Ribbon Communications server and allows multiple clients (phones, computer software) to read and modify a user's personal directory of contacts. When one client changes a contact all other clients are immediately notified of the change by the Ribbon Communications server.
- E.911—Enhanced 911 services specific to Ribbon Communications C20 server implementation.

Multiple Appearance Directory Number - Single Call Appearance (MADN-SCA)

Multiple appearance directory number—single call appearance (MADN-SCA) enables a group of users to share a single directory number that displays as a single line to each member of the group.

When this feature is enabled, users can initiate or receive calls on this shared line. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 server.

Only one call can be active on the line at a time on the MADN-SCA shared line. When a call is in progress, any incoming calls to the line receive a busy tone.

MADN-SCA Parameters

The following list includes all parameters available for configuring MADN-SCA and feature options.

NOTE: If you configure the line-specific parameter `reg.x.server.y.address` , you must also configure values in the line-specific parameter `reg.x.server.y.specialInterop` .

If you configure the global parameter `voIpProt.server.x.address` , you must also configure values in the global parameter `voIpProt.server.x.specialInterop` .

For all deployments, including Ribbon Communications, line-specific configuration parameters override global configuration parameters. If you set values in both line-specific and global parameters, line-specific parameters are applied and global parameters are not applied.

`reg.x.address`
The user part (for example, 1002) or the user and the host part (for example, `1002@polycom.com`) of the registration SIP URI.
Null (default)

string address

reg.x.server.y.specialInterop
Specify the server-specific feature set for the line registration.
Standard (Default)

GENBAND

ALU-CTS

ocs2007r2

lcs2005

voIpProt.server.x.specialInterop
Enables server-specific features for all registrations.
Standard (default)

All other phones = Standard, GENBAND, GENBAND-A2, ALU-CTS, DT, ocs2007r2, lcs2005

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.bargeInEnabled
0 (default) - barge-in is disabled for line x.
1 - barge-in is enabled (remote users of shared call appearances can interrupt or barge in to active calls).

reg.x.callsPerLineKey
Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration.
This per-registration parameter overrides `call.callsPerLineKey` .

24 (default)

1-24

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.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.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.auth.domain
The domain of the authorization server that is used to check the user names and passwords.

Null (default)string

`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).

Configuring Privacy on a MADN-SCA Line

In the UC Software download, Poly provides the following two sample enhanced feature key (EFK) macros that you can configure to display on the phone to change privacy states: `privacyReleaseRestoreESK.cfg` and `privacyEnableESK.cfg` .

When you set the line to shared, an incoming call alerts all the members of the group simultaneously, and the call can be answered by any group member. On the server, you can configure a privacy setting that determines whether or not, after the call is answered, other members of the group can barge in to the same call and whether or not a call on hold can be picked up by other members of the group.

Optionally, you can configure star codes on the server that you can dial on the phone to toggle the privacy setting during a single active call. Note the following call behavior. If the line is configured for privacy by default, you can use a star code to toggle privacy on and off during an active call. When the call ends, the line resets to privacy settings. If the line is configured on the server with privacy off, you can use a star code to toggle to privacy on during an active call but you cannot toggle back to privacy off during the call. When the call ends, the line resets to privacy off.

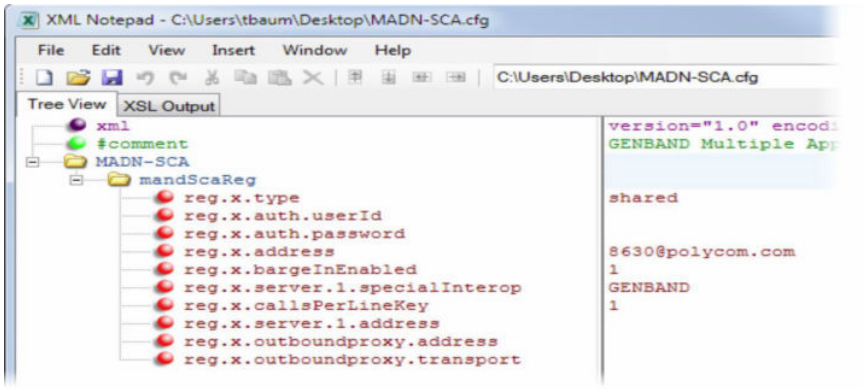
Example MADN-SCA Configuration

The following example configuration shows the minimum configuration you need to enable MADN-SCA on the phone.

Use the parameters illustrated in the example below.

1. Enter values for the following parameters in a configuration file and save.

   The value `8630@polycom.com` is an example registration address.



2. Enter the name of the configuration file to the CONFIG_FILES field of the primary configuration file and save.

Global Address Book (GAB)

Ribbon Communications global address book (GAB) is a read-only global directory set up by an administrator and can co-exist with other corporate directories on the phone.

Global Address Book Parameters

Use the parameters in the following list to configure this feature.

feature.corporateDirectory.alt.enabled
0 (default) - Disables the global address book service.
1 - Enables the global address book service.

dir.corp.alt.address
Enter the URL address of the GAB service provided by the server.
Null (default)

Hostname

FQDN

dir.corp.alt.port
Set the port that connects to the server if a full URL is not provided.
0 (default)

Null

1 to 65535

dir.corp.alt.user
Enter the user name used to authenticate to the Ribbon Communications server.
Null (default)

UTF-8 encoding string

dir.corp.alt.viewPersistence
Determine if the results from the last address directory search displays on the phone.
0 (default) - Disabled

1 - Enabled

dir.corp.alt.attribute.x.filter
Enter a filter to use to set a predefined search string through configuration files.
Null (default)

UTF-8 encoding string

dir.corp.alt.attribute.x.sticky
0 (default) – the filter string criteria for attribute x is reset after a reboot.
1 – the filter string criteria is retained through a 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.

dir.corp.alt.attribute.x.label
Enter a label to identify a user.
Null (default)

UTF-8 encoding string

dir.corp.alt.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

`dir.corp.alt.attribute.x.type`
Define how x is interpreted by the phone. Entries can have multiple parameters of the same type.
first_name

last_name (default)

phone_number

SIP_address

Other – for display purposes only.

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.

`dir.local.serverFeatureControl.method`
Specifies a method for synchronizing the directory and server.
None (default)

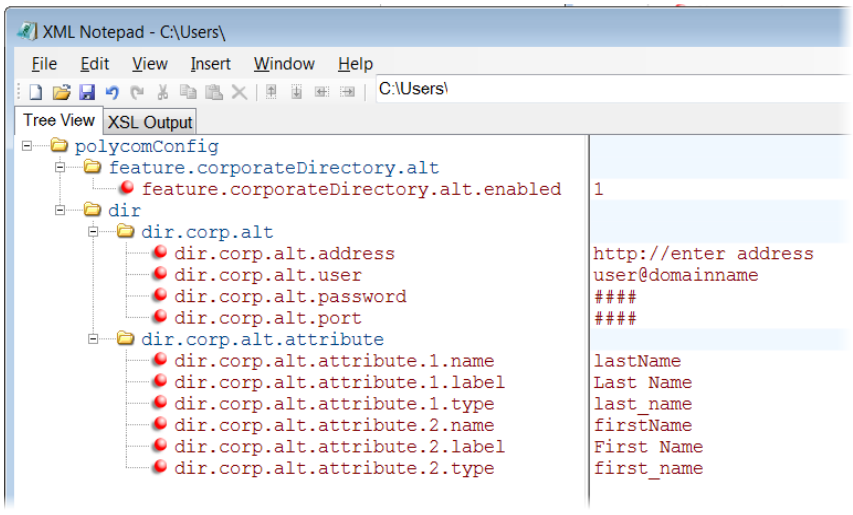
GENBANDSOPI - Enables the GENBANDSOPI protocol on the phone to get the personnel address book service from the Ribbon Communications server.

Example GAB Configuration

The following example shows the minimum parameters you need to configure to enable GAB on the phone.

1. Enable GAB by configuring the values in `feature.corporateDirectory.alt` and `dir.corp.alt` .

   The following illustration includes an example GAB address book parameters in `dir.corp.alt.attribute` .



2. Save the configuration file.

3. Enter the name of the configuration file to the CONFIG_FILES field of the primary configuration file and save.

Personal Address Book (PAB)

The personal address book (PAB) enables users to read and modify a personal directory of contacts on their phone.

When users modify contact information using any soft client, desk phone, or mobile client registered to the same line, the change is made on all other clients, and users are notified immediately of the change by the Ribbon Communications server.

Personal Address Book Parameters

Use the parameters in the following list to configure this feature.

Note that when you enable server control, five telephone number fields per contact are available.

`feature.corporateDirectory.alt.enabled`
0 (default) - Disables the global address book service.
1 - Enables the global address book service.

`dir.local.serverFeatureControl.method`
Specifies a method for synchronizing the directory and server.
None (default)

GENBANDSOPI - Enables the GENBANDSOPI protocol on the phone to get the personnel address book service from the Ribbon Communications server.

`dir.local.serverFeatureControl.reg`
Specifies the phone line to enable the personal address book feature on.
1 (default)

1 -34

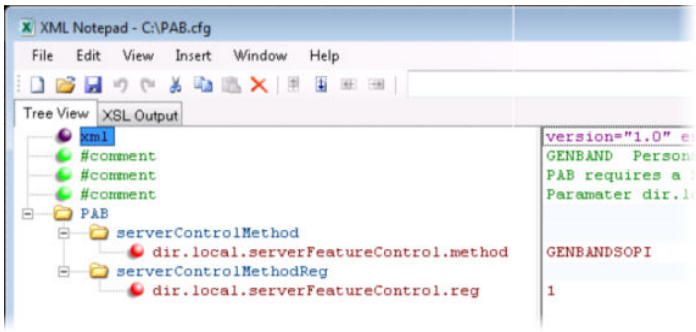
`dir.genband.local.contacts.maxSize`
Specify the maximum number of contacts available in the Ribbon Communications personnel address book contact directory.
100 (default)

1 - 100

Example Personal Address Book Configuration

The following example shows an example PAB configuration.

1. Enter the values shown for the following parameters and save the configuration file.



2. Enter the configuration file to the CONFIG_FILES field of the primary configuration file and save.

Enhanced 911 (E.911) Location for Ribbon Communications

The Enhanced 911 (E.911) feature enables you to set the location of the phone for emergency calls on the phone or on the provisioning server.

With the Enhanced 911 (E.911) feature, you can set the location of the phone for emergency calls on the phone or on the provisioning server. When the phone starts up, the phone prompts users to choose a location, which is stored on the phone. The location that users set for the phone is used to identify the phone location to 911 operators dispatching emergency services. This feature is available for all phones and is disabled by default only in a Ribbon Communications environment.

By default, users can make a 911 call when the phone is locked, regardless of the call state, or when other features are in use. When a 911 call is in progress, the call control option does not display, users cannot use the hard keys to control a call, and DND or call forwarding are disabled.

Enhanced 911 (E.911) Location Parameters for Ribbon Communications

Use the parameter below to configure this feature.

`feature.genband.E911.enabled`
0 (default) - Disable the Ribbon Communications E.911 feature.
1 - Enable the Ribbon Communications E.911 feature.

Change causes system to restart or reboot.

Manually Set the Phone's Location

Users can set their location for emergency calls on the phone.

1. Register the phone.
2. The phone displays a warning message to set your location for 10 seconds.
3. Press the warning message to enter a location.

   If the warning message disappears, on the phone, go to **Settings** > **Status** > **Diagnostics** > **Warnings**.
4. Select **Details** to enter a location to the location tree navigation menu.
5. Choose a location and press **Save**.

6. On the phone, go to **Status** > **Location Information**.

   The location information displays in the Status menu.

Emergency Instant Messages

Configure audio alerts for incoming instant messages and set the duration of time that emergency messages display.

Emergency Instant Message Parameters

Use the following parameters to configure emergency messages on phones registered with Ribbon Communications.

`feature.instantMessaging.displayTimeout`
Specify the time in minutes instant messages display.

Messages display until one of the following occurs:

- Timeout
- Another instant message is received
- A pop-up message displays
- The phone receives an incoming call
- The user presses any key or message on the phone

1 minute (default)

1 - 60 minutes

`feature.instantMessaging.ring`
instantMessage (default) - The phone plays a configured tone when an emergency instant message is received.
Silent - No tone is played.

`feature.instantMessaging.enabled`
0 (default) - The phone does not display emergency instant messages.
1 - Received emergency instant messages display on the phone.

Enable Server-Specific Features

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

The phone supports the following features:

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

1. Open the configuration file.

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

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

3. Save the configuration file.

18 Diagnostics and Status

Poly phones include diagnostic tools to check that they are running properly.

Network Ping

Use the ping feature to return a network diagnostics report for network issue troubleshooting.

Send a ping using the local interface or system web interface. Pinging a network using the system web interface enables you to adjust aspects of the ping to gather more information, but it relies on the network connection between a computer and the phone.

The returned network ping report gathers the following information:

- Network connectivity
- Server reachability
- Latency
- Lost packets
- Bandwidth
- Frame size

Ping a Network Address from the Local Interface

Ping a network address to test connectivity using the phone's local interface.

1. Select **Settings** > **Diagnostics** > **Network**.
2. Select **Ping**.
3. Enter the network address that you want to ping and test connectivity for.
4. Select **Send**.

   The phone sends a ping to the network address and returns a network diagnostics report.

Ping a Network Address from the System Web Interface

Ping a network address to test connectivity from the phone's system web interface. The ping returns the network connectivity, server reachability, lost packets, bandwidth, and frame size.

1. In the system web interface, go to **Diagnostics** > **Ping & Traceroute**.
2. Select **Ping**.
3. Enter the **IP/Hostname** for the network you want to test.
4. **Optional:** In the **Options** field, configure the packet count and packet size, in bytes, the test sends to the network.

   NOTE: If you don't enter a value for packet count and packet size, the phone sends the default values.

   - Send between 1 and 30 packets. The default value is `3` packets.
   - The packets can be 1 to 65507 bytes. The default packet size is `56` bytes.

```
-c<packet count>
 -s<packet size>
```

For example, `-c15 -s64` sends 15 packets of 64 bytes to the network.

5. Select **Run Test.**

Traceroute

A traceroute test shows you the network path to key servers. Send a traceroute using the local interface or system web interface.

Send a Traceroute from the Local Interface

Use the phone's local interface to send a traceroute. The phone displays the path report onscreen.

1. Select **Settings** > **Diagnostics** > **Network**.
2. Select **Network Tools**.
3. Select **Traceroute**.
4. Enter the network address for the route you want to trace.
5. Select **Send**.

   The phone sends a traceroute command to the network and returns a network path report.

Send a Traceroute from the System Web Interface

Use the system web interface to execute a traceroute test. The test returns the network key paths to servers.

1. In the system web interface, go to **Diagnostics** > **Ping & Traceroute**.
2. In the system web interface, go to **Diagnostics** > **Network** > **Ping Test & Traceroute**.
3. Select **Traceroute**.
4. Enter the **IP/Hostname** for the network you want to test.
5. **Optional:** In the **Options** field, configure the maximum number of hops the test can take to search for the destination and the amount of time, in seconds, the test waits for a response.

   NOTE: If you don't enter a value for maximum hops and wait timeout, the phone sends the default values instead.

   - The available values are 1 to 30 hops. The phone allows up to `30` hops by default.
   - The available values are 2 to 60 seconds. The phone waits `2` seconds by default.

   ```
   -h<maximum hops count> -w<wait timeout>
   ```

   For example, `-h15 -w4` allows for 15 hops during the test over 4 seconds in the network path to search for the destination.
6. Select **Run Test**.

DNS Testing

Use this tool to check if the configured DNS can resolve addresses to key servers.

The DNS test page displays information for the following parameters:

- DNS server
- DNS secondary server
- DNS domain
- DNS address override DHCP
- DNS domain override DHCP

Configure a Test DNS Server Account

Create a test account for your phone to query.

1. Open the configuration file.
2. Configure query A records 1. The default is `Null`. The maximum string length is 255 characters.

```
diags.networkAssessment.DNS.A.1="<URL>"
```

3. Configure query A records 2. The default is `Null`.

```
diags.networkAssessment.DNS.A.2="<URL>"
```

4. Configure query A records 3. The default is `Null`.

```
diags.networkAssessment.DNS.A.3="<URL>"
```

5. Configure query A records 4. The default is `Null`. The maximum string length is 255 characters.

```
diags.networkAssessment.DNS.A.4="<URL>"
```

6. Configure up to four AAAA records. The default is `Null`. The maximum string length is 255 characters. Replace *n* with the desired iteration number from `1` to `4`.

```
diags.networkAssessment.DNS.AAAA.n="<URL>"
```

7. Configure up to four SRV records. The default is `Null`. The maximum string length is 255 characters. Replace *n* with the desired iteration number from `1` to `4`.

```
diags.networkAssessment.DNS.SRV.n="<URL>"
```

8. Configure up to four NAPTR records. The default is `Null`. The maximum string length is 255 characters. Replace *n* with the desired iteration number from `1` to `4`.

```
diags.networkAssessment.DNS.NAPTR.n="<URL>"
```

9. **Optional:** Add an alternate server for executing DNS questions. The default is `Null`. The maximum string length is 255 characters..

   If you leave the parameter with the default setting, the phone sends DNS queries to the current DNS primary server.

   ```
   diags.networkAssessment.DNS.testAddress="<URL>"
   ```

10. Save the configuration file.

Run a DNS Test from the System Web Interface

Use the phone's system web interface to verify if the phone can reach the configured servers on your network.

Before performing this task, complete the steps in Configure a Test DNS Server Account on page 290.

1. In the system web interface, go to **Diagnostics** > **DNS Test**.
2. Enter an IP address or a URI.
3. Select **Run**.

Display the Phone's DNS Cache

Display the phone's DNS cache to view resource records such as date, type, name, and TTL.

1. In the system web interface, go to **Diagnostics** > **DNS Test**.
2. In the section titled **Show DNS Cache**, select **Run**.

NTP Server Connection Testing

Test your connection to a defined NTP test server.

Configure an NTP Test Address

Set up a test address the phone uses to perform an NTP server test.

The test address is an alternate NTP server not provided by DHCP. Use this address to validate the DHCP provided NTP server replies against a user configured server.

1. Open the configuration file.
2. Configure the NTP test address. The default value is `ntp.polycom.com`. The maximum string length is 255 characters.

```
diags.NetworkAssessment.NTP.testAddress="<URL>"
```

3. Save the configuration file.

View NTP Server Test Information

View the information that you receive from an NTP server test. The NTP test checks if your local phone can sync to the network servers and a test address. This test also validates the NTP servers and time.

NOTE: The NTP test page shows the current NTP servers.

1. In the system web interface, go to **Diagnostics** > **NTP Test**.
2. Select **Run NTP Test**.

   The results on the NTP test page show if the NTP query is successful.

19 Troubleshooting

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

Find a Phone's Information

Access and record general information about the phone in case you need to contact technical support.

1. Go to **Menu** > **Help and Support** > **About**.
2. Record the information in a safe place.

System Logs

System log files contain information about system activities and the system configuration profile.

After you set up system logging, you can retrieve system log files.

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

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

For information on configuring system log parameters, refer to the *Poly Edge E Series Phones Parameter Reference Guide*.

Configuring Log Files

Configure how the phone creates log files.

Log file names use the following format: `[MAC address]-[Type of log].log`. For example, if the MAC address of your phone is `0004f2203b0`, the log file name is `0004f2203b0-app.log`.

The phone writes information into several different log files. The types of information in each type of log file are:

- **Application Log** – The application log file contains complete phone functionality data including SIP signaling, call controls and features, digital signal processor (DSP), and network components.
- **System Log** - The system log file contains the android logs.

Logging Levels

The event logging system supports multiple classes of events.

NOTE: Logging parameter changes can impair system operation. Don't change any logging parameters without prior consultation with Technical Support.

The phone supports two types of logging:

- Level, change, and render
- Schedule

Table 19-1 **Logging Levels**

Logging Level	Description
0	Debug only
1	High detail event class
2	Moderate detail event class
3	Low detail event class
4	Minor error
5	Major error that eventually incapacitates 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. Example: 0210281716 - 2002 October 28, 17:16
  - 2 - absolute time with seconds resolution. Example: 1028171642 - October 28, 17:16:42
- 1-5 character component identifier (such as "so")
- Event class
- Cumulative log of events missed due to excessive CPU load
- The event description

Enable Log Uploads to a USB Flash Drive

Configure your phones to copy application and boot logs to a USB flash drive connected to the phone.

You can configure the phone to copy the application logs and boot 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 and boot logs to the USB flash drive periodically using `log.render.file.upload.period` parameter.

1. Open the configuration file.
2. Enable the phone to upload logs to a connect USB flash drive.

```
feature.usbLogging.enabled="1"
```

3. Save the configuration file.

Retrieve Logs Using the System Web Interface

You can view and export log files using a phone's system web interface.

1. Log in to the system web interface as an administrator
2. Go to **Diagnostics** > **Logs**.
3. Use the tabs to adjust log settings, download the various types of log files, or view live logging.

Retrieve Logs from the Support Information Package

Export the **Support Information Package** (`.tar` file) using the system web interface.

The support information package includes the following log files:

- PBU file
- App log file
- Boot log file
- Audit log file

1. Log in to the system web interface as an administrator.

2. Go to **Diagnostics** > **Download Support Information Package** and download the support information package.
3. On your computer, unzip the `.tar` file to view the log files.

Upload a Phone's Configuration Files

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

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

1. Go to **Settings** > **Advanced** > **Admin Settings** > **Upload Configuration**.
2. Choose the files to upload:
   - **All Sources**
   - **Configuration Files**
   - **Local**
   - **Web**
   - **SIP**
   - **Cloud**

   If you select **All Sources**, the phone uploads the `<MACaddress>-upload-all.cfg` file.

   If you use the system web interface, you can also upload **Device Settings**. For more information, see Configure a Phone Through the System Web Interface on page 4.
3. Select **Upload**.

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

Test Phone Hardware

Test the phone hardware directly from the phone's local interface.

1. Go to **Settings** > **Diagnostics** > **Test Hardware**.
2. Select the option you want to test:
   - **Audio Diagnostics**: Test the speaker, microphone, handset, and a third-party headset
   - **Keypad Diagnostics**: Test the keypad response
   - **Display Diagnostics**: Test the LCD for faulty pixels
   - **Brightness Diagnostics**: Test the screen brightness
   - **LED Diagnostics**: Test the LEDs

Capturing your phone screens

Use the screen capture feature to verify whether the screen displays properly in the capture. This helps troubleshoot for display screen issues.

Capture Your Phone's Screen Through the System Web Interface

Capture your phone's current screen through the system web interface .

1. In the system web interface, go to **Diagnostics** > **Screen Capture**.
2. Select **Phone**.
3. Select **Capture**.
4. **Optional:** Select **Download** to save the image as a `.bmp` file to your local device.

Capture Your Phone's Expansion Module Screen Through the System Web Interface

Use the system web interface to capture the screen of an expansion module attached to your phone.

1. In the system web interface, go to **Diagnostics** > **Screen Capture**.
2. Select **Expansion Module**.
3. Use **Display Number** to select which expansion module and **Page Number** to select which page of the expansion module to capture.
4. Select **Capture**.
5. **Optional:** Select **Download** to save the image as a `.bmp` file to your local device.

Configure Remote Packet Capture

Configure the remote packet capture options for your phone.

IMPORTANT: Dependencies and overrides may affect other parameters. For more information, review the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide.*

The phone generates core files when errors occur by default.

1. Open the configuration file.
2. Enable all onboard packet capture features.

```
diags.pcap.enabled="1"
```

3. Enable the remote packet capture server.

```
diags.pcap.remote.enabled="1"
```

4. **Optional:** Configure the remote packet capture password. The phone's MAC address is the default password.

```
diags.pcap.remote.password="<alphanumeric password>"
```

5. **Optional:** Configure the remote packet port number. The default is port 2002.

```
diags.pcap.remote.port="<TCP port>"
```

6. Save the configuration file.

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.

Table 19-2 Updated Error Messages and Possible Solutions

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. • 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: • 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.

Table 19-2 Updated Error Messages and Possible Solutions (continued)

Error Message	Cause and Possible Solution
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. • Download compatible PVOS 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.

PVOS error messages

If an error occurs in PVOS, an error message and a warning icon display on the phone.

The following table describes possible PVOS error messages.

Table 19-3 PVOS Error Messages

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

Table 19-3 PVOS Error Messages (continued)

Error Message	Cause
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.

Table 19-4 Network Authentication Failure Error Codes

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'.	None.
30xxx	TLS Certificate failure The phone displays the following codes: • 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	Server Certificate failure 'xxx' may use the following values: • 009 - Certificate not yet Valid • 010 - Certificate Expired • 011 - Certificate Revocation List • (CRL) not yet Valid • 012 - CRL Expired	None.
4xxx	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.	See section 7.2 of RFC 2246 for further TLS alert codes and error codes.

Table 19-4 Network Authentication Failure Error Codes (continued)

Event Code	Description	Notes
5xxx	Credential failures 5xxx - wrong user name or password	None.
6xxx	PAC failures: • 080 - No PAC file found • 081 - PAC file password not provisioned • 082 - PAC file wrong password • 083 - PAC file invalid attributes	None.
7xxx	Generic failures: • 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	None.

Troubleshooting power and start-up issues

The following procedures provide tips for resolving power and start-up issues.

Power and start-up issues

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

Table 19-5 Power and Start-Up Issues

Power or Start-up Issue	Possible Solutions:
The phone has power issues or the phone has no power.	Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do the following: • 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.	If the phone doesn't boot, there may be a corrupt or invalid firmware image or configuration on the phone: • 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.

The phone has power issues

Use this procedure to troubleshoot power issues with your phone.

Problem

The phone has power issues or no power. The problem might be with the phone, the AC outlet, or the PoE network switch.

Workaround

Try one of the following:

- 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.
- Check to see if the phone is plugged into an outlet controlled by a light switch.
- If the phone is plugged into a power strip, try plugging it directly into a wall outlet instead.

The phone doesn't boot up

Use this procedure to troubleshoot a phone that doesn't boot up.

Problem

If the phone doesn't boot up, its firmware image or configuration might be corrupt or invalid.

Workaround

Try one of the following:

- Ensure that the provisioning server is accessible on the network and that a valid software load and valid Configuration files are available.
- Ensure that the phone configuration has the correct address for the provisioning server on the network.

Troubleshooting screen and system access issues

The following procedures provide tips for resolving screen and system access issues.

Screen and system access issues

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

Table 19-6 Screen and System Access Issues

Issue	Cause and Possible Solution
There's no response from feature key presses.	If your phone keys don't respond to presses: • 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. Reboot the phone to attempt reregistration to the call server. Go to **Menu** > **Settings** > **Advanced** > **Reboot Phone**).
The display shows the message "Network Link is Down".	This message displays when the LAN cable isn't properly connected. Do the following: • 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. Reboot the phone to attempt reregistration to the call server. Go to **Menu** > **Settings** > **Advanced** > **Reboot Phone**).

There's no response from feature keys

Use this procedure to troubleshoot feature keys not responding.

Problem

The feature keys on the phone don't respond as expected.

Workaround

Try one of the following:

- Press the keys more slowly.
- Check the key mapping. Its map might point to a different function.

- Check whether the key is disabled.
- Make a call to the phone to check for inbound call display and ringing. If successful, try pressing feature keys while a call is active to access a directory or buddy status.
- Confirm that the line is registered to the call server. Go to **Menu** > **Status** > **Lines**.

NOTE: If the line isn't registered to the call server, reboot the phone. Go to **Menu** > **Settings** > **Advanced** > **Reboot Phone**.

The display indicates that the network link is down

Use this procedure to troubleshoot a **Network Link is Down** message.

Problem

The display shows the following message:

Network Link is Down

This message happens when the LAN cable isn't properly connected.

Workaround

Try one of the following:

- Check the termination at the network switch or hub end of the network LAN cable.
- Check that the network 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.
- Reboot the phone to re-register to the call server. Go to **Menu** > **Settings** > **Advanced** > **Reboot Phone**.

Troubleshooting calling issues

The following procedures provide tips for resolving calling issues.

Calling issues

The following table provides possible solutions to common issues.

Table 19-7 Calling Issues

Issue	Cause and Possible Solution
There's no dial tone.	If there's no dial tone, power may not be correctly supplied to the phone. Try the following: • 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.	If there's no ringtone but the phone displays a visual indication when it receives an incoming call, do the following: • Adjust the ring level from the front panel using the volume up/down keys. • Check the status of handset, headset (if connected), and hands-free speakerphone.
The line icon shows an unregistered line icon.	If the phone displays an icon indicating that a line is unregistered, reregister the line and place a call.
Lifting the handset does not answer calls when the ringtone is silent.	By default, lifting the handset does not answer incoming calls if the line is using a silent ringtone. To answer the call, use the Answer softkey or touch the line key that is associated with the ringing call. You can change the default behavior using configuration so that the ring type that is associated with the visual ringer uses the more common "ring" type instead of "silent."

There's no dial tone

Use this procedure to troubleshoot the absence of a dial tone.

Problem

If there's no dial tone, power might not be correctly supplied to the phone.

Workaround

Try the following:

- Check that the display is illuminated.
- Make sure that 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.

There's no dial tone on one of the audio paths

Use this procedure to troubleshoot the absence of a dial tone on one of the audio paths.

Problem

The dial tone isn't present on one of the audio paths.

Workaround

Try one of the following options:

- Check whether the dial tone is present on another path by following these steps:
  1. Switch between handset, headset (if present), or hands-free speakerphone.
  2. If the dial tone exists on another path, connect a different handset or headset to isolate the problem.
- Check the configuration for gain levels.

The phone doesn't ring

Use this procedure to troubleshoot the phone not ringing.

Problem

The phone doesn't ring.

Workaround

If there's no ringtone but the phone displays a visual indication when it gets an incoming call, do the following:

- Adjust the ring level from the front panel using the volume up/down keys.
- Check the status of the handset, the headset (if connected), and the hands-free speakerphone.

Unregistered line icon

Use this procedure to troubleshoot an unregistered line icon.

Problem

The line icon shows an unregistered line icon.

Workaround

If the phone displays an icon indicating that a line is unregistered, reregister the line and place a call.

Lifting the handset does not answer calls when the ringtone is silent

Use this procedure to change the default answering behaviour when the ringtone is silent.

1. Open the configuration file.
2. Add the following settings:

   ```
   se.rt.visual.type="ring"
   ```

```
se.pat.ringer.ringer1.inst.1.value="1"
```

3. Save the configuration file.

Troubleshooting display issues

The following procedures provide tips for resolving display screen issues.

Display issues

The following table provides tips for resolving display screen issues.

Table 19-8 Display Issues

Issue	Cause and Possible Solution
There's no display or the display is incorrect.	If there's no display, power may not be correctly supplied to the phone. Do the following: • 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. Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to *Capture Your Device's Current Screen*.
The display is too dark or too light.	The phone contrast may be set incorrectly. Do one of the following: • Adjust the contrast. • Reboot the phone to obtain the default level of contrast.
The display is flickering.	Certain types of older fluorescent lighting may cause the display to flicker. If your phone is in an environment with fluorescent lighting, angle or move the Poly phone away from the lights.
The time and date are flashing.	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: • Reconnect the phone to the LAN. • Configure an SNTP server. Disable the time and date if you don't want to connect your phone to a LAN or SNTP server.

There's no display or the display is incorrect

Use this procedure to troubleshoot a blank screen.

Problem

If there's no display, power might not be correctly supplied to the phone.

Workaround

- 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.

The display is too dark or too light

Use this procedure to adjust your displace brightness.

Problem

The phone contrast may be set incorrectly.

Workaround

- Adjust the contrast.
- Reboot the phone to obtain the default level of contrast.

The phone display is flickering

Use this procedure to troubleshoot a flickering phone display.

Problem

Certain types of older fluorescent lighting may cause the display to flicker.

Workaround

If your Poly phone is in an area with fluorescent lighting, angle or move the phone away from the lights.

The time and date are flashing

Use this procedure to troubleshoot a flashing date and time on your phone.

Problem

The time and date on your Poly phone display are flashing.

Workaround

- Reconnect the phone to the LAN.
- Configure an SNTP server.
- If you don't want to connect your phone to a LAN or SNTP server, disable the time and date.

Audio Issues

The following table describes possible solutions to audio issues.

Table 19-9 **Audio Issues**

Issue	Cause and Possible Solution
There is no audio on the headset	If there is no audio on your headset, the connections may not be correct. Do one of the following: • Ensure the headset is plugged into the jack marked Headset at the rear of the phone. • Ensure the headset amplifier (if present) is turned on and adjust the volume.

Troubleshooting audio issues

Use this procedure to troubleshoot audio issues.

Problem

There's no audio on the headset.

Workaround

If there's no audio on your headset, the connections might not be correct. Do one of the following:

- Ensure that the headset is plugged into the Headset jack at the rear of the phone.
- Ensure that the headset amplifier (if present) is on, and then adjust the volume.

Software upgrade issues

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

Table 19-10 Software Upgrade Issues

Issue	Cause and Possible Solutions
Some settings or features aren't working as expected on the phone.	The phone's configuration may be incorrect or incompatible. 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.
The phone displays a Config file error message for five seconds after it boots up.	You're using configuration files from a PVOS version earlier than the PVOS image running on the phones. Configuration parameters and values can change each release and specific parameters may or may not be included. See the PVOS Administrator's Guide and Release Notes for the PVOS version you've installed on the phones. Correct the configuration files, remove the invalid parameters, and restart the phone.
When using the system web interface to upgrade phone software, the phone is unable to connect to the Poly Hosted Server.	Occasionally, the phone is unable to connect to the Poly-hosted server because of the following: • 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. To troubleshoot the issue: • Try upgrading your phone later. • Verify that new software is available for your phone using the PVOS Release Matrix. • Verify that your network's configuration allows the phone to connect to `http://downloads.polycom.com`. If the issue persists, try manually upgrading your phone's software.

Phone settings or features aren't working

Use this procedure to troubleshoot phone settings or features that aren't working as expected.

Problem

The phone's configuration might be incorrect or incompatible.

Workaround

Check for errors on the phone.

1. Go to **Menu** > **Status** > **Platform** > **Configuration**.

2. Check for the following error messages:
   - **Errors Found**
   - **Unknown Params**
   - **Invalid values**
3. If any of the specified messages are present, correct your Configuration files and restart the phone.

Phones display a Configuration file error message

Use this procedure to troubleshoot Configuration file error messages on your phones.

Symptom

When starting, phones display a Configuration file error message for five seconds.

Problem

Your Configuration files are from a Poly VideoOS version earlier than the image on your phones. Configuration parameters and values can change with each release. Newer releases might not include some parameters from previous releases.

Workaround

To correct the Configuration files, remove the invalid parameters and restart the phone. For more information, refer to the Administrator Guide and Release Notes for the Poly VideoOS version on the phones.

Phones can't connect to the Poly-hosted server

Use this procedure to troubleshoot your phone's connection to the server.

Problem

Phones might be unable to connect to the Poly-hosted server due to one of the following:

- The server is temporarily unavailable.
- The phone has no software upgrade information to receive.
- The network configuration is preventing the phone from connecting to the server.

Workaround

Try one of the following:

- Upgrade your phone later.
- Use the PVOS Release Matrix to verify that new software is available for your phone.
- Verify that your network's configuration allows the phone to connect to `http://downloads.polycom.com`.
- If the issue persists, try manually upgrading your phone's software.

Provisioning Issues

If settings you make from the central server aren't working, check first for priority settings applied from the phone menu system or system web interface. Afterward, check for duplicate settings in your configuration files.

To make sure that the provisioning server address is correct, that DNS is able to resolve the server address, and to see if there are any errors, refer to Run a DNS Test from the System Web Interface on page 291.

Table 19-11 Provisioning Issues

Issue	Cause and Possible Solutions
After powering on the phone and connecting it to the network, the phone doesn't reach out to the correct provisioning server. The configured provisioning server address (in **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Provisioning Server**) is correct, but the Provisioning Server field in **Settings** > **Status** > **Platform** > **Configuration** shows a different address.	The network may be configured with a DHCP Option 160 or 66 for the provisioning server. You can either ask the network administrator to remove the DHCP Option 160/66 configuration from the DHCP server, or set the "Boot Server" field to static, under**Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Provisioning Server** > **DHCP Menu**.

Troubleshooting provisioning issues

Use this procedure to troubleshoot provisioning issues.

Problem

After you power on the phone and connect it to the network, the phone doesn't connect to the correct provisioning server. This is a result of conflicting provisioning server addresses in the following locations:

- In **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Provisioning Server**, the configured provisioning server address is correct.
- In **Settings** > **Status** > **Platform** > **Configuration**, the **Provisioning Server** field shows a different address.

Workaround

Try one of the following:

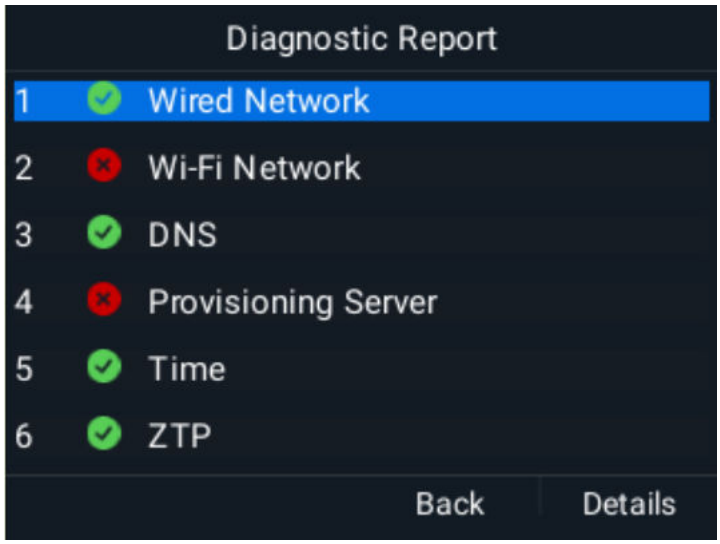
- If settings you make from the central server aren't working, check the following, in this order:
  1. Check for priority settings applied from the local interface or system web interface.
  2. Check for duplicate settings in your Configuration files.
- The network might be configured with a DHCP Option 160 or 66 for the provisioning server. Do one of the following:
  - Ask the network administrator to remove the DHCP Option 160/66 configuration from the DHCP server.
  - Set the **Boot Server** field to static, under **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Provisioning Server** > **DHCP Menu**.

- Refer to Run a DNS Test from the System Web Interface on page 291 to:
  - Make sure that the provisioning server address is correct.
  - Make sure that DNS is able to resolve the server address.
  - See if there are any errors.

Run a Diagnostics Check

If you are having problems with your phone, run a diagnostics check to determine if there are any issues.

1. Do one of the following:
   - Go to **Menu** > **Help & Support**.
   - Go to **Menu** > **Settings** > **Diagnostics**.
2. Select **Run Diagnostics**.
3. On the *Diagnostics Check* screen, select **Yes** to run the check.



   The icon next to the item indicates the status:
   - **Passed**
   - **Failed**
   - **Disabled**
4. On the *Diagnostics Report* screen, do one of the following:
   - Choose a component and select **Details** to see detailed information.
   - Select **Back** to return to the *Help & Support* screen.

Run a diagnostics check

Use this procedure to troubleshoot problems with your phone.

Workaround

If you are having problems with your phone, run a diagnostics check to determine if there are any issues.

1. Do one of the following:
   - Go to **Menu** > **Help & Support**.
   - Go to **Menu** > **Settings** > **Diagnostics**.
2. Select **Run Diagnostics**.
3. On the *Diagnostics Check* screen, select **Yes** to run the check.



The icon next to the item indicates the status:

- **Passed**
- **Failed**
- **Disabled**

4. On the *Diagnostics Report* screen, do one of the following:
   - Choose a component and select **Details** to see detailed information.
   - Select **Back** to return to the *Help & Support* screen.

Preparing to Troubleshoot Issues

To prepare to troubleshoot issues with your phone, you can investigate existing warnings, run a diagnostics check, or test the phone hardware.

View Warnings

When a phone is unable to perform certain tasks, a **Warning** icon displays in the status bar.

View details about the issues from the *Warnings* screen.

1. Go to **Settings** > **Status** > **Diagnostics**.
2. Select **Warnings**.

   The *Warnings* screen displays, listing any issues.

Remove warnings

Clear warnings displayed on the phone's screen.

After you view phone warnings, you can temporarily remove the warning icon from the status bar. However, the warning displays in the **Warnings** list until you resolve the issue. The warning icon displays each time your phone has a warning that you haven't viewed.

- In the *Warnings* screen, select **Clear Icon**.

Speakerphone

If your speakerphone doesn't work, your system administrator may have disabled it. If this is the case, a message displays after you press the speakerphone key informing you that Handsfree mode is disabled. In this case, use the handset or a headset to handle calls.

Troubleshooting speakerphone

Use this procedure to troubleshoot your speakerphone not working.

Problem

When you press the speakerphone key, the speakerphone doesn't work. If you receive a message stating **Handsfree mode is disabled**, your system administrator disabled it.

Workaround

If your system administrator disabled the speakerphone, use the handset or a headset to handle calls.

USB Port

If you attach a USB device to your phone, and the phone does not detect the attached USB device, your system administrator may have disabled the USB port on your phone.

In this case, you cannot attach a USB device to your phone to use the following features:

- Call recording
- Picture frame
- USB headset

Contact your system administrator for help on enabling the USB port on your phone.

USB not detected

Use this procedure to troubleshoot your phone not detecting an attached USB device.

Problem

Your phone doesn't detect an attached USB device, which prevents you from using the following features:

- Call recording
- Picture frame
- USB headset
- Video calls on VVX 501 and VVX 601 phones with a USB camera
- USB charging device on the VVX 601 phones

Workaround

If your phone can't detect an attached USB device, your system administrator might have disabled the USB port on your phone. Contact your system administrator for help on re-enabling the USB port.

Troubleshooting Bluetooth headset issues

If you encounter any issues related to Bluetooth headsets, use the following procedures for possible solutions to common problems.

Bluetooth Headset Issues

If you encounter any issues using a Bluetooth headset, see the following table for possible solutions to common problems.

Table 19-12 **Common Bluetooth Headset Issues and Solutions**

Issue	Corrective Action
The Bluetooth settings do not display on my phone	Do one of the following: • Check with your system administrator to see if the Bluetooth feature is enabled on your phone.
My headset doesn't pair automatically.	If your headset is an older model, you may need to enter a password before the headset can pair with your phone. Refer to your headset documentation for more information.

Bluetooth settings don't display

Use this procedure to troubleshoot a phone not showing Bluetooth settings.

Problem

Your phone doesn't display its Bluetooth settings.

Workaround

Do one of the following:

1. Check with your system administrator to see if you can enable the Bluetooth feature on your phone.
2. If your phone is part of the Poly CCX or Poly VVX series, check the **Bluetooth Radio** setting to make sure that it is on.

Headset doesn't pair automatically

Use this procedure to troubleshoot problems with automatic pairing.

Problem

The Bluetooth headset fails to pair automatically.

Workaround

If your headset is an older model, you might need to enter a password before the headset can pair with your phone. For more information, refer to your headset documentation.

Troubleshooting recording issues

If you encounter any issues recording calls, use the following procedures for possible solutions to common problems.

Recording Issues and Solutions

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

Table 19-13 Common Recording Issues and Solutions

Issue	Corrective Action
The message "USB device is full. Recording canceled" displays when I pressed Start.	Check that there's sufficient space on the USB flash drive.
The recording stops during a call.	If the USB flash drive becomes full during recording, recording stops and the message "USB device is full. Recording stopped" displays. Delete previous recordings to make space on the USB flash drive.
The message "USB device removed unsafely. Recording canceled" displays when I remove my USB flash drive during a call.	Don't remove the USB flash drive while recording. If you want to remove the drive during a call, press **Stop**, and then remove the drive.
The message "Unsupported USB device attached" displays.	Use the Compatibility Matrix for a list of compatible headsets.

Recording fails immediately after starting

Use this procedure to troubleshoot recording failures when starting a call.

Problem

When you press **Start**, you receive the following error message:

"USB device is full. Recording canceled."

Workaround

Check the USB flash drive and ensure it has enough space to store the recording.

Recording fails during a call

Use this procedure to troubleshoot recording failures during a call.

Problem

During a call, the recording stops and you receive the following error message:

"USB device is full. Recording stopped."

Workaround

Delete previous recordings on the USB flash drive to clear up space.

Recording canceled after removing USB flash drive

Use this procedure to troubleshoot a canceled recording.

Problem

If you remove the USB flash drive while you're recording a call, you receive the following error message:

"USB device removed unsafely. Recording canceled."

Workaround

Don't remove the USB flash drive while recording.

To remove the drive during a call:

1. Press **Stop**.
2. Remove the drive.

Unsupported USB headset causes recording to fail

Use this procedure to troubleshoot an unsupported headset.

Problem

When you try to record a call while using a USB headset, the following message displays:

Unsupported USB device attached.

Workaround

For a list of compatible headsets, refer to the Compatibility Matrix.

Viewing the Phone's Status

View the status of your phone and various features.

View System Information

View information that may be helpful for troubleshooting issues, including the phone's model number, software version, MAC address, and IP address.

1. Go to **Settings** > **Status**.
2. Select **System Information**.

Check the status of the calendar

Issues with the phone's connection to the Microsoft server may cause calendar problems.

Without a functioning connection, you might not see the **Calendar** icon on the *Home* screen or you might not receive meeting reminders.

1. Go to **Settings** > **Calendar**.
2. On the **Calendar** screen, select **Connect**.

View the PAB status

View the status of the Personal Address Book (PAB) on your phone to determine any issues with the PAB. Contact your system administrator for further troubleshooting help.

- Go to **Settings** > **Status** > **Contact Directory**.

  The following information displays:

  - Status
  - Server Control Method
  - Server URL
  - Registration Index and User ID

View the GAB Status

View the status information and server URL for the global address book.

- Go to **Settings** > **Status** > **Global Address Book**.

  The status information and the server URL for the GAB display.

20 Getting help

Poly is now a part of HP. The joining of Poly and HP paves the way for us to create the hybrid work experiences of the future. Information about Poly products has transitioned from the Poly Support site to the HP Support site.

The Poly Documentation Library is continuing to host the installation, configuration/administration, and user guides for Poly products in HTML and PDF format.

In addition, the Poly Documentation Library provides Poly customers with information about the transition of Poly content from Poly Support to HP Support.

The HP Community provides additional tips and solutions from other HP product users.

HP Inc. addresses

Contact HP at the following office locations.

HP US
HP Inc.
1501 Page Mill Road
Palo Alto, CA 94304
United States
Phone:+ 1 650-857-1501

HP Germany
HP Deutschland GmbH
HP HQ-TRE
71025 Boeblingen, Germany

HP Spain
HP Printing and Computing Solutions, S.L.U.
Cami de Can Graells 1-21 (Bldg BCN01)
Sant Cugat del Valles
Spain, 08174
902 02 70 20

HP UK
HP Inc UK Ltd
Regulatory Enquiries, Earley West
300 Thames Valley Park Drive
Reading, RG6 1PT
United Kingdom

Document information

Review the following document information.

Model ID: Poly Edge E Series

Document part number: P54696-001A

Last update: June 2025

Email us at documentation.feedback@hp.com with queries or suggestions related to this document.