Poly CCX Business Media Phones with OpenSIP Administrator Guide 9.0.0

SUMMARY

This guide provides administrators with information about configuring, maintaining, and troubleshooting the featured product.

Legal information

Privacy policy

HP complies with applicable data privacy and protection laws and regulations. HP products and services process customer data in a manner consistent with the HP Privacy Policy. Please refer to HP Privacy Statement.

Open source software used in this product

This product contains open source software. You may receive the open source software from HP up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to HP of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact HP by email at ipgoopensourceinfo@hp.com.

Table of contents

1 Before you begin

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

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

- Poly CCX 400 Business Media Phone
- Poly CCX 500 Business Media Phone
- Poly CCX 505 Business Media Phone
- Poly CCX 600 Business Media Phone
- Poly CCX 700 Business Media Phone
- Poly CCX EM60 Expansion Module
- Polycom EagleEye Mini USB camera

Audience, purpose, and required skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

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

Icons used in Poly documentation

This section describes the icons used in Poly documentation and what they mean.

⚠ **WARNING!** Indicates a hazardous situation that, if not avoided, **could** result in serious injury or death.

⚠ **CAUTION:** Indicates a hazardous situation that, if not avoided, **could** result in minor or moderate injury.

IMPORTANT: Indicates information considered important but not hazard-related (for example, messages related to property damage). Warns the user that failure to follow a procedure exactly as described could result in loss of data or in damage to hardware or software. Also contains essential information to explain a concept or to complete a task.

NOTE: Contains additional information to emphasize or supplement important points of the main text.

TIP: Provides helpful hints for completing a task.

Poly CCX phones model numbers

The following table lists the product names and software model numbers for Poly CCX business media phones. The phone uses software model numbers 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 CCX model numbers

Product name	Software model number
Poly CCX 400 business media phone	3111-49700-001
Poly CCX 500 business media phone	3111-49710-001
Poly CCX 505 business media phone	3111-49730-001
Poly CCX 600 business media phone	3111-49770-001
Poly CCX 700 business media phone	3111-49740-001

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.

2 Getting Started

Understand Poly Voice Software (PVOS) and review methods to configure your phones.

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

PVOS overview

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

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

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

Methods for configuring phones

Poly offers several methods to configure or provision phones.

Configure the phone settings using one of the following methods:

- Simple setup
- System web interface
- USB flash drive
- Configuration files through the system web interface to copy phone settings from one phone to another

Poly phones come installed with updater software that resides in the flash memory of the phone. When you start 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).

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

Provisioning in a DHCP Network Environment

Your deployment must meet the following requirements so your phones can communicate with the provisioning server in a DHCP network environment:

- You must enable DNS, even if the DHCP server returns the provisioning server address in IPv4 format. Disabling DNS may prevent you from provisioning your phones.
- If you manually configure the provisioning server, you must configure a primary or secondary DNS server.
- The phones must have permission to resolve information either through a network server or static cache.

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. USB
5. Poly Clariti Manager
6. Centralized provisioning
7. 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 *Poly CCX Business Media Phones Parameter Reference Guide*

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

   To find your phone's IP address, go to **Settings** > **Status** > **System Information**.

2. Select **Admin** as the login type and enter the administrator password.
3. Select **Simple Setup**.
4. Configure the following settings:

   Table 2-1 Simple Setup settings

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

5. Select **Save**.

Configure a Phone Through the System Web Interface

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

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`.
   - The `*.sip.ld` file for your phone.
3. Insert the USB flash drive into a USB port on the phone, enter the administrator password, and power cycle the phone.

Wait several minutes for your device to restart.

3 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 HP Support.

Power CCX phones

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

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

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.

Poly CCX Power over Ethernet classes

For Power over Ethernet classes on CCX phones, see the following table.

NOTE: The values outlined in the table below do not include Wi-Fi usage.

Table 3-1 Poly CCX Power over Ethernet classes

Phone Model	PoE Class	PoE Class Maximum	Normal Call	Maximum with All USB Loading
CCX 400	3	12.95 W	5 W	12 W
CCX 500	0	12.95 W	8 W	12 W
CCX 505	0	12.95 W	8 W	12 W
CCX 600	4	25.5 W	11 W	18 W
CCX 700	4	25.5 W	13 W	20 W

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. Choose the system's base profile from the displayed list.

   For more information on base profiles, see {Xref Error! Target does not exist.}.

7. Select **Next** and confirm your selection.

The phone starts in your selected base profile.

Enable USB Audio Mode on CCX Phones

Configure a CCX business media phone for use as an external USB audio device.

On CCX 500, CCX 505, and CCX 600 phones, connect a USB cable from your PC to the USB-C port on the side of your phone to enable USB audio mode by default. On CCX 400 phones, you must configure the USB port on your phone before you can use it as a USB audio peripheral for your PC.

CCX 400 phones in USB audio mode can't connect to USB headsets, even if users disconnect their phone from a computer. To re-enable use with USB headsets, revert the parameters to their default settings. Users can use headsets that connect to the RJ9 port on the back of the phone in either configuration.

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

NOTE: These parameters are automatically configured for USB audio mode when you set the phone to the Microsoft USB Phone base profile.

1. Open the configuration file.
2. Disable host mode.

```
feature.usb.host.enabled="0"
```

3. Enable USB device mode and USB audio mode.

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

```
feature.usb.device.audio="1"
```

4. Save the configuration file.

Disable USB Audio Mode

Once you disable USB audio mode, users can't set the phone as a USB audio device from a connected computer.

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

USB audio mode is enabled by default on Poly CCX 500, CCX 505, CCX 600, and CCX 700 business media phones.

1. Open the configuration file.
2. Disable USB audio mode on the phone.

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

3. Save the configuration file.

Enable USB Phone Mode

Set up your phone to work in USB phone mode when connected to a computer.

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

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

USB phone mode enables users to place calls directly from the phone hardware through softphone clients, such as Skype for Business or Microsoft Teams, on their Windows computers.

NOTE: Mac computers don't support dialing from the USB phone.

The softphone client on the computer must support Human Interface Device (HID) connections to support USB phones. No other native call applications can run on the phone while in USB phone mode.

NOTE: For the best performance, only use USB phone mode with one softphone client at a time.

1. Open the configuration file.
2. Configure USB phone mode.

```
device.baseProfile.set="1"
```

```
device.baseProfile="USBOptimized"
```

3. Save the configuration file.

Poly CCX phones base profiles

Select a base profile when you set up your phone for the first time. After initial setup, use the phone's system web interface to select a base profile.

The following table shows the base profiles that are available and supported on CCX business media phones.

Table 3-2 Poly CCX phones base profiles

Phone Model	Generic	Microsoft Teams	Zoom Phone	Microsoft USB Phone	8x8 Work	Dialpad
CCX 400	Yes	Yes	Yes	Yes	No	No
CCX 500	Yes	Yes	Yes	Yes	No	No
CCX 505	Yes	Yes	Yes	Yes	No	No
CCX 600	Yes	Yes	Yes	No	No	No
CCX 700	Yes	No	Yes	No	No	No

Generic base profile

This base profile provides the full Poly OpenSIP experience. Your CCX phone runs the Generic application, and the phone is managed using HP Support. For more information about the Generic base profile and HP Support, see the HP Support website.

After users sign in to their phones, they can make calls, view their calendar, and attend meetings. To assist users with the Generic base profile provisioned on Poly CCX business media phones, see the *Poly CCX Business Media Phones with OpenSIP User Guide*.

Microsoft Teams base profile

This base profile provides a full Microsoft Teams experience. Your CCX phone runs the Microsoft Teams application, and the phone is managed using the Microsoft Teams Admin Center. For more information about Microsoft Teams and the Microsoft Teams Admin Center, see the Microsoft documentation website.

After users sign in to their phones, they can make Microsoft Teams calls, view their calendar, and attend meetings. To assist users with Microsoft Teams provisioned on Poly CCX business media phones, see the *Poly CCX Business Media Phones with Microsoft Teams User Guide*.

Zoom Phone base profile

This base profile provides a full Zoom Phone experience. Your CCX phone runs the Zoom Phone application, and the phone is managed using Zoom Phone System Support. For more information about Zoom Phone and Zoom Phone System Support, see the Zoom Support website.

After users sign in to their phones, they can make Zoom Phone calls, view their calendar, and attend meetings. To assist users with Zoom Phone provisioned on

Poly CCX business media phones, see the *Quick Tips for Poly CCX Business Media Phones with Zoom* guide.

Microsoft USB Phone base profile

The Microsoft USB Phone base profile is an experimental feature pending USB peripheral certification with Microsoft, and its complete design and support by Poly and Microsoft is not yet determined. The Microsoft USB Phone base profile is compatible with the classic and new Microsoft Teams desktop applications. Feature functionality varies between the classic and new Microsoft Teams applications, and future CCX and Microsoft Teams updates will focus only on supporting the new Microsoft Teams application.

This base profile provides a traditional desk phone experience to augment a computer's soft client when users connect their CCX phone to the computer using a USB cable: a dialpad to place outgoing calls, and a handset, hands-free speakerphone, or optional headset that enables Poly's Acoustic Clarity, NoiseBlockAI, and Acoustic Fence technologies.

IMPORTANT: On CCX 600 and CCX 700 phones, support for the Microsoft USB Phone base profile is deprecated in PVOS 8.1.0 and later.

8x8 Work base profile

IMPORTANT: The 8x8 Work base profile is not available in PVOS 9.0.0. Support for the 8x8 Work base profile remains available in previous PVOS releases. Subscribers to this service will receive updates from their provider once the partner application is ready and certified for use on Poly CCX business media phones running PVOS 9.0.0 or later.

This base profile provides a limited 8x8 Work experience. Your CCX phone runs the 8x8 Work application, and the phone is managed using 8x8 Support. For more information about 8x8 Work and 8x8 Support, see the 8x8 Support website.

After users sign in to their phones, they can make 8x8 Work calls, view their calendar, and attend meetings using audio only.

Dialpad base profile

IMPORTANT: The Dialpad base profile is not available in PVOS 9.0.0. Support for the Dialpad base profile remains available in previous PVOS releases. Subscribers to this service will receive updates from their provider once the partner application is ready and certified for use on Poly CCX business media phones running PVOS 9.0.0 or later.

This base profile provides a full Dialpad experience. Your CCX phone runs the Dialpad application, and the phone is managed using the Dialpad Help Center. For more information about Dialpad and the Dialpad Help Center, see the Dialpad Help Center website.

After users sign in to their phones, they can make Dialpad calls, view their calendar, and attend meetings.

Set the Base Profile from the Settings Menu

You can use the phone **Settings** menu to set a phone's base profile.

1. Select **Menu**.
2. Go to **Settings** > **Advanced** .
3. Enter the administrator password (the default is `456`).
4. Select **Administration Settings** > **Network Configuration** > **Base Profile**.
5. Select the base profile that you want to set.
6. Select Back and save the configuration.

   The phone restarts, and the selected base profile loads.

Set the Base Profile Using the System Web Interface

You can use the system web interface to set a phone's base profile.

1. Turn on the phone and wait until it completes the power-up process.
2. Get the IP address of the phone by navigating to **Settings** > **Status** > **Platform** > **Phone**.

   The IP address displays in the **IP** field.
3. Enter the phone's IP address in the address bar of a web browser.

   The system web interface login screen displays.
4. Choose **Admin** to log in as an administrator, and then enter the administrator password (the default is `456`) and click **Submit**.
5. On the Home page, navigate to the **Simple Setup** menu.
6. From the **Base Profile** drop-down list, select the base profile that you want to set.
7. Click **Save**.
8. In the confirmation dialog, choose **Yes**.

   The phone restarts, and the selected base profile loads.

4 Call Servers

Register your phones with a SIP server and configure call server features for your Poly phones to use. PVOS supports SIP 2.0 based on RFC 3261.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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 CCX 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.

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 CCX 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 CCX 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 CCX 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.

Call Server Features

CCX phones support several call 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.

Create a Custom TCP Keep-Alive Message

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

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

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.

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

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.

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.

Enable Server-Specific Features

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

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

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.

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, see the parameter reference topic(s) in the *Poly CCX 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.

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 CCX 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 CCX 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.

5 Networking

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.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

System Names Transmitted with Network Protocols

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

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

For example: CCX700_D1EB

Table 5-1 System and Model Names

Model	System Name
CCX 400	CCX400_*<MAC>*
CCX 500	CCX500_*<MAC>*
CCX 505	CCX505_*<MAC>*
CCX 600	CCX600_*<MAC>*
CCX 700	CCX700_*<MAC>*

Configuring Internet Protocol settings

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

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

Configure a static IPv4 address

Configure IPv4 mode in the phone's local interface.

Connect your phone to an Ethernet network connection.

IMPORTANT: Configuring the following parameter(s) 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 CCX 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 CCX 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 CCX 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.

Wi-Fi network connectivity

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

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

IMPORTANT: 5GHz operation is not permitted in all countries. CCX 505, 600, and 700 default to a country setting of "Worldwide Regulatory Domain" that complies with a global set of WiFi regulatory standards. The CCX's country of operation must be changed if this spectrum is available in your country before 5GHz operation is permitted.

Note the following when using Wi-Fi:

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

Your phone supports the following wireless modes:

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

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

Configure Wi-Fi using a configuration file

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

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

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

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

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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Enable Wi-Fi.

```
device.wifi.enabled="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>"
```

4. Enable DHCP for Wi-Fi.

```
device.wifi.dhcpEnabled="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>"
```

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

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

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

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

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

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

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.

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

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.

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.

Enable Bluetooth

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

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

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

```
feature.bluetooth.enabled="1"
```

3. Enable Bluetooth radio.

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

NOTE: If the Bluetooth device name is not set, the phone will use the other configured settings as the Bluetooth device name, like the System Name (`system.name`) or label for registration line 1 (`reg.1.label`).

4. 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.

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 CCX Parameter Reference Guide*.

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.

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

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

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

```
bluetooth.pairedDeviceMemorySize="<Max number of devices>"
```

4. 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, see the parameter reference topic(s) in the *Poly CCX 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>"
```

5. **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>"
```

6. Save the configuration file.

Enable the Bluetooth Menu in the Poly Control Panel

Enable access to the Bluetooth menu from the **Poly Control Panel**.

1. Open the configuration file.
2. Enable Bluetooth menu access from the **Poly Control Panel**.

```
apps.android.statusBar.Bluetooth.enabled="1"
```

3. Save the configuration file.

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.

Setting the time and date

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

Configure time and daylight saving time

Configure time, time zone, and daylight saving time on the 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Configure the SNTP server to automatically configure the time.

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

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

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

4. **Optional:** Configure Daylight Saving Time.

```
tcpIpApp.sntp.daylightSavings.fixedDayEnable="1"
tcpIpApp.sntp.daylightSavings.start.month="<set month
to start DST>"
```

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

5. Save the configuration file.

Set the time zone location

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

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

1. Open the configuration file.
2. Set the correct time zone location to display on the local interface and the system web interface.

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

Use the following parameters to configure the time zone location.

Table 5-2 Time Zone Location Parameter Values

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

Table 5-2 Time Zone Location Parameter Values (continued)

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

Table 5-2 Time Zone Location Parameter Values (continued)

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

Table 5-2 Time Zone Location Parameter Values (continued)

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

Table 5-2 Time Zone Location Parameter Values (continued)

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

3. Save the configuration file.

Configure Olson time zone

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

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

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

Table 5-3 Olson Time Zone IDs

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

Table 5-3 Olson Time Zone IDs (continued)

Olson Time Zone ID	Poly Time Zone ID
Europe/Sarajevo	(GMT +1:00) Sarajevo,Skopje
Africa/Brazzaville	(GMT +1:00) West Central Africa
Africa/Windhoek	(GMT +1:00) Windhoek
Asia/Amman	Amman
Europe/Athens	(GMT +2:00) Athens
Asia/Beirut	Beirut
Africa/Cairo	(GMT +2:00) Bucharest,Cairo
Europe/Helsinki	(GMT +2:00) Helsinki,Kyiv
Asia/Jerusalem	(GMT +2:00) Jerusalem
Africa/Harare	(GMT +2:00) Harare,Pretoria
Europe/Minsk	(GMT +3:00) Minsk
Asia/Istanbul	(GMT +3:00) Istanbul
Europe/Moscow	(GMT +3:00) Moscow
Asia/Kuwait	(GMT +3:00) Kuwait,Riyadh
Africa/Nairobi	(GMT +3:00) Nairobi
Asia/Tehran	(GMT +3:30) Tehran
Asia/Baku	(GMT +4:00) Baku,Tbilisi
Asia/Yerevan	(GMT +4:00) Yerevan
Asia/Dubai	Dubai
Asia/Kabul	(GMT +4:30) Kabul
Asia/Karachi	(GMT +5:00) Karachi
Asia/Tashkent	(GMT +5:00) Tashkent
Asia/Yekaterinburg	(GMT +5:00) Yekaterinburg (RTZ 4)
Asia/Calcutta	(GMT +5:30) Kolkata,New Delhi
Asia/Colombo	(GMT +5:30) Sri Jayawardenepura
Asia/Katmandu	(GMT +5:45) Kathmandu
Asia/Dhaka	(GMT +6:00) Astana,Dhaka
Asia/Rangoon	(GMT +6:30) Yangon (Rangoon)
Asia/Krasnoyarsk	(GMT +7:00) Krasnoyarsk (RTZ 6)
Asia/Bangkok	(GMT +7:00) Bangkok,Hanoi
Asia/Jakarta	(GMT +7:00) Jakarta
Asia/Shanghai	(GMT +8:00) Beijing,Chongqing
Asia/Hong_Kong	(GMT +8:00) Hong Kong,Urumqi
Asia/Irkutsk	(GMT +8:00) Irkutsk (RTZ 7)

Table 5-3 Olson Time Zone IDs (continued)

Olson Time Zone ID	Poly Time Zone ID
Asia/Kuala_Lumpur	(GMT +8:00) Kuala Lumpur
Asia/Taipei	(GMT +8:00) Taipei,Perth
Asia/Tokyo	(GMT +9:00) Tokyo,Seoul,Osaka
Asia/Yakutsk	(GMT +9:00) Sapporo,Yakutsk (RTZ 8)
Australia/Adelaide	Adelaide
Australia/Darwin	Darwin
Australia/Brisbane	Brisbane
Australia/Hobart	(GMT +10:00) Hobart
Australia/Sydney	Sydney,Canberra
Asia/Vladivostok	(GMT +10:00) Vladivostok
Pacific/Guam	(GMT +10:00) Guam,Port Moresby
Asia/Magadan	(GMT +10:00) Magadan (RTZ 9)
Pacific/Auckland	(GMT +12:00) Auckland,Anadyr
Pacific/Fiji	(GMT +12:00) Fiji Islands
Pacific/Majuro	(GMT +12:00) Marshall Islands
Pacific/Tongatapu	(GMT +13:00) Nuku'alofa

1. Open the configuration file.
2. Enter an Olson time zone ID. If you set it to an invalid or unrecognized value, the time zone resets to GMT with daylight saving time disabled.

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

3. Save the configuration file.

Configure location information for emergency services

The Enhanced 911 (E.911) feature enables the phone to obtain location information to share with responders when users dial 911 to report an emergency. This ensures that the operator dispatches emergency services to the correct location.

The phones obtain location information from the following sources:

- LLDP-MED
- LIS compliant with RFC 5985
- DHCP via option 99
- Via XML configuration files

The steps in this process accommodate most configurations. For more information on E.911 configuration parameters, see *Poly CCX Business Media Phones Parameter Reference Guide* .

1. Open the configuration file.
2. Enable the E.911 feature.

> **NOTE:** The INVITE sent for emergency calls from the phone includes the geolocation header defined in RFC 6442 and PIDF presence element as specified in RFC 3863 with a GEOPRIV location object specified in RFC 4119 for OpenSIP environments.

```
feature.E911.enabled="1"
```

3. Configure the source of the phone's location information.

   The following values apply:

   - `LLDP` (default) – Use the network switch as the source of location information.
   - `LIS` - Use the location information server as the source of location information.
   - `DHCP` - Use DHCP as the source of location information.
   - `CONFIG` - Use location information defined in the configuration.

```
locInfo.source="<location information source>"
```

4. 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.

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 CCX 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.

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:

- 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 CCX 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.

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 CCX Parameter Reference Guide* .

Configure jitter buffer for wired network voice traffic

Configure jitter buffer for wired network voice traffic.

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

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

1. Open the configuration file.
2. Enter an average jitter setting, in milliseconds. The default is `20`. The range of values is 0 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 CCX Parameter Reference Guide*.

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

If 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 CCX 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.

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 CCX Parameter Reference Guide*.

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

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

3. Save the configuration file.

Configure IP Type-of-Service for Video

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

Make sure that `qos.ip.rtp.video.dscp="Null"`. Setting a value in `qos.ip.rtp.video.dscp` overrides other `qos.ip.rtip.video.*` parameters.

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

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

1. Open the configuration file.

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

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

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

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

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

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

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

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

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

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

7. Save the configuration file.

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 CCX 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.

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 CCX Parameter Reference Guide*.

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

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

3. 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>"
```

4. 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>"
```

5. Set the SIP server port .

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

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

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

6. 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>"
   ```

7. 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 CCX 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 536870912 .

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

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

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 CCX 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.

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.

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 CCX 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.

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 SIP RTP for FECC

Configure the SIP 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 CCX 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 CCX 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.

Configure RTP video ports

Select a specific port range for RTP video 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Enable RTP video ports.

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

3. Set the starting range for RTP video ports.

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

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

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

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

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

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 CCX 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 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.

6 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 65
   - 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 CCX 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 CCX 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 CCX 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: Client certificates and key must be in PKCS#8 PEM format.. Only CA 1 and 2 and Platform 1 and 2 are valid for Wi-Fi.

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

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: Client certificates and key must be in PKCS#8 PEM format. Only CA 1 and 2 and Platform 1 and 2 are valid for Wi-Fi.

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

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.

7 Securing the phones

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

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Phone passwords

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

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

- Administrator password: `456`
- User password: `123`

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

Configure password settings

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

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 CCX 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 or ZTP, 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.

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.

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 s
```

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.

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

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

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

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Set the duration of a single session in the idle state, in seconds. The default is `900`. The value range is 60 to 86400.

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

3. Set the maximum number of concurrent sessions the phone allows. The default is `10`. The value range is 1 to 20.

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

4. Save the configuration file.

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.

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 CCX 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.

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 CCX 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.

Hide the address of record

Configure your phone to hide the address of record (SIP address) for lines on the phone and Busy Lamp Field (BLF) lines on the phone's screen.

The `reg.x.address` defines the AOR for the lines registered on the phone. By default, it displays beneath the registered line label in multiple locations on the phone.

1. Open the configuration file.
2. Hide the address of record for registered lines on the phone's screen.

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

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 CCX 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 CCX 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.

Enable FIPS 140-2 encryption

The Federal Information Processing Standard (FIPS 140-2) compliance is a cryptographic function. Enable phones to use the FIPS 140-2 compliant cryptography.

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 CCX Parameter Reference Guide*.

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

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

3. Save the configuration file.

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. Optionally, add basic authentication credentials for the 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 CCX 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.

Disabling hardware ports

Disable unused hardware ports to increase security.

Disable the USB ports

Disable unused USB ports to increase the device security.

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 CCX Parameter Reference Guide*.

1. Open the configuration file.

2. Disable the USB ports.

   On Poly CCX 500, CCX 505, CCX 600, and CCX 700 business media phones, set:

   ```
   feature.usb.host.enabled="0"
   ```

   On Poly CCX 400 business media phones, set:

   ```
   feature.usb.host.enabled="1"
   ```

3. Save the configuration file.

Disable the Headset Ports

Disable unused headset ports on the phone.

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

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

1. Open the configuration file.
2. Enable device parameter updates.

   ```
   device.set="1"
   ```

3. Disable the headset connection ports.

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

4. Save the configuration file.

Disable the PC port

Disable the unused PC port on 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Disable the computer connection port.

   ```
   device.net.etherModePC="0"
   device.net.etherModePC.set="1"
   ```

3. 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 801.2X EAP authentication methods:

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

- EAP-MD5

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

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-None - No authentication
   - EAP-TLS
   - EAP-PEAPv0-MSCHAPv2
   - EAP-PEAPv0-GTC
   - EAP-TTLS-MSCHAPv2
   - EAP-TTLS-GTC
   - EAP-FAST
   - EAP-MD5

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

5. If you set the 802.1X method as `EAP-FAST`, you can set the following parameters as well:

```
device.net.dot1x.eapFastInBandProv="<0> or <1>"
device.net.dot1x.eapFastInBandProv.set="1"
device.pacfile.data="<Optional PAC file name>"
device.pacfile.data.set="1"
device.pacfile.password="<Password for PAC file if
needed>"
device.pacfile.password.set="1"
```

6. Save the configuration file.

8 Configuring audio settings

Configure modifications to the default audio configurations to optimize the audio quality of your phones.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Automatic gain control

Automatic gain control (AGC) boosts the volume of near-end conference participants. AGC is enabled by default to ensure far-end audio clarity.

NOTE: You can't disable this feature. Changing the default settings may cause accessibility concerns for people who use audio augmentation assistive technology.

If you are running an application that also provides AGC through the software, Poly recommends that you disable the application AGC.

Enable AEC for Headsets

The default configuration enables acoustic echo cancellation (AEC) for both the handset and speakerphone. Enable AEC for connected Poly Bluetooth headsets to reduce echo during calls.

AEC includes the following features:

- Talk state detector: Determines whether the near-end user, far-end user, or both are speaking.
- Linear adaptive filter: Adaptively estimates the loudspeaker-to-microphone echo signal and subtracts that estimate from the microphone signal.
- Nonlinear processing: Suppresses any echo remaining after the linear adaptive filter.

1. Open the configuration file.
2. Enable AEC for headsets.

```
voice.aec.bt.hd.enable="1"
```

3. Save the configuration file.

Noise suppression

Poly phones offer multiple options to suppress background noise during calls. Some options are integrated into the phone itself, but you can configure others.

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

Poly NoiseBlock

The default configuration enables Poly NoiseBlock on Poly phones.

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

Disable Poly NoiseBlock

Disable Poly Noiseblock and Poly NoiseBlockAI on your phones.

Poly NoiseBlock automatically mutes the microphone when a user stops speaking. It reduces interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter.

1. Open the configuration file.
2. Disable Poly NoiseBlock.

```
voice.ns.hf.block="0"
```

3. Save the configuration file.

Enable Poly NoiseBlockAI

Enable Poly NoiseBlockAI on your phones.

Poly NoiseBlockAI suppresses background noise while a call participant actively speaks. It also reduces interruptions caused by common office sounds (keyboard tapping, shuffling papers, etc.) and background chatter. Call recipients hear only the intended speaker's voice.

NOTE: You can't enable both Poly NoiseBlock and Poly NoiseBlockAI at the same time. The same parameter configures both modes.

1. Open the configuration file.
2. Enable Poly NoiseBlockAI.

```
voice.ns.hf.block="2"
```

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, see the parameter reference topic(s) in the *Poly CCX 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, see the parameter reference topic(s) in the *Poly CCX 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, see the parameter reference topic(s) in the *Poly CCX 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.

Enable this setting to optimize CCX 600 phone performance while using a Polycom EagleEye Mini USB camera with Acoustic Fence.

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

For more information about VAD, see Voice Activity Detection parameters in the *Parameter Reference Guide*.

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 CCX Parameter Reference Guide*.

Comfort noise provides a minimal level of audio on the line to ensure callers that the call is still connected. You can add and adjust the level of comfort noise for speakerphone and headset calls.

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, see the parameter reference topic(s) in the *Poly CCX 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.

Audio codecs

Configure the audio codecs for your phones.

This section provides basic information for configuring audio codecs. For more information on configuring audio codecs, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide* .

Supported Audio Codec Specifications

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 8-1 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 α-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 8-1 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 256 Kbps 512 Kbps 705.6 Kbps 768 Kbps	132 Kbps 260 Kbps 516 Kbps 709.6 Kbps 772 Kbps	8 ksps 16 ksps 32 ksps 44.1 ksps 48 ksps	10 ms	3.5 kHz 7 kHz 14 kHz 20 kHz 22 kHz
All systems	Siren 7	SIREN7	16 Kbps 24 Kbps 32 Kbps	32 Kbps 40 Kbps 48 Kbps	16 ksps	20 ms	7 kHz
All systems	Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 ksps	20 ms	14 kHz
All systems	iLBC	RFC 3951	13.33 Kbps 15.2 Kbps	31.2 Kbps 24 Kbps	8 ksps	20 ms 30 ms	3.5 kHz
All systems	SILK	SILK	6 to 20 Kbps 7 to 25 Kbps 8 to 30 Kbps 12 to 40 Kbps	36 Kbps 41 Kbps 46 Kbps 56 Kbps	8 ksps 12 ksps 16 ksps 24 ksps	20 ms	3.5 kHz 5.2 kHz 7 kHz 11 kHz

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 8-2 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.G719.32kbps="<priority value>"
voice.codecPref.G719.48kbps="<priority value>"
voice.codecPref.G719.64kbps="<priority value>"
voice.codecPref.G722="<priority value>"
voice.codecPref.G7221.16kbps="<priority value>"
voice.codecPref.G7221.24kbps="<priority value>"
voice.codecPref.G7221.32kbps="<priority value>"
voice.codecPref.G7221_C.24kbps="<priority value>"
voice.codecPref.G7221_C.32kbps="<priority value>"
voice.codecPref.G7221_C.48kbps="<priority value>"
voice.codecPref.G729_AB="<priority value>"
voice.codecPref.iLBC.13_33kbps="<priority value>"
voice.codecPref.iLBC.15_2kbps="<priority value>"
voice.codecPref.Lin16.8ksps="<priority value>"
voice.codecPref.Lin16.16ksps="<priority value>"
voice.codecPref.Lin16.32ksps="<priority value>"
```

```
voice.codecPref.Lin16.44_1ksps="<priority value>"
voice.codecPref.Lin16.48ksps="<priority value>"
voice.codecPref.Opus="<priority value>"
voice.codecPref.SILK.8ksps="<priority value>"
voice.codecPref.SILK.12ksps="<priority value>"
voice.codecPref.SILK.16ksps="<priority value>"
voice.codecPref.SILK.24ksps="<priority value>"
voice.codecPref.Siren7.16kbps="<priority value>"
voice.codecPref.Siren7.24kbps="<priority value>"
voice.codecPref.Siren7.32kbps="<priority value>"
voice.codecPref.Siren14.24kbps="<priority value>"
voice.codecPref.Siren14.32kbps="<priority value>"
voice.codecPref.Siren14.48kbps="<priority value>"
voice.codecPref.Siren22.32kbps="<priority value>"
voice.codecPref.Siren22.48kbps="<priority value>"
voice.codecPref.Siren22.64kbps="<priority value>"
```

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.

9 Configuring Video Settings

Poly CCX 600 and CCX 700 business media phones support video calls.

NOTE: Poly CCX 600 business media phones require an optional Polycom EagleEye Mini USB camera to send video.

Camera Options

Configure the camera the phone uses for video calls.

Control where the **Camera** settings appear and whether users can access it without administrative permissions.

If your phone connects to a PTZ camera, you can configure several camera presets for the camera's position.

Disable Far End Camera Control

Disable Far End Camera Control (FECC) to stop far-end participants from controlling the framing and angle of the local camera.

FECC enables participants to adjust the pan, tilt, zoom (PTZ) of the camera. When disabled, only the meeting host can control the PTZ camera.

IMPORTANT: Configuring the following parameter(s) 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Disable FECC.

```
feature.fecc.enabled="0"
```

3. Save the configuration file.

Enable the Camera Button in the Main Menu

Enable the **Camera** button on the main menu, which enables users to control a connected pan, tilt, zoom (PTZ) camera.

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

1. Open the configuration file.

2. Enable the **Camera** button in the main menu.

```
homeScreen.camera.enable="1"
```

3. Save the configuration file.

Remove Camera Settings from the Basic Menu

By default, camera settings, including preset storage and modifications, are available under the **Basic** menu, which is available for all users. You can move camera settings to the **Advanced** menu so only administrators have access to them.

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

1. Open the configuration file.
2. Move camera settings to the **Advanced** menu.

```
video.camera.menuLocation="Advanced"
```

3. Save the configuration file.

Configure a Camera Home Preset

Configure the home preset for your pan, tilt, zoom (PTZ) camera.

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

1. Open the configuration file.
2. Enable the camera to move to its home position when it's idle.

```
video.camera.preset.home.uponIdle.enabled="1"
```

3. Set the number of minutes the camera remains idle before moving to its home position. The range in minutes is 0-3600.

```
video.camera.preset.home.uponIdle.delay="<# of
minutes>"
```

4. Set the pan coordinates for the home position. The value range is 0-1000.

```
video.camera.preset.home.pan="<x>"
```

5. Set the tilt coordinate for a camera home preset. The value range is from 0-1000.

```
video.camera.preset.home.tilt="<x>"
```

6. Set the zoom coordinate for a camera home preset. The value range is from 0-1000.

```
video.camera.preset.home.zoom="<x>"
```

7. Save the configuration file.

Configuring the Call Modes

Configure video-enabled phones to place audio-only or audio-video calls by default.

All outgoing calls on video-enabled phones start in audio-video mode. If you mute your video signal, the phone displays a video-muted image instead of the video feed. Audio-only calls don't transmit any video signal, but users can add video to the active audio-only call.

NOTE: Incoming video calls display video even when you set the system default to audio-only.

- **Set the Default Call Mode**: Change the default call mode for outgoing calls to audio-only calls.
- **Mute Video**: Start audio-video calls with muted video.
- **Enable the Audio Call Button**: Give users the option to place an audio-only call from the *Home* screen, when the phone places audio-video calls by default.
- **Retain Call Mode Preferences**: Enable the phone to remember the last call mode setting for the next outgoing call.

Set the Default Call Mode to Audio-Only

Configure your video-enabled phone to place audio-only calls by default.

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

In an audio-only call, you can add video to the call. You can mute video after you add it, but you can't turn it off.

1. Open the configuration file.
2. Set the default call mode to audio.

```
video.callMode.default="audio"
```

3. Save the configuration file.

Mute Video at the Start of Video Calls

Starting a call with muted video helps prevent sending video feed before all call participants are ready to appear on camera.

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

1. Open the configuration file.
2. Start the video transmission with muted video.

```
video.autoStartVideoTx="0"
```

3. Save the configuration file.

Enable the Audio Call Button

On phones set to place audio-video calls by default, add the **Audio Call** button to the *Home* screen so users can directly place an audio-only call.

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

1. Open the configuration file.
2. Enable the **Audio Call** button on the *Home* screen.

```
up.homeScreen.audioCall.enabled="1"
```

3. Save the configuration file.

Enable Call Mode Persistence

Configure the phone to maintain the last call mode setting (audio-only video) and use the same setting for the next call.

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

1. Open the configuration file.
2. Enable call mode persistence.

```
audioVideoToggle.callMode.persistent="1"
```

3. Save the configuration file.

10 Configuring call controls

You can configure calling features for the Poly phone once it's connected to your VoIP network.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Call hold

Enables users to pause activity on an active call so that they can use the phone for another task.

When an active call is placed on hold, a message displays informing the held party that they are on hold.

Poly phones use the preferred call holding protocols by default, and typically don't require additional configuration.

Configure call hold reminders

Configure the phone to send an audible alert after a call is on hold for a specified amount of time.

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

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 Transfer Directly to Voicemail

Configure an enhanced feature key (EFK) that enables users to transfer calls directly to another user's voicemail inbox. This can be helpful if the other user is unavailable and the incoming caller wants to leave a message for them.

1. Enable the EFK feature.

```
feature.enhancedFeatureKeys.enabled="1"
```

2. Configure the new softkey that enables users press to transfer the call to voicemail. Replace `x` with the desired softkey index value.

   This example configuration enables the softkey,*x*, and configures it for transferring the call. It displays when the user selects **Transfer** during an active call, and is labeled **Voicemail**.

```
softkey.x.enable="1"
softkey.x.use.transfer="1"
softkey.x.action="*<voicemail prefix>$P2N5$$Trefer$"
softkey.x.label="Voicemail"
softkey.x.insert="<available softkey position on
screen>"
```

3. Configure the enhanced feature used by the new softkey. This configures the screen where the user can enter the extension for the voicemail inbox's owner to complete the transfer. Replace `y` with the EFK index value.

```
efk.efkprompt.y.status="1"
efk.efkprompt.y.label="Voicemail Extension"
efk.efkprompt.y.type="numeric"
efk.efkprompt.y.userfeedback="visible"
efk.efkprompt.y.digitmatching="none"
```

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 CCX 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 CCX 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 CCX 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.

Limit call forwarding options

Simplify the call forwarding options so that call forwarding is either turned on or off.

This removes the options to forward calls when busy, when DND is active, or when there is no answer, so that Call Forwarding Always (CFA) is the only option when call forwarding is enabled on the phone.

1. Open the configuration file.
2. Limit the call forwarding options.

```
feature.forward.bypassTypeSelect"1"
```

3. 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.

Flexible Call Appearances

A number of features associate with flexible call appearances, including multiple line registrations, multiple line keys per registration, and multiple call appearances. Flexible line keys (FLK) support static busy lamp field (BLF) and enhanced feature keys (EFK).

The following table includes the following types of call appearances:

- **Registrations**: The maximum number of user registrations
- **Line Keys**: The maximum number of line keys
- **Line Keys Per Registration**: The maximum number of line keys per user registration
- **Calls Per Line Key**: The maximum number of concurrent calls per line key
- **Concurrent Calls (including Conference Legs)**: The runtime maximum number of concurrent calls, and the number of conference participants minus the conference initiator.

Table 10-1 Flexible Call Appearances

Phone Model	Registrations	Line Keys	Line keys Per Registration	Calls Per Line Key	Concurrent Calls
CCX 400	24	28	24	24	24 (2)
CCX 500	24	28	24	24	24 (2)
CCX 505	24	28	24	24	24 (2)
CCX 600	24	60	24	24	24 (2)
CCX 700	24	60	24	24	24 (2)

Using the Any Category

After you enable the line key assignment feature, the default category of a line key is **Any** instead of **Unassigned**. This enables the phone to display speed dials and other user-defined keys even when they aren't explicitly defined in the generated configuration file.

If there are unassigned functions after the phone processes its configuration file, the phone adds these functions one by one to blank line keys not explicitly categorized as **Unassigned** in the following order:

1. SIP Registrations
2. EFK
3. BLF
4. Presence
5. SpeedDial

Multiple Line Registrations

Poly phones can have multiple line registrations. When multiple registrations are available, users can select which registration to use for certain features, including which registration to use for outgoing calls or when initiating new instant messages.

Each registration requires an address or phone number.

NOTE: You must use a unique address or a phone number for each registration. Using the same address or phone number for multiple registrations might cause unexpected behavior.

CCX business media phones support a maximum of 34 registrations.

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

You can set the value for the `reg.x.callsPerLineKey` parameter to a value higher than `1`, for example, `3`. After you set the value to `3`, you can have three call appearances on line 1. By default, any additional incoming calls automatically go to voicemail.

If you set more than two call appearances, a call appearance counter displays at the top-right corner of the phone's screen.

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.

Switching Call Applications on CCX Phones

Configure the phone to switch between the OpenSIP call application and an enabled third-party call application.

The following table outlines the call applications users can switch to on each of the CCX phone models.

Table 10-2 Call Application Switching on CCX Business Media Phones

Phone Model	OpenSIP	Microsoft Teams	Zoom Phone
CCX 400	Supported	Supported	Supported
CCX 500	Supported	Supported	Supported
CCX 505	Supported	Supported	Not supported
CCX 600	Supported	Supported	Supported
CCX 700	Supported	Not Supported	Supported

Enable Call Application Switching

Configure CCX phones to switch to the Poly OpenSIP call application while the phone's base profile is set to Microsoft Teams.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot.

1. Open the configuration file.
2. Enable call application switching.

```
apps.android.appSwitcher.enabled="1"
```

3. Enable the phone to switch to the Poly OpenSIP call application.

```
apps.android.statusBar.UCS.enabled="1"
```

4. Enable the phone to switch to Microsoft Teams call application.

```
apps.android.appSwitcher.MSTeams.enabled="1"
```

5. Save the configuration file.

Configure Poly OpenSIP for Failover Calling

Configure your phone to offer a registered open SIP line as a backup calling method for third-party call application outages.

You must register at least one open SIP line on the phone.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot.

In the event that a third-party call application—set as the phone's base profile—can't place calls, users can switch to the Poly OpenSIP call application to place a call with a registered line.

1. Open the configuration file.
2. Enable call application switching.

```
apps.android.appSwitcher.enabled="1"
```

3. Display the navigation bar on third party applications.

```
apps.android.navBar.enabled="1"
```

4. Enable the phone to switch to the Poly OpenSIP call application.

```
apps.android.statusBar.UCS.enabled="1"
```

5. Enable the **Place a Call** button on the OpenSIP *Home* screen.

```
homeScreen.placeACall.enable="1"
```

6. Enable the phone to place SIP calls on the registered line.

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

7. 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 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.

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, see the parameter reference topic(s) in the *Poly CCX 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.

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.

Use network signaling for caller ID

Configure the phone to get caller identification information from network signaling.

By default, the phone checks an incoming call against the local contact directory for caller identification. If the phone finds a match, the matching contact's name displays. Otherwise, the phone displays the incoming phone number.

The phone can't pull caller ID information from an LDAP corporate directory integration.

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

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.

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 local call recording

Local call recording enables the phone to record audio calls to a connected USB device.

NOTE: Federal, state, and local laws may legally require that you notify some or all of the call parties when a call recording is in progress.

When users record their calls, the phone saves the recorded audio calls in WAV format and includes a date/time stamp. Users can then playback the recorded audio on the phone itself or a computer.

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

1. Open the configuration file.

2. Enable local call recording.

```
feature.callRecording.enabled="1"
```

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.

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.

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.

Busy Lamp Field Icons

The phone displays icons to indicate line status to users.

Table 10-3 BLF Icons

States	Line Icons
Monitored line is idle	
Monitored line is busy	
Monitored line is on hold	
Monitored line is unregistered	

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 an index number for the new resource. Use any unused positive integers. 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.

```
attendant.resourceList.x.type="<resource type>"
```

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

BLF and KSE are mutually exclusive. If you enable KSE, BLF is no longer available to monitor calls.

Key system emulation includes the following behavior:

- An audio notification plays on the phones in the user group when someone parks a call.
- A reminder tone continuously plays after a designated time interval if no one answers the call.
- There are no audio and reminder notifications for a self-parked call.
- The LED patterns and the line icons for a self-parked call are different from a call parked by other users in the group. This helps to differentiate between a self-parked call and a remote-parked call.
- The LED indicator turns solid red for a self-parked call and turns blinking red for a remote-parked call.

NOTE: Key system emulation is applicable to only the 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 server SIP URI>"
```

6. Specify an index number for the new BLF resource. Use any unused positive integers. 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. Enable the phone to display **Attendant Call Action** on the phone when you configure dynamic BLF on the phone.

```
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 resource's BLF index number.

    The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFReminderTone.inst.x.type="chord"
se.pat.misc.callParkBLFReminderTone.inst.x.value="cs4"
se.pat.misc.callParkBLFReminderTone.inst.x.param="0"
se.pat.misc.callParkBLFReminderTone.inst.x.atten="0"
```

13. **Optional:** Configure the reminder ringtone. Replace *x* with the resource's BLF index number.

    The following code block provides a ringtone configuration example. Configure your ringtone based on your deployment's requirements.

```
se.pat.misc.callParkBLFAudioNotification.inst.x.type="chord"
se.pat.misc.callParkBLFAudioNotification.inst.x.value="cs4"
se.pat.misc.callParkBLFAudioNotification.inst.x.param="0"
se.pat.misc.callParkBLFAudioNotification.inst.x.atten="0"
```

14. Save the configuration file.

Local digit map

The local digit map feature assists with off-hook dialing and helps the phone conform to a dial plan.

Digit maps consist of a single string or a list of strings. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of RFC 3435.

When dialing a number, the digit map behavior is based on the following:

- Any string of a digit map matches: The phone places the call automatically.
- No string matches: You can specify the phone's behavior.

- The number ends with **#**: You can specify the phone's behavior.

You can specify digit map timeout. This is the time between the caller dialing a number and the phone placing the call.

Configure a local digit map

Specify the digit map used for the dial plan.

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

The default digit map is as follows:

```
[2-9]11|0T|+011xxx.T|0[2-9]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. 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, see the parameter reference topic(s) in the *Poly CCX 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. 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, see the parameter reference topic(s) in the *Poly CCX 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.

11 Messaging

Poly phones support several methods to communicate using messaging in addition to making direct calls.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Set the URI for the voicemail server. The phone sends a SUBSCRIBE request when it boots up. Replace *x* with the desired line key value.

```
msg.mwi.x.subscribe="<voicemail server 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 Instant Messaging

Send and receive instant text messages through your phone.

Support for instant messaging varies by call server. Consult your SIP server partner to find out if it supports this feature.

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

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.

Group Paging with the Poly Control Panel

Configure the **Poly Control Panel** group paging functionality on Poly phones with third-party call applications that may not natively support paging.

Configure group paging in the **Poly Control Panel** to perform one of the following actions when the user selects the **Group Page** icon:

Enable group paging in the Poly Control Panel

Enable group paging in the **Poly Control Panel**.

When you enable this feature, the default configuration is that users can only send group pages in the **Poly Control Panel** to page group 1.

IMPORTANT: Configuring the following parameter(s) causes the phone to reboot.

1. Open the configuration file.
2. Enable group paging.

```
apps.android.appSwitcher.enabled="1"
```

3. Display group paging in the **Poly Control Panel**.

```
apps.android.appSwitcher.Paging.enabled="1"
```

4. Save the configuration file.

Configure group paging from the Poly Control Panel to a defined page group

Configure the phone so that when users select group paging in the **Poly Control Panel**, the phone opens the channel defined in the `ptt.defaultChannel` parameter.

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

1. Open the configuration file.
2. Display group paging in the **Poly Control Panel**.

```
apps.android.appSwitcher.Paging.enabled="1"
```

3. Configure the channel that the phone automatically opens when users select group paging from the **Poly Control Panel**.

```
ptt.defaultChannel="<group paging index>"
```

4. Save the configuration file.

Configure group paging from the Poly Control Panel to a user-selected page group

Configure the phone to display the *Group Page List* when a user selects group paging in the **Poly Control Panel**. The user must select a page group before the phone broadcasts the page to the selected group.

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

1. Open the configuration file.
2. Display group paging in the **Poly Control Panel**.

```
apps.android.appSwitcher.Paging.enabled="1"
```

3. Configure the phone to display the full list of group page channels when users select the group paging icon from the **Poly Control Panel**.

```
apps.android.appSwitcher.Paging.useDefaultChannel="0"
```

4. Save the configuration file.

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 CCX 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:** Add a label to a specific group. Repeat this parameter for each group label.

```
ptt.pageMode.group.x.label="<string>"
```

6. **Optional:** Specify the group the phone uses for emergency pages. The default is `25`.

```
ptt.pageMode.emergencyGroup="<group number>"
```

7. 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 emergency channel is 25.

```
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.

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.

Change the IP Multicast Address

Specify the IP multicast address for both PTT and group paging.

NOTE: The PTT and group paging features use an IP multicast address. If you want to change the default IP multicast address, make sure that the new address doesn't already have an official purpose as specified in the IPv4 Multicast Address Space Registry.

For more information on PTT and group paging multicast packets, see the *Polycom UC Software PTT/Group Paging Audio Packet Format Engineering Advisory 70568* at the Poly Online Support Center.

1. Open the configuration file.
2. Enter the new multicast IP address.

```
ptt.address="<IP address>"
```

3. Save the configuration file.

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.

12 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 line key 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 CCX 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.

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 CCX 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. Enable the phone to send a re-INVITE to the server when setting up a conference on a shared line.

```
call.shared.exposeAutoHolds="1"
```

4. 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, see the parameter reference topic(s) in the *Poly CCX 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 CCX 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>"
```

13 Configuring phone settings

Customize your phone using various applications and keysets.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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.

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, see the parameter reference topic(s) in the *Poly CCX 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:

- Shared lines don't support call server-based DND.
-
- If you enable call server-based DND, but don't turn it on with DND enabled on the phone, the **Do Not Disturb** message displays on the phone but incoming calls continue to ring.
- Call server-based DND disables local call forwarding and DND. However, if an incoming call doesn't route through the server, an audio alert may play on the phone.

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

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, see the parameter reference topic(s) in the *Poly CCX 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.

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.

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, see the parameter reference topic(s) in the *Poly CCX 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.

Microphone mute

Microphone mute is an embedded feature on your phone, and you can't configure or disable it. However, you can configure supporting features related to muting the microphone.

Enable microphone mute/unmute alert

Configure the phone to play a tone when a user mutes or unmutes the microphone.

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

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, see the parameter reference topic(s) in the *Poly CCX 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.

Disable the Poly Control Panel

Prevent users from accessing the **Poly Control Panel**.

The **Poly Control Panel** offers a shortcut for users to access Bluetooth settings and send group pages, if enabled. Disabling the **Poly Control Panel** doesn't prevent users from accessing these features.

1. Open the configuration file.
2. Disable user access to the Poly Control Panel.

```
apps.android.statusBar.enabled="0"
```

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.

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

Transmit levels are fixed according to the TIA/EIA-810-A standard.

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

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

Set any or all of these parameters for particular devices to enable the call volume to persist between calls.

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 CCX Parameter Reference Guide*.

DTMF tones are encoded in the Real-time Transport Protocol (RTP) stream by default. When you disable `tone.dtmf.viaRtp`, DTMF isn't encoded in the RTP stream.

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

Supported ring classes

The following table provides the available ring classes to create or assign ringtones.

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, see the parameter reference topic(s) in the *Poly CCX 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, see the parameter reference topic(s) in the *Poly CCX 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, see the parameter reference topic(s) in the *Poly CCX 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 registered line number.

   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, see the parameter reference topic(s) in the *Poly CCX 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`

Table 13-2 Sound Effect Pattern Instruction Types (continued)

Instruction	Definition	Example
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

Table 13-3 Call Progress Tones (continued)

Call Progress Pattern	Description
`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.
ringer2	Low Trill	Long single A3 Db3 major warble
ringer3	Low Double Trill	Short double A3 Db3 major warble
ringer4	Medium Trill	Long single C3 E3 major warble
ringer5	Medium Double Trill	Short double C3 E3 major warble
ringer6	High Trill	Long single warble 1
ringer7	High Double Trill	Short double warble 1
ringer8	Highest Trill	Long single Gb3 A4 major warble
ringer9	Highest Double Trill	Short double Gb3 A4 major warble
ringer10	Beeble	Short double E3 major
ringer11	Triplet	Short triple C3 E3 G3 major ramp
ringer12	Ringback-style	Short double ringback
ringer13	Low Trill Precedence	Long single A3 Db3 major warble Precedence
ringer14	Ring Splash	Splash
ringer15	N/A	Sampled audio file 1
ringer16	N/A	Sampled audio file 2
ringer17	N/A	Sampled audio file 3
ringer18	N/A	Sampled audio file 4
ringer19	N/A	Sampled audio file 5
ringer20	N/A	Sampled audio file 6
ringer21	N/A	Sampled audio file 7

Table 13-4 Ringtone Pattern Names (continued)

Parameter Name	Ringtone Name	Description
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
`callParkBLFAudioNotification`	call Park BLF Audio Notification	Cadence of parked call audio notification

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

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

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.

14 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 CCX Business Media Phone Parameter Reference Guide*

LED indicator pattern types

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

Table 14-1 LED Indicator Pattern Type

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

Set an LED pattern for active calls

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

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 CCX 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.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 CCX 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 CCX 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 CCX 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 CCX 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 CCX 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.

Enable the LED indicator for incoming calls

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

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 CCX Parameter Reference Guide*.

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

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

3. Save the configuration file.

Enable the LED indicator for missed calls on a call server

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

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

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

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 CCX Parameter Reference Guide*.

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

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

3. Save the configuration file.

Disable the Headset Key LED in Headset Memory Mode

Disable the flash pattern for the **Headset** key in Headset Memory Mode.

The **Headset** key flashes green for analog headsets and blue for USB headsets by default while in headset memory mode. Disable the key flashes if the user finds it distracting or bothersome.

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.

Disable Message Waiting Indicator in Power Saving Mode

Disable the message waiting indicator LED 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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Disable the message waiting indicator LED in power saving mode.

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

3. Save the configuration file.

15 Third-Party Servers

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

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Microsoft Exchange Integration

Integrate your OpenSIP phones with a Microsoft Exchange server to join meetings, make calls to Outlook contacts, and access Outlook calendars.

Configuring the Microsoft Exchange server

Configure the phone to use Microsoft Exchange server services on your phone.

These options are available once you connect to a Microsoft Exchange server:

- **Visual Voicemail**: Enable unified messaging and enable messages to play on the phone for each user.
- **Synchronizing Call Logs**: Enable the option to save calls logs to each user's conversation history in Outlook.
- **Outlook Address Book Search**: Enables users to search their Outlook contacts from the phone.

After you configure the Exchange server and features, users can log into their accounts in the **Basic** settings menu on the phones local interface. Users can also log in from the system web interface under **Settings** > **Applications** > **Exchange Sign in**.

Manually connect to a Microsoft Exchange server

Manually configure the phone to use a specific Microsoft Exchange server address.

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

By default, the phone uses autodiscovery to determine the Microsoft Exchange server address, which relies on local DNS records and login domain information. The phone prioritizes the setting in `exchange.server.url`, even if you keep autodiscovery enabled.

1. Open the configuration file.

2. Enter the Microsoft Server address.

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

3. Save the configuration file.

Enable Exchange voicemail

Configure your OpenSIP phone to access voicemails left for a Microsoft Exchange account.

Make sure you set `feature.exchangeCalendar.enabled="1"`.

1. Open the configuration file.
2. Enable Exchange Voicemail.

```
feature.exchangeVoiceMail.enabled="1"
```

3. Save the configuration file.

Enable Exchange contacts synchronization

Enable an OpenSIP phone to synchronize contacts and call log information with the logged in user's Exchange account.

Make sure you set `feature.exchangeCalendar.enabled="1"`.

1. Open the configuration file.
2. Enable the phone to synchronize Exchange contacts.

```
feature.exchangeContacts.enabled="1"
```

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.

Configure Exchange address book service

Enable an OpenSIP phone to search with the logged in user's Exchange address book.

Make sure you set `feature.exchangeCalendar.enabled="1"`.

1. Open the configuration file.
2. Enable the Exchange Skype for Business address book service.

```
feature.lync.abs.enabled="1"
```

3. **Optional:** Set the maximum number of contacts displayed when searching through the Exchange address book. The default is 12 results.

```
feature.lync.abs.maxResult="<integer>"
```

4. **Optional:** Set the phone's access to the Exchange address book to read only. This prevents users from making any changes to their address book from the phone.

```
feature.lync.abs.maxResult="<integer>"
```

5. Save the configuration file.

Microsoft Exchange calendar

For phones connected to an Exchange calendar, a **Calendar** icon displays on the phone *Home* screen.

Users can view and join Outlook calendar events directly from the phone. The phone displays the day and meeting view for scheduled events. However, the phone doesn't support the ability to schedule calendar events or view email from the phone.

Provision a Microsoft Exchange calendar

Enable a phone to access a Microsoft Exchange Calendar using a configuration file.

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

1. Open the configuration file.
2. Enable the Microsoft Exchange Calendar feature.

```
feature.exchangeCalendar.enabled="1"
```

3. Enter the Microsoft Exchange server URL.

```
exchange.server.url="<Exchange server address>"
```

4. Save the configuration file.

Enable Microsoft Exchange calendar using the system web interface

Use the system web interface to configure one phone at a time with the Microsoft Exchange calendar.

1. Log in to the system web interface using admin credentials.
2. Go to **Settings** > **Applications** > **Exchange Applications**.
3. In the **Exchange Calendar** field, select **Enable**.
4. Enter the exchange web services URL using a Microsoft Exchange Server URL.

   `https://<mail.com>/ews/exchange.asmx`
5. Select **Save**.
6. Select **Yes**.

   The **Calendar** icon displays on the phone screen.

Verify the Microsoft Exchange integration

After you configure your phone for Microsoft Exchange services, confirm that the services work properly.

Integrate the phone with the Microsoft Exchange server.

- On the phone's local interface, go to **Settings** > **Status** > **Diagnostics** > **Warnings**.

  If the phone doesn't display any warnings, then the services work correctly.

Configure calendar meeting details

Configure the information that displays in Exchange meeting details with the `exchange.meeting.show*` parameter.

Configure the following:

- **Subject**: Displayed by default. A brief description of the meeting's purpose.
- **Location**: Displayed by default. Where the meeting takes place.
- **Invitee(s)**: Displayed by default. A list of meeting participants.
- **Agenda/Notes**: Displayed by default. When you hide Agenda/Notes, a message indicates that the meeting is private.
- **Meeting Organizer**: Displayed by default. The organizer doesn't display for meetings displayed on the monitor.
- **Show More Actions**: Displayed by default. If users can dial multiple numbers to join a meeting, the **Show More Actions** option displays in **Meeting Details** to enable users to choose the dial-in number.
- **Show Only Current or Next**: Deactivated by default. When enabled, the phone only displays either the current or next meeting on the calendar.
- **Show Tomorrow**: Enabled by default. Allows the phone to display meetings scheduled for the next day as well as the current day.

NOTE: This process is optional, depending on the desired configuration.

1. Open the configuration file.
2. Hide the list of meeting attendees.

```
exchange.meeting.showAttendees="0"
```

3. Hide the **Agenda/Notes**.

```
exchange.meeting.showDescription="0"
```

4. Hide the meeting location.

```
exchange.meeting.showLocation="0"
```

5. Hide the **Show More Actions** option.

```
exchange.meeting.showMoreActions="0"
```

6. Configure the phone to display only the current or next meeting on the calendar.

```
exchange.meeting.showOnlyCurrentOrNext="0"
```

7. Hide the meeting organizer.

```
exchange.meeting.showOrganizer="0"
```

8. Hide meeting's subject.

```
exchange.meeting.showSubject="0"
```

9. Configure the phone to only show the current day's meetings on the calendar.

```
exchange.meeting.showTomorrow="0"
```

10. Save the configuration file.

Enable Calendar Month View

Enable the **Month View** softkey for users to retrieve calendar events for all the days in the month.

1. Open the configuration file.
2. Enable the **Month View** softkey.

```
calendar.monthView.enabled="1"
```

3. Save the configuration file.

Ribbon Communications Server

Ribbon Communications application server, also called EXPERiUS™ A2, provides full-featured, IP-based multimedia communications applications for business and consumers.

Deploy EXPERiUS A2 as a standalone server or in combination with a Ribbon Communications CONTiNUUM™ C20 server. Note that feature availability varies depending on your chosen deployment.

The following features are available for phones registered with the Ribbon Communications servers:

- **MADN-SCA**: A shared group feature that provides support for conference barge in, privacy, and remote call appearance. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 server.
- **Global Address Book**: The global address book (GAB) feature is a corporate directory application managed by the Ribbon Communications server.
- **Personal Address Book**: The personal address book (PAB) feature, managed by the Ribbon Communications server, allows multiple clients (phones, computer software) to read and modify a user's personal directory of contacts. When one client changes a contact, all other clients immediately receive a notification of the change by the Ribbon Communications server.
- **E.911**: Enhanced 911 services specific to Ribbon Communications C20 server implementation.

Multiple Appearance Directory Number - Single Call Appearance

Multiple appearance directory number-single call appearance (MADN-SCA) enables a group of users to share a single directory number that displays as a single line to each member of the group.

When you enable this feature on your users' phones, they can initiate or receive calls on this shared line. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 servers.

Only one call can be active on the MADN-SCA shared line at a time. When a call is in progress, any incoming calls to the line receive a busy tone.

Configure MADN-SCA

Configure MADN-SCA on a registered line.

Note the following:

- If you configure the line-specific parameter `reg.x.server.y.address`, you must also configure values in the line-specific parameter `reg.x.server.y.specialInterop`.
- If you configure the global parameter `voIpProt.server.x.address`, you must also configure values in the global parameter `voIpProt.server.x.specialInterop`.

- For all deployments, including Ribbon Communications, line-specific configuration parameters override global configuration parameters. If you set values in both line-specific and global parameters, line-specific parameters apply and global parameters don't apply.

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

1. Open the configuration file.
2. Configure the shared line. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

```
reg.x.type="shared"
reg.x.address="<registered line SIP URI>"
reg.x.server.y.address="<SIP server address>"
```

3. Limit the number of concurrent active calls allowed on the registered line. Replace *x* with the desired line key value.

```
reg.x.callsPerLineKey="1"
```

4. Specify the server-specify feature as `GENBAND`. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

```
reg.x.server.y.specialInterop="GENBAND"
```

5. **Optional:** Enable barge-in for the registered line. Replace *x* with the desired line key value.

```
reg.x.bargeInEnabled="1"
```

6. **Optional:** Enter the line's authentication credentials. Replace *x* with the desired line key value.

```
reg.x.auth.userId="<line authentication username>"
reg.x.auth.password="<line authentication password>"
```

7. **Optional:** Configure the SIP server's proxy server. Replace *x* with the desired line key value.

```
reg.x.outboundProxy.address="<SIP proxy server
address>"
reg.x.outboundProxy.address="<transport method for
SIP server>"
```

8. Save the configuration file.

Configuring Privacy on a MADN-SCA Line

Configure privacy settings for shared MADN-SCA lines.

When you set the line to `shared`, an incoming call alerts all the members of the group simultaneously, and any group member can answer it. On the server, you

can configure a privacy setting that determines if other members of the group can barge into the same call after another member answers it. You can also configure if members of the group can pick up a call on hold regardless of who put it on hold.

Optionally, configure star codes on the server that you can dial on the phone to toggle the privacy setting during a single active call. Star codes apply in the following scenarios:

- If you configure the line for privacy by default, users can use a star code to toggle privacy on or off during an active call. When the call ends, the line resets to privacy settings.
- If you configure the line on the server with privacy off, users can use a star code to toggle the privacy on during an active call. However, users can't toggle back to privacy off during the call. When the call ends, the line resets privacy to off.

Enable MADN-SCA Barge-In

Enable all users on a shared MADN-SCA line to barge-in on an active call if any of the other users on the line accept the call.

1. Open the configuration file.
2. Enable call barge-in on the MADN-SCA line. Replace the variable *x* with the line's registration index.

```
reg.x.bargeInEnabled="1"
```

3. Save the configuration file.

Enable Private Hold on MADN-SCA Shared Lines

Private hold enables users on a MADN-SCA 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) causes the phone to reboot. For more information, see the parameter reference topic(s) in the *Poly CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Enable private hold on the MADN-SCA shared line. Replace *x* with the registered line number.

```
reg.x.enablePvtHoldSoftKey="1"
```

3. Enable the phone to send a re-INVITE to the server when setting up a conference on a shared line.

```
call.shared.exposeAutoHolds="1"
```

4. Save the configuration file.

Configure the Global Address Book

Enable and configure the phone to use a Ribbon Communications global address book (GAB). Ribbon Communications GAB is a read-only global directory set up by an administrator and can co-exist with other corporate directories on the phone.

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

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

3. Configure the connection to the Ribbon Communications GAB server.

```
dir.corp.alt.address="<URL address for Ribbon GAB>"
dir.corp.alt.port="<port for Ribbon GAB>"
dir.corp.alt.user="<Ribbon GAB username>"
dir.corp.alt.password="<Ribbon GAB password>"
```

NOTE: You may not need to provide a port if you provide a full URL for the Ribbon Communications server.

4. Save the configuration file.

Configure the Personal Address Book

Enable and configure the phone to use a Ribbon Communications personal address book (PAB). The PAB enables users to read and modify a personal directory of contacts on their phone.

When users modify contact information using any soft client, desk phone, or mobile client registered to the same line, the change updates all other clients. The Ribbon Communications server then immediately notifies users of the change.

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

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

3. Enable the GENBANDSOPI protocol on the phone to get the PAB service from the Ribbon Communications server.

```
dir.local.serverFeatureControl.method="GENBANDSOPI"
```

4. Specify the phone line on which to enable the personal address book.

```
dir.local.serverFeatureControl.reg="<line key>"
```

5. **Optional:** Specify the maximum number of contacts available for the Ribbon Communications PAB contact directory.

   The default is `100`. The value range is 1 to 100.

```
dir.genband.local.contacts.maxSize="<max number of
contacts>"
```

6. Save the configuration file.

E.911 Location for Ribbon Communications

Enhanced 911 (E.911) is disabled by default in a Ribbon Communications environment. Users can still manually set their location for emergency services. You can configure a phone's location with a configuration file.

By default, users can make a 911 call on a locked phone, regardless of the call state, or when other features are in use. During an active 911 call, the call control option doesn't display, users can't use the hard keys to control a call, and DND and call forwarding don't display.

Manually Set the Phone's Location for Emergency Calls

Users can manually set their location for emergency calls on the phone's local interface.

Register the phone.

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

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.

BroadSoft BroadWorks server

Integrate your phone with BroadSoft BroadWorks R18 and BroadWorks R20 features.

Some BroadSoft features include:

- Anonymous call rejection
- Simultaneous Ring
- Line ID blocking
- BroadWorks Anywhere
- Remote Office
- BroadSoft Server-Based call forwarding

NOTE: You can't register lines with the BroadWorks R18 server and the R20 and later simultaneously. You must register all lines on the phone to the same BroadWorks server.

Authentication with BroadWorks XSP service interface

Some BroadSoft features require the phone to authenticate with the BroadWorks Xtended Service Platform (XSP) service interface. Configure your phones to use advanced features available on the BroadSoft BroadWorks server.

The phones support the following advanced BroadSoft features:

- BroadSoft Enhanced Call Park
- Executive-Assistant
- BroadSoft UC-One directory, favorites, and presence
- BroadSoft UC-One personal call control features

Authenticate 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.

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.

Polycom BroadSoft UC-One application

The Polycom BroadSoft UC-One application integrates with BroadSoft Enterprise Directory and BroadCloud services—a set of hosted services by BroadSoft.

The BroadSoft UC-One application provides the following features:

- **BroadSoft Directory**: Displays information for all users in the enterprise. For example, work and mobile phone numbers.
- **BroadSoft Self-Presence**: Displays the user's aggregated presence received from the BroadSoft Messaging Server (UMS) on the phone.
- **BroadCloud Presence**: Enables users to share presence information with the BroadTouch Business Communicator (BTBC) client application.

- **BroadCloud Favorites**: Enables users to mark contacts as favorites with the BroadTouch Business Communicator (BTBC) client application.

Enable 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 CCX 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.

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.

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 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 BroadWorks Call Decline on a Shared Line

Enable the phones to reject incoming calls on a shared line in a BroadSoft BroadWorks environment.

When enabled, a user can reject an incoming call on the shared line using the **Reject** softkey, preventing the call from ringing on all phones registered with the shared line.

1. Open the configuration file.
2. Enable call decline on shared lines in the BroadSoft BroadWorks environment.

```
call.shared.reject="1"
```

3. Save the configuration file.

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, see the parameter reference topic(s) in the *Poly CCX 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.

Flexible Seating

Flexible Seating enables a user of an assigned primary phone to simultaneously access a registered line as a guest from an alternate host phone.

The user's primary registration is active on the primary and host phone. Users can access the BroadSoft UC-One contact directory and favorites on the host phone, but the Poly contact directory and favorites aren't available.

NOTE: Flexible Seating differs from the hoteling feature in that it provides only the primary registration's label on the host phone without any synchronization of features or settings.

The following conditions apply to the Flexible Seating feature:

- The primary phone and host phone don't sync automatically, but you can manually sync the phones on the BroadSoft BroadWorks server.
- The phone configured for the host user can't accept incoming calls. The host user can make only emergency outgoing calls as defined by the BroadWorks server.
- With the Phone Lock enabled, the phone can't place outgoing calls to numbers defined in the authorized call list, except the emergency numbers set on the BroadWorks server.
- The host user account is a placeholder account that supports guest users.
- The guest user can't change the user password. You can change the host phone's user password from the system web interface at any time. You can change the host phone's user password from the phone screen only after the guest user logs out.

Flexible Seating doesn't support the following features:

- Hoteling
- Visitor Desk Phone (VDP)
- User Profile Feature
- Local Call Forwarding

- Local DND

On the BroadWorks server, you can set a period of time when the server automatically logs out a user from a phone in case a user doesn't log out.

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, see the parameter reference topic(s) in the *Poly CCX 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.

BroadSoft BroadWorks Configuration Tags

The following table shows the Poly parameters you can map to the corresponding BroadSoft tags.

Table 15-1 BroadSoft BroadWorks Configuration Tags

Poly Configuration Parameter	BroadSoft Tag
`hoteling.reg`	%BWHOTELINGLINE-x%
`hotelingMode.type`	%BWHOTELINGMODE-x%

Guest Profile PIN

You can configure a PIN for each guest profile, which enables users to access their guest profile on a host phone by providing their PIN.

Using a PIN prevents other users from logging into a guest phone without the phone password or guest PIN. The guest profile PIN takes precedence over the local phone password and the guest user must log out of the phone with the PIN before another user can log in with their password.

Executive-Assistant Lines

Enable the BroadSoft Executive-Assistant feature on lines registered with the BroadWorks R20 or later server and assign the lines as either an executive or an assistant.

NOTE: All corresponding executive and assistant lines must register to the same server.

After you enable the feature, users can set filters to control whether calls route to an assistant or the executive line first. Executives can also enable screening, which enables the executive's phone to display the incoming call notification for all filtered calls.

In addition, depending on the role you assign the user, an **Executive** or **Assistant** icon displays on the phone's home screen. You can also simplify the Executive and Assistant menus by adding or removing **Pick Call** and **Barge-in** softkeys from the menu.

The BroadWorks server allows the following configuration options:

- A private executive line with an assistant with a private line
- Shared executive line with an assistant with a private line
- Shared executive line with a shared line alias on the assistant's phone
  - You must configure the shared line as a shared location with the Executive Service on the BroadWorks server.
  - In this option, the main line registration is a private line for the assistant, and the secondary registration is a shared line for the executive.

Enhanced Feature Keys for Executive-Assistant Menus

You can create Enhanced Feature Keys (EFK) which allow users to quickly access the **Overview Executives** menu for assistants or the **Executive Settings** menu for executives.

You can create an **Executive** or **Assistant** line key, softkey, or speed dial that displays on the *Lines* screen.

- When a user presses the **Executive** EFK on the executive's phone, the **Executive Settings** menu displays.
- When a user presses the **Assistant** EFK on the assistant's phone, the **Overview Executives** menu displays.

Configure a line or softkey for this feature using the following EFK macros:

- Executive menu: `"$FExecutiveMenu$"`
- Assistant menu: `$FAssistantMenu$`

Configure a Phone for Executive or Assistant Lines

Configure two phones as either an executive phone or as an assistant phone for the BroadWorks Executive-Assistant feature.

In the BroadWorks Web Portal, you must enable the Executive Service for private and shared executive lines, and the Executive-Assistant Service for private and shared assistant lines. You must also authenticate the phone with the BroadSoft XSP service interface.

1. Open the configuration file.
2. Enable the BroadSoft Executive-Assistant feature on the phone.

```
feature.BSExecutiveAssistant.enabled="1"
```

3. Configure the registered line the phone uses for BroadSoft Executive-Assistant feature.

```
feature.BSExecutiveAssistant.regIndex="<line key value>"
```

4. **Optional:** If you're configuring an assistant phone, change its role. Phones default to the executive role.

```
feature.BSExecutiveAssistant.userRole="AssistantRole"
```

5. **Optional:** Remove the **Pick Call** and **Barge-in** softkeys from the Executive or Assistant menu options on the phone's home screen.

   If you're configuring an executive phone:

```
feature.BSExecutiveAssistant.SimplifiedExec.enabled="1"
```

   If you're configuring an assistant phone:

```
feature.BSExecutiveAssistant.SimplifiedAssistant.enabled="1"
```

6. Save the configuration file.

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.

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, see the parameter reference topic(s) in the *Poly CCX 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.

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.

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, see the parameter reference topic(s) in the *Poly CCX 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.

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 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.

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.

BroadSoft Server-Based call forwarding

The BroadSoft server forwards incoming calls instead of the phone forwarding incoming calls.

To enable server-based call forwarding, you must enable the feature on both the server and the registered phone. If you enable server-based call forwarding on one registration, it only affects that registration.

The phone doesn't forward calls if you enable server-based call forwarding and leave it inactive, even if a user presses the **Forward** softkey.

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

Enable 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, see the parameter reference topic(s) in the *Poly CCX 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.

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.

Enable uaCSTA on a Dedicated Line

You can configure only one User Agent Computer Supported Telecommunications Applications (uaCSTA) line on each phone.

When you configure phones for uaCSTA with a CSTA server, you can remotely control the phone and access phone services using a computer telephony integration (CTI) application on your computer.

Poly phones support two types of user agent configurations for CSTA:

To ensure CSTA works correctly, Poly recommends that you configure the CSTA line as the last among all registered lines on the phone.

- A dedicated line to control or monitor all the other lines on the phone.
- A single line to act as both SIP line and CSTA line.

Poly phones support the Minimum and Basic profiles compliant with “ECMA TR/087: Using CSTA for SIP Phone User Agents (uaCSTA).” For information, see ECMA international.

NOTE: Poly phones don't support the Network Reached event.

Poly supports the following CSTA services

- MonitorStart
- MonitorStop
- MakeCall Without Prompt
- AnswerCall
- ClearConnection
- DeflectCall in alerting state
- HoldCall
- RetrieveCall
- SingleStepTransferCall
- SnapshotDevice
- Conference Call
- Transfer Call
- ConsultationCall
- SetForwarding
- GetForwarding
- SetDoNotDisturb
- GetDoNotDisturb
- GetSwitchingFunctionDevices

Poly supports the following CSTA events:

- ServiceInitiated
- Originated
- Delivered
- Diverted
- Established
- ConnectionCleared
- Held
- Retrieved

- Failed
- Transferred
- BackInService
- OutOfService
- Conferenced
- SwitchingFunctionDevices

1. Open the configuration file.
2. Set the CSTA line registration. Replace *x* with the desired line key value. Replace *y* with the desired server key value.

```
reg.x.csta="1"
reg.x.server.y.specialInterop="CSTA"
```

When you correctly register a CSTA line on a Poly phone, the CSTA line displays on the phone with an icon  and the default label **CSTA**.

If you incorrectly register the CSTA line, an icon  shows that the line is unregistered.

NOTE: A CSTA-registered line has no functionality to users. If a user selects a CSTA line on the phone, a message displays stating that no action is available.

3. Save the configuration file.

16 Directories and contacts

Configure your phones to use a local contact directory, a corporate directory, or both.

Call logs stored in the **Missed Calls**, **Received Calls**, and **Placed Calls** call lists enable users to view phone events. Events include remote party identification, time and date of call, and call duration.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Local contact directory

Configure phones with a local contact directory and link contacts to speed dial buttons.

Set the maximum number of contacts in the local directory

Configure the maximum number of contacts the phones store.

Phones can store a maximum of 3000 contact entries in a contact directory file 4 MB or smaller.

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

1. Open the configuration file.
2. Enter the maximum number of contacts allowed in the local directory. The default value is 500 contacts.

```
dir.local.contacts.maxNum="<1 to 3000>"
dir.local.contacts.maxNum="<1 to 500>"
```

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. Open the configuration file.
2. Locate the XML directory file in the phone's software update folder.

   The default file name is `000000000000-directory~.xml`.
3. 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`
4. Save the configuration 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. Open the configuration file.
2. Locate the XML directory file in the provisioning folder.

   The default file name is `000000000000-directory~.xml`.
3. Remove the tilde (~) at the end of the file name.

   `000000000000-directory.xml`
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 CCX 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 16-1 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`.
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

Table 16-1 Contact Directory XML Elements (continued)

Element	Description	Permitted Values
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
up	User photo The contact's photo icon set by the `icons.x` parameter.	1 to 24

Configure When Directory Files Update

Enable the phone to download the global directory file more frequently.

By default, a phone that uses a global directory file updates only after it receives a checksync NOTIFY message from the server. When you enable this parameter, the phone also downloads the global directory file following a reboot, configuration change, or software update.

When the phone updates, the following events happen:

- The phone downloads the global directory (`000000000000-directory.xml`) and per-phone (*<MACaddress>*`-directory.xml`) directory files.
- The directory files merge with the phone's directory.
- The phone ignores changes to the global directory that conflict with the phone's personal directory.

NOTE: Setting the `hotelingMode.type` parameter to `2` or `3` overrides this parameter.

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 CCX 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.

Poly CCX business media phones can support up to 500 speed dial entries.

This example shows adding a speed dial to the main directory file `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="01-01-2023-01:01:0
```

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 .

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 CCX Parameter Reference Guide*.

Access to a corporate directory on the phone is read only. Phone users can't add or remove contacts to the corporate directory.

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.alt.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.

Securely store LDAP credentials

Enable multiple users to enter their LDAP user credentials directly in the phone to access the corporate (LDAP) directory and store those credentials on the phone.

Any LDAP credentials that users enter on the phone are encrypted and stored only on the phone. The credentials also persist after the phone restarts or reboots.

When you configure this feature for phones with BroadSoft Flexible Seating, the phones can store up to 50 user credentials. If the number of user credentials reaches 50, the phone removes the user who has the longest period of inactivity when additional users are added.

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 phone to accept user credentials on the local interface.

```
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

Call list elements and attributes

The following table describes each element and attribute that displays in the call log.

Table 16-2 Call List Elements and Attributes

Element	Description	Permitted Values
direction	Call direction with respect to the phone user.	In Out

Table 16-2 Call List Elements and Attributes (continued)

Element	Description	Permitted Values
disposition	Indicates what happened to the call.	Busy Forwarded Normal Partial Preempted Rejected RemotelyHandled Transferred
line	The line protocol.	H.323 SIP
startTime	The start time of the call. For example, 2010-01-05T12:38:05 in local time.	String
duration	The duration of the call, beginning when the call connects and ending when the call is terminates. For example, `PT1H10M59S`.	String
count	The number of consecutive missed and abandoned calls from a call destination.	Positive Integer
destination	The original destination of the call. This parameter designates the outgoing call destination. The local phone supplies the name initially from the name field of a local contact entry. Later, call signaling may update the name. Use this field for basic redial scenarios. For incoming calls, the called destination identifies the requested party. The requested party may be different than any of the parties that eventually connect. The destination may indicate a SIP URI, which is different from any SIP URI assigned to any lines on the phone.	Address
source	The source of the call (caller ID from the call recipient's perspective).	Address

Table 16-2 Call List Elements and Attributes (continued)

Element	Description	Permitted Values
connection	An array of connected parties in chronological order. As a call progresses, the connected party at the far end may change. For example, if the far end transfers the call to someone else. The connected element allows the phone to save the progression of connected parties for later use. All calls that contain a connected state must have at least one connection element created.	Address
finalDesination	The final connected party of a call forwarded or transferred to a third party.	Address

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.

17 Customizing your phone

Configure the phone to display various features, functions, and customization options.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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 `VVXLocalization` folder in your PVOS package.
2. Open the language file in a Unicode-compatible XML editor.
3. Edit the dictionary as desired.

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 CCX 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 AirPlay-certified devices. This setting overrides the setting in `system.name` when searching for the phone from AirPlay-certified devices.

```
content.airplayServer.name="<UTF-8 encoded string>"
```

4. **Optional:** Set a name specifically for Android and Windows devices. This setting overrides the setting in `system.name` when searching for the phone from Android or Windows devices.

```
content.wirelessDisplay.sink.name="<UTF-8 encoded
string>"
```

5. **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>"
```

6. Set the SIP URI registration/H.323 extension. Replace *x* with the desired line key value.

```
reg.x.address="<SIP URI / H.323 ID>"
```

7. 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>"
```

8. 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>"
```

9. 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.

Configure labels in the local interface

Configure the phone number and labels that display on the *Home* screen through the phone's local interface.

1. Select **Settings** > **Advanced** > **Administration Settings**.
2. Select **Home Screen Label**.

3. Select the **Type**.

   If you select **Custom** for the **Type**, enter a custom message to display in the **Label** field.

4. Choose a **Location** for the phone number or label to display.

5. Select **Save**.

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, see the parameter reference topic(s) in the *Poly CCX 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. **Optional:** Set the label so it displays below the date instead of at the top of the screen.

```
homeScreen.labelLocation="BelowDate"
```

4. 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.

Enable and configure the digital phone label

The digital phone label displays a custom message in the status bar. Enable the digital phone label and enter a brief message to display in the phone's status bar.

The message you enter for the digital phone label supports up to 14 digits. The phone supports letters, though it may truncate longer messages. The label is helpful for displaying the phone's number or other frequently contacted numbers on the *Home* screen.

1. Open the configuration file.
2. Enable the digital phone label.

```
lcl.status.LineInfoAtTop="1"
```

3. Enter the message used for the digital phone label.

```
lcl.status.LineInfoAtTopText="<string>"
```

4. 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 the time in a 12-hour clock format.

   The default displays the time in a 24-hour clock format.

```
lcl.datetime.time.24HourClock="0"
```

3. Configure the date to appear above the time display.

   The default displays the time above the date.

```
lcl.datetime.date.dateTop="1"
```

4. Save the configuration file.

Change the date format

Configure how the date displays on the phone screen.

1. Open the configuration file.
2. Configure how the day and date display on the phone.

   By default, phones display the day and date as "Thursday, 3 July" with a value of `D,dM`.

```
lcl.datetime.date.format="<date format string>"
```

Use the following table to choose values for the `lcl.datetime.date.format` parameter. The table shows values for Friday, August 20, 2019 as an example.

Table 17-1 Date Format Table

lcl.datetime.date.format	lcl.datetime.date.longformat	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

3. **Optional:** Change the day and month display the short format (Fri/Nov) instead of the default long format (Friday/November).

```
lcl.datetime.date.longFormat="0"
```

4. Save the configuration file.

Contact Support Menu

Enable the **Contact Support** menu to display contact information, such as contact hours, phone numbers, and other support information. Service providers can add support contact information.

Enable and Configure the Contact Support Menu

Enable and configure the **Contact Support** menu to display contact information.

1. Open the configuration file.
2. Enable the **Contact Support** menu.

```
ui.menu.helpAndSupport.contact.enabled="1"
```

NOTE: If you don't add information such as contact support hours or phone numbers, the **Contact Support** menu doesn't display even if you enable this parameter.

3. Save the configuration file.

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. And 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 Support Organization Hours and Contact Information

Add up to three entries for your support organization's hours of operation, email addresses, or URLs 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 phone numbers or two phone numbers and an email address or URL, for example.

3. Save the configuration file.

Add a Customer Logo

Customize the **Contact Support** menu by adding a company logo to the page.

Place the image file on the provisioning server.

The supported image file formats are:

- .bmp
- .jpg
- .jpeg
- .jpe
- .jfif
- .png

1. Open the configuration file.

2. Add a customer logo to the **Contact Support** menu:

```
ui.menu.helpAndSupport.contact.customerLogo="<image
filename>"
```

3. Save the configuration file.

Customize the QR Code

By default, the QR code links to overview and explainer videos about the Poly CCX business media phones, but you can also customize it to link to another resource.

1. Open the configuration file.
2. Customize the QR code.

```
ui.menu.helpAndSupport.contact.help.QrCode_URL="<QR
Code URL>"
ui.menu.helpAndSupport.contact.help.QrCode_Title="<QR
Code Title>"
```

3. Save the configuration file.

Set a Preferred Home Screen

Configure the page that displays as the phone's *Home* screen.

By default, the phone's *Home* screen displays the time, date, and icons to access **Settings** and to place a call. Depending on the phone's configuration, it may also display icons to forward calls, enable DND, and access messages.

1. Open the configuration file.
2. Set the phone's preferred *Home* screen.
   - `default` (Default) - *Home* screen
   - `line` - *Lines* screen
   - `meeting` - *Meetings* screen

```
feature.preferredHomeScreen="<value>"
```

3. Save the configuration file.

Set Up a Custom Background

Replace the phone's and the expansion module's default background image with a custom image or import multiple images that users can select from.

Poly phones support `.jpeg`, `.bmp`, and `.png` image file formats. The phone doesn't support progressive/multi-scan `.jpeg` images.

The custom background displays behind the time, date, and line and key labels on the *Home* screen. The phone looks for custom background image from a folder in your network.

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

1. Open the configuration file.
2. Enable the phone to use a custom background.

```
bg.background.enabled="1"
```

```
bg.color.selection="2,1"
```

3. 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>"
```

```
bg.color.bm.1.em.name="<custom background URL>"
```

Refer to the following table for the maximum image size supported for each phone model.

Table 17-2 Maximum Phone Screen Image Size

Phone	Screen Size (px)
CCX 400	720 × 1280
CCX 500	720 × 1280
CCX 505	720 × 1280
CCX 600	1024 × 600
CCX 700	1024 × 600

4. Save the configuration file.

Configure a Line Registration Key Icon

Configure your phone to display custom icons for registered lines or user photos for contacts in the local contact directory and favorites on the *Home* screen.

Poly recommends uploading `.png` images that are 106 × 106 pixels with a size of 100 KB or smaller. You can upload images as large as 200 × 200 pixels, however, the phone automatically scales the icons to 106 × 106 pixels.

NOTE: The phone only supports `.png` image files. It doesn't support other image filetypes, such as `.jpg`, `.tiff`, `.bmp`, `.webp`, and `.gif`.

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

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

NOTE: Make sure that the icons configured and distributed through PVOS don't violate any Intellectual Property rights.

1. Open the configuration file.
2. Define the line registration key icon by mapping it to a `.png` image file in your FTP or provisioning server. Replace *y* with the icon index number.

```
icons.y="<icon filename or URL>"
```

   The first icon you define is `icons.1`. Define subsequent icons with the next available index number: the second and third icons you define are `icons.2` and `icons.3`, respectively.

3. Assign the icon to a line registration. Replace *x* with the desired line key value.

```
reg.x.icon="icon<y>"
```

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

1. Open the configuration file.
2. Disable the digital picture frame feature.

   ```
   feature.pictureFrame.enabled="0"
   ```

3. Save the configuration file.

Defining the Phone Key Layout

The following figures and tables show the default key layouts for the CCX Business Media Phones.

You can define certain hard key functions using parameters in the configuration files. See Key Mapping Parameter on page 221.

CCX 400 Business Media Phone Key Layout

The following figure and table show the available phone key functions.

Figure 17-1 CCX 400 Phone Key Layout

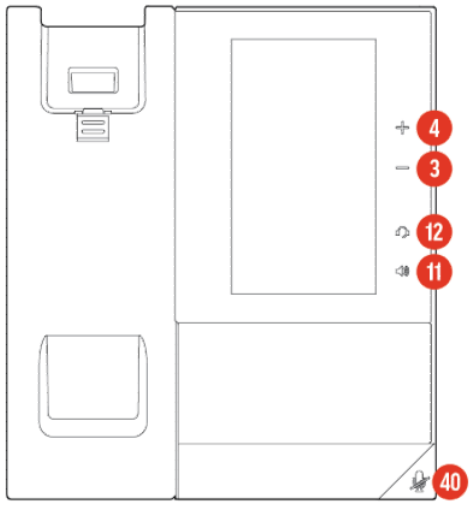

Table 17-3 CCX 400 Key Functions

Key ID	Function
3	VolDown
4	VolUp
11	Handsfree
12	Headset
40	MicMute

CCX 500 and CCX 505 Business Media Phones Key Layout

The following figure and table show the available phone key functions.

Figure 17-2 CCX 500 and CCX 505 Phone Key Layout

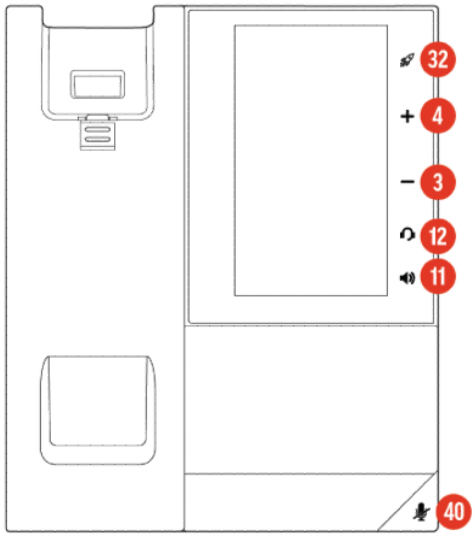

Table 17-4 CCX 500 and CCX 505 Key Functions

Key ID	Function
3	VolDown
4	VolUp
11	Handsfree
12	Headset
32	TeamsHome or Null NOTE: For CCX phones showing the Teams icon, when in the Microsoft Teams base profile, the default function is TeamsHome. For all other CCX phones, not showing the Teams icon, the default function is Null.
40	MicMute

CCX 600 and CCX 700 Business Media Phones Key Layout

The following figure and table show the available phone key functions.

Figure 17-3 CCX 600 and CCX 700 Phone Key Layout

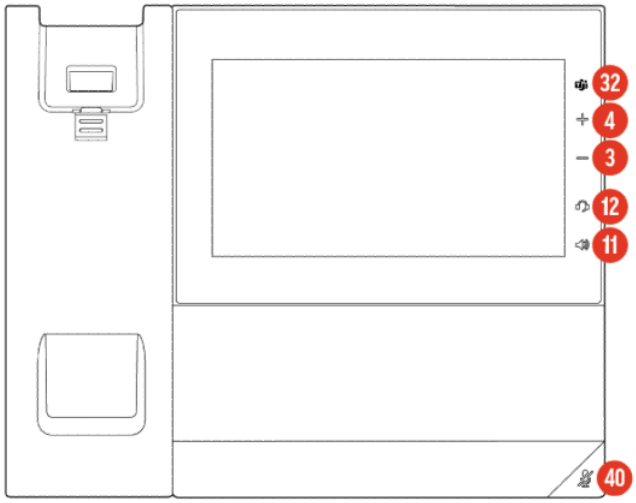

Table 17-5 CCX 600 and CCX 700 Key Functions

Key ID	Function
3	VolDown
4	VolUp
11	Handsfree
12	Headset
32	TeamsHome or Null NOTE: For CCX phones showing the Teams icon, when in the Microsoft Teams base profile, the default function is TeamsHome. For all other CCX phones, not showing the Teams icon, the default function is Null.

Table 17-5 CCX 600 and CCX 700 Key Functions (continued)

Key ID	Function
40	MicMute

Mapping Internal Key Functions

The following table shows a complete list of internal key functions for improved feature keys and hard key mappings.

Note the following guidelines:

- The **Function** value is case-sensitive.
- Some functions depend on the call state. Generally, if the softkey displays on a call screen, the softkey function is executable.
- Some functions need you to enable the feature. For example, the BuddyStatus and MyStatus soft keys require you to enable the presence feature.
- You don't need to enable the enhanced feature key feature to execute hard key remappings. This includes the speed dial function on older platforms. On newer platforms, use line key functions.

Table 17-6 Key Labels and Internal Functions

Function	Description
ACDLogin	Log in to Automatic Call Distribution.
ACDLogout	Log out from Automatic Call Distribution.
Answer	Answer an incoming call. This function applies to call screen only.
ArrowDown	Move arrow down.
ArrowLeft	Move arrow left.
ArrowRight	Move arrow right.
ArrowUp	Move arrow up.
BargeIn	Barge In to show appearances. 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.

Table 17-6 Key Labels and Internal Functions (continued)

Function	Description
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.
Delete	Delete the selected item.
DeviceSettings	Opens the phone's Settings menu when in the Microsoft Teams base profile.
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
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	Do Not Disturb menu
EnterRecord	Enter a call record. This function applies to call screen only.
Exit	Exit existing menu. This function applies to the Menu only.
GAB	Displays Ribbon communications Global Address Book.
GroupPickup	Group call pick-up on the phone.
Handsfree	Use handsfree.

Table 17-6 Key Labels and Internal Functions (continued)

Function	Description
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.
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
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	Disables key functionality.
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.

Table 17-6 Key Labels and Internal Functions (continued)

Function	Description
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	Set the available status for server-based Automatic Call Distribution agent.
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$".
ServerACDAgentAfterCallWork	Set the after-call work status for server-based Automatic Call Distribution agent. Example: softkey.1.action="$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
TeamsHome	Returns to the Microsoft Teams Home screen when in the Microsoft Teams base profile.

Table 17-6 Key Labels and Internal Functions (continued)

Function	Description
TeamsSettings	Opens the Microsoft Teams Settings menu when in the Microsoft Teams base profile.
Transfer	Transfer a call. This function applies to call screen only.
UCOneDir	Displays the UCOne directory.
VoiceMail	Displays voicemail messages for a registration line. This function must have a prefixed line index.

Key Mapping Parameter

The following parameter enables you to change the default functions of your phone's keypad keys. This process is called remapping.

If you want to change the default function of a key, you must specify the key you want to change and a new function for the key.

- For a list of products and their model codes, see Poly CCX phones model numbers on page 2.
- To find the key number, location of the key on each phone model, and default key functions, see Defining the Phone Key Layout on page 214.
- For a list of parameter values you can assign as functions to a phone key, see Mapping Internal Key Functions on page 217.

⚠ **CAUTION:** Poly doesn't recommend remapping or changing the default functions of the keys on your phone.

`key.x.function.prim`

`x` is the Key ID for the relevant phone, and `function` is the function name. For a list of functions, see Mapping Internal Key Functions on page 217. For a list of your phone's Key IDs, see one of the following:

- CCX 400 Business Media Phone Key Layout on page 214
- CCX 500 and CCX 505 Business Media Phones Key Layout on page 215
- CCX 600 and CCX 700 Business Media Phones Key Layout on page 216

For example, to disable the handsfree button on your phone, use the following parameter: `key.11.function.prim="Null"`.

CAUTION: Changing the parameter causes the system to restart.

18 Poly CCX EM60 expansion module

The Poly CCX EM60 expansion module is a console supported on several CCX business media phones that enables you to add additional lines to your phone.

NOTE: CCX 400 and CCX 500 phones don't support expansion modules.

Each CCX EM60 expansion module supports the following features:

- 5" color LCD display
- Three pages with twenty line keys each, for a total of sixty lines configurable as Teams presence, OpenSIP line registrations, call appearances, speed dials, Direct Station Select (DSS), or Busy Lamp Field (BLF)
- Dual-color (red or green) illuminated LEDs for line status information per key
- One USB 2.0 (Type-A) port
- One USB 2.0 (Type-C) port
- Supports one expansion module per CCX phone

IMPORTANT: USB headsets are not supported on CCX EM60 expansion modules. Bluetooth and RJ-9 headsets are supported.

Poly CCX EM60 expansion module hardware

The following figure displays the hardware features on CCX EM60 expansion modules. The table lists each feature numbered in the figure.

Figure 18-1 Poly CCX EM60 hardware features

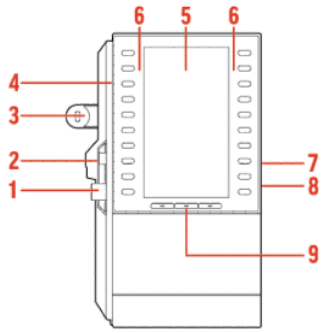

Table 18-1 Poly CCX EM60 hardware features reference callouts

Reference Number	Feature	Feature Description
1	USB-A plug	Connects the USB-A plug on the expansion module into the USB-A port on the side of a CCX phone

Table 18-1 Poly CCX EM60 hardware features reference callouts (continued)

Reference Number	Feature	Feature Description
2	USB-C plug	Connects the USB-C plug on the expansion module into the USB-C port on the side of a CCX phone
3	Locking tab	Connects the expansion module to a CCX phone
4	Line keys	Configured as line registration, call appearance, speed dial, Direct Station Selection (DSS), or busy lamp field (BLF) keys
5	Color display	A 5" color LCD screen with a backlight to view contacts and speed dials
6	LED indicators	Illuminates in green or red to provide line status information
7	USB-C port	The CCX EM60 expansion module includes one USB-C port reserved for future use
8	USB-A port	The CCX EM60 expansion module includes one USB-A port reserved for future use
9	Page keys	Three page keys to manage contacts

IMPORTANT: Ensure that you connect the CCX EM60 expansion module to the phone correctly by fully inserting the USB-A and USB-C plugs into the USB-A and USB-C ports on the phone. Use the locking tab to secure the expansion module to the phone, and use the correct stand to match the phone model.

Compatible base profiles and phone models

The following table lists the base profiles and phone models compatible with the CCX EM60 and provides the number of expansion modules that are supported.

Table 18-2 Base profile and phone model compatibility with a CCX EM60

Phone model	Generic	Microsoft Teams	Microsoft USB Phone	Zoom Phone	8x8 Work	Dialpad
CCX 505	1	1	Not supported	Not supported	Not supported	Not supported
CCX 600	1	1	Not supported	Not supported	Not supported	Not supported
CCX 700	1	Not supported	Not supported	Not supported	Not supported	Not supported

CCX power usage

CCX business media phones use more power when you connect an expansion module.

Table 18-3 Power usage without an EM60

Model	Idle	In Call
CCX 505	2.8 W	8 W
CCX 600	5.8 W	11 W
CCX 700	7.6 W	13 W

Table 18-4 Power usage with 1 EM60

Model	Idle	In Call
CCX 505	5 W	10.2 W
CCX 600	8 W	13.2 W
CCX 700	9.8 W	15.2 W

CCX PoE classes do not change when an EM60 is connected:

- CCX 505: PoE Class 0
- CCX 600: PoE Class 4
- CCX 700: PoE Class 4

The maximum power output from the EM60 USB ports is:

- USB-C: 2.5 W, 0.5 A
- USB-A: 0.5 W, 0.1 A

Poly CCX EM60 expansion module power limitations

Poly recommends using the CCX EM60 external AC adapter (5 VDC/3 A) for all installations (sold separately).

IMPORTANT: Connect external power to the CCX EM60 expansion module and not the host CCX phone.

When a power supply isn't directly connected to the CCX EM60, the following limitations apply:

- Hardware revisions of CCX 600 and CCX 700 phones manufactured before November 2022 (revisions A through O) do not support the use of an EM60.

TIP: You can find the hardware revision number on the white label on the back of your phone.

- CCX 505, CCX 600, and CCX 700 phones do not provide power to the EM60's USB-A port regardless of the CCX's manufacturing date or revision.

Table 18-5 CCX EM60 power supply part numbers

Part number	Part name
86H66AA#ABG	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-AUST
86H66AA#AC4	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-BRZL
86H66AA#ABB	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-EURO
86H66AA#ACJ	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-INDIA
86H66AA#ABJ	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-JPN2
86H66AA#AB1	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-KOR
86H66AA#ABM	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-LTNA
86H66AA#AB2	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-PRC
86H66AA#ABU	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-UK
86H66AA#ABA	Poly Edge E100-450 CCX 350 EM60 Power Supply - 5V/3A-US

Poly CCX EM60 expansion module line keys

The line keys on CCX phones and expansion modules are numbered sequentially, and the line key numbering on an expansion module depends on how many lines the phone supports and the base profile that you use.

In the Generic base profile, indexing depends on your preferred *Home* screen selection.

In the Microsoft Teams base profile, the expansion module line keys display contacts only, and you manage indexing using the Microsoft Teams application.

Configure preferred home screen using a configuration file

Configure your preferred Home screen to determine the line key allocation on your phone and expansion module using the configuration file.

1. Open the configuration file.
2. Configure the required page view using one of the following parameters:

```
feature.preferredHomeScreen="default"
```

```
feature.preferredHomeScreen="line"
```

```
feature.preferredHomeScreen="meeting"
```

3. Save the configuration file.

Configure preferred home screen using the local interface

Configure your preferred Home screen to determine the line key allocation on your phone and expansion module using the local interface.

1. On the device, go to **Settings** > **Basic** > **Preferences** > **Home Page**.

2. Choose one of the following:
   - Default
   - Line View
   - Meeting

Line key distribution scenarios

When you use the Generic base profile, line key allocation occurs in one of three modes, depending on your preferred *Home* screen selection.

Default view

- The *Lines* page is removed completely and is no longer available by swiping.
- Swiping the line keys at the bottom of the page is disabled.
- On CCX 505 phones, line keys at the bottom of the screen show indexes 1 to 3, and indexing on the expansion module starts at index 4.
- On CCX 600 and CCX 700 phones, line keys at the bottom of the screen show indexes 1 to 5, and indexing on the expansion module starts at index 6.

Line view

- Line key page 1 remains on the host phone, and line keys from the CCX phone's virtual line key pages 2 to 4 move to the expansion module.
- On CCX 505 phones, lines keys at the bottom of the screen show indexes 1 to 7, and indexing on the expansion module starts at index 8.
- On CCX 600 and CCX 700 phones, line keys at the bottom of the screen show indexes 1 to 15, and indexing on the expansion module starts at index 16.
- You can swipe from **Line** view to **Default** view.

Meeting view

- The *Lines* page is removed completely and is no longer available by swiping.
- Line key index 1 starts on the expansion module.
- You can swipe from **Meeting** view to **Default** view.

19 Phone Maintenance

Perform system management and maintenance tasks on your phone and upgrade the software.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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 CCX 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 CCX 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 CCX models 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 CCX 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 Poly CCX 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
- Zoom phone (CCX)
- 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)

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 CCX Parameter Reference Guide*.

1. Open the configuration file.
2. Enable user-controlled software updates.

```
prov.usercontrol.enabled="1"
```

3. 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"
```

4. **Optional:** Adjust the postponement duration using the HH:MM format.

   The default is `02:00` (2 hours).

```
prov.usercontrol.postponeTime="<HH:MM>"
```

5. 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:
   - Poly CCX 400: `3111-49700-001.sip.ld`
   - Poly CCX 500: `3111-49710-001.sip.ld`
   - Poly CCX 505: `3111-49730-001.sip.ld`
   - Poly CCX 600: `3111-49770-001.sip.ld`
   - Poly CCX 700: `3111-49740.001.sip.ld`
4. Insert the USB flash drive into the USB port.

   The phone detects the flash drive automatically.
5. Enter the administrator password.

   The phone starts the update within 30 seconds of entering the correct administrator password.

   The system may reboot several times during the update. The update is complete when the indicator lights stop blinking and the *Home* screen displays.

Updating PVOS with Windows Device Manager

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

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

Configure Windows to Update PVOS via Device Manager

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

1. On your Windows computer, open the **Registry Editor** (`regedit.exe`).

NOTE: Windows may prompt you asking if you want to make changes to your computer before it opens **Registry Editor**. Accept the prompt to proceed.

2. Go to `HKLM\SOFTWARE\Microsoft\`.

   `HKLM` may also display as `HKEY_LOCAL_MACHINE`.

3. Create the following subkeys: `\DriverFlighting\Partner\`.
4. Under the `\Partner` subkey, create a string named `TargetRing` and enter `Drivers` as the value.
5. Close the **Registry Editor**.

Update PVOS Using a Windows Computer

Update your phone in USB phone mode (USB optimized) using the connected Windows computer.

Make sure that the phone is in USB phone mode, powered on, and connected to a computer with the latest Windows updates. Make sure you configure your computer to update your phone with **Device Manager**.

1. On the computer, open **Device Manager**.
2. Locate the connected Poly phone as a device.

TIP: The phone may display in the following locations within **Device Manager**:

- `Other devices\`
- `Universal Serial Bus controllers\Other\`

3. Right-click the phone entry and select **Update Driver** > **Search Automatically for updated driver software**.

NOTE: This process may take some time.

4. Select **Finish** to begin updating the phone.

Disable PVOS Updates through Windows

Prevent the phone from updating through Windows **Device Manager** in USB phone mode.

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

NOTE: You can still update PVOS using the system web interface or a USB flash drive.

1. Open the configuration file.

2. Disable PVOS updates through Windows **Device Manager**.

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

3. Save the configuration file.

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.

Factory reset the phone at power-up

If your phone isn't performing optimally and continuing to restart, factory reset the phone while it is powering up.

1. Disconnect the power, then reconnect power to the Poly phone.
2. Do one of the following:
   - On CCX 400 phones, as soon as the message waiting light turns red, press and hold all four corners of the screen simultaneously.
   - On CCX 500, CCX 505, CCX 600, CCX 700 phones, as soon as the Poly logo displays for the second time, press and hold all four corners of the screen simultaneously.
3. Release when the Mute key illuminates and cycles through several colors.

   The phone restarts and begins the factory reset process.

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.

20 Monitoring the phones

Poly phones have several features that enable you to monitor the phone's performance and usage.

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

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 20-1 Secondary Device Details

Bluetooth Headset	USB Headset	Expansion Module	PC Port	Polycom EagleEye Mini USB Camera
• 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	• Connection Type • Display Name • Peripheral Type • Power Source • Software Version • 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

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 CCX 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 CCX 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.

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 20-2 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 CCX 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.

21 Troubleshooting

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

Most administrative tasks use a configuration file to set up your phones. Download all configuration files needed from Poly Lens. For information on using different configuration methods, see Methods for configuring phones on page 3 .

Record Your Phone's Version Information

Record your phone's version information and save it in a safe place. You may need it when contacting technical support.

1. Go to **Settings** > **Status** > **System Information**.
2. In the **System Information** screen, record the following:
   - Model(s)
   - Updater signature
   - Version
   - Platform

Capturing the Phone's Screen

Capture the phone's current screen as a saved image on your computer.

This can be helpful when explaining a problem or providing instructions.

Enable Screen Capture

Enable screen capture and the **Screen Capture** option in the **Basic** menu.

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

1. Open the configuration file.
2. Enable the screen capture feature.

```
up.screenCapture.value="1"
```

3. Enable the **Screen Capture** option in the **Basic** menu.

```
up.screenCapture.enabled="1"
```

4. Save the configuration file.

Capture the Phone's Screen

Capture and save a screenshot of the phone's display.

Before you capture the phone's screen, locate and record the phone's IP address at **Status** > **Platform** > **Phone** > **IP Address**.

1. On the device, go to **Settings** > **Basic** > **Preferences** > **Screen Capture** and select **Enabled**.

> **NOTE:** You must repeat this step each time the device restarts or reboots.

2. Set the phone to the screen you want to capture.
3. In a web browser, enter `https://<phoneIPaddress>/captureScreen`.
4. Enter the username `Polycom` and the phone's current administrator password.

   The web browser displays an image showing the phone's current screen. You can save the image as a `.bmp` or `.jpg` file.

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 CCX Business Media Phone Parameter Reference Guide* .

Configuring Log Files

Configure how the phone creates log files.

Log file names use the following format: `[MAC address]-[Type of log].log`. For example, if the MAC address of your phone is `0004f2203b0`, the 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 21-1 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** > **View & Download Logs** > **Audit**.

Retrieve Logs from the Support Information Package

Export the **Support Information Package** (`.tar` file) using the system web interface.

The support information package includes the following log files:

- PBU file
- App log file
- Boot log file
- Audit log file

1. Log in to the system web interface as an administrator.
2. Go to **Diagnostics** > **Download Support Information Package** and download the support information package.
3. On your computer, unzip the `.tar` file to view the log files.

View the Phone's Status

Troubleshoot phone issues by viewing the phone's **Status** menu.

1. Go to **Settings** > **Status** and select a status menu item.

2. View the following information:

Table 21-2 Menu Information

Menu Item	Available Information
System Information	• Model • Part Number • Platform (Profile) • MAC Address • Wi-Fi MAC Address (on supported models) • Bluetooth MAC Address (on supported models) • IP Address • Version • Updater Signature • System Name
Platform	• Phone's serial number or MAC address • Current IP address • Updater version • Application version • Names of the configuration files in use • Address of the provisioning server
Network	• TCP/IP Setting • Ethernet port speed • Connectivity status of the PC port (if it exists) • Statistics on packets sent and received since last boot • Last time the phone rebooted • Call Statistics showing packets sent and received on the last call
Lines	• Detailed status of each of the phone's configured lines
Diagnostics	• Hardware tests to verify correct operation of the microphone, speaker, handset, and third-party headset, if present • Hardware tests to verify correct operation of the microphones and speaker • Tests to verify proper functioning of the phone keys • List of the functions assigned to each of the phone keys • Real-time graphs for CPU, network, and memory use
Licenses	Reports licenses installed on the phone.
Location Information	Reports the phone's location information if it's available.

Table 21-2 Menu Information (continued)

Menu Item	Available Information
Calendar	• Reports the calendar server, domain, user, and reminder status. • Provides an option to disconnect from the calendar server.

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>-update-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 5.
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** > **Status** > **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
- **Touch Screen Diagnostics**: Test the touchscreen response
- **Brightness Diagnostics**: Test the screen brightness
- **LED Diagnostics**: Test the LEDs

Perform Network Diagnostics

You can use ping and traceroute to troubleshoot network connectivity problems.

1. Go to **Settings** > **Status** > **Diagnostics** > **Network**.
2. Choose one of the following:
   - **Ping**
   - **Trace Route**
3. Enter a URL or IP address.
4. Press **Start**.

Configure Remote Packet Capture

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

The phone generates core files when errors occur by default.

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.

Error messages

The phone displays messages that describe any errors it encounters during operation.

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 21-3 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.
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 21-4 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.
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 21-5 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.
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.

Table 21-5 Network Authentication Failure Error Codes (continued)

Event Code	Description	Notes
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.

Power and start-up issues

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

Table 21-6 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.

Screen and system access issues

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

Table 21-7 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**).

Calling issues

The following table provides possible solutions to common issues.

Table 21-8 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.

Table 21-8 Calling Issues (continued)

Issue	Cause and Possible Solution
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.

Display issues

The following table provides tips for resolving display screen issues.

Table 21-9 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.

Audio Issues

The following table describes possible solutions to audio issues.

Table 21-10 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.

Software upgrade issues

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

Table 21-11 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.

Table 21-11 Software Upgrade Issues (continued)

Issue	Cause and Possible Solutions
When using the system web interface to upgrade phone software, the phone is unable to connect to the Poly Hosted Server.	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.

Provisioning Issues

If settings you make from the central server aren't working, check first for priority settings applied from the local interface or system web interface. Afterward, check for duplicate settings in your configuration files.

22 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

HP US
HP Inc.
1501 Page Mill Road
Palo Alto 94304, U.S.A.
650-857-1501

HP Germany
HP Deutschland GmbH
HP HQ-TRE
71025 Boeblingen, Germany

HP UK
HP Inc UK Ltd
Regulatory Enquiries, Earley West
300 Thames Valley Park Drive
Reading, RG6 1PT
United Kingdom

Document information

Model ID: CCX 400, CCX 500, CCX 505, CCX 600, CCX 700

Document part number: 3725-13761-006A

Last update: May 2024

Email us at documentation.feedback@hp.com with queries or suggestions related to this document.