PVOS 8.0.1 | December 2022 | 3725-13765-002A

Poly Voice Software
Poly CCX Business Media Phones with Microsoft Teams
Administrator Guide

Contents

Before You Begin

This guide provides general guidance on deploying Poly CCX business media phones in Microsoft Teams and Microsoft Skype for Business environments. This guide also provides instructions on configuring supported features.

Poly UC Software supports the following Poly CCX devices with Microsoft Teams and Skype for Business:

- Poly CCX 350 business media phones
- Poly CCX 400 business media phones
- Poly CCX 500 business media phones
- Poly CCX 505 business media phones
- Poly CCX 600 business media phones

Audience, Purpose, and Required Skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

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

Related Poly and Partner Resources

See the following sites for information related to this product.

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

Privacy Policy

Poly products and services process customer data in a manner consistent with the Poly Privacy Policy. Please direct comments or questions to privacy@poly.com.

Poly CCX Phones Model Numbers

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

CCX Model Numbers

Product Name	Model Number
Poly CCX 350 business media phone	3111-49690-001
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

Getting Started

Poly CCX business media phones provide a native interface for Microsoft Teams and integration with Skype for Business.

Poly CCX Phones Overview

Poly CCX phones provide a unified communications experience from your desktop phone.

CCX business media phones contain the following features and capabilities:

- Embedded Microsoft Teams application
- HD Voice
- Integrated Bluetooth capabilities (available on CCX 500, CCX 505, and CCX 600 business media phones)
- Integrated Wi-Fi capabilities (available on CCX 505 and CCX 600 business media phones)
- USB audio device capabilities
- Color touch displays (except on CCX 350 business media phones)
- Integrated contact list, calendar, and meetings

Setting Up the Phone

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

Power CCX Phones

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

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

Task

» 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.

Poly CCX Power over Ethernet Classes

Phone Model	PoE Class	PoE Class Maximum	Normal Call	Maximum with All USB Loading
CCX 350	3	12.95 W	5 W	12 W
CCX 400	3	12.95 W	5 W	12 W
CCX 500	0	12.95 W	7 W	12 W
CCX 505	0	12.95 W	7 W	12 W
CCX 600	4	25.5 W	11 W	18 W

Complete the Setup Wizard

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

Task

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

   Note: You can't set the administrator password as the default password, which is `456`.
3 Review the Poly End User License Agreement (EULA) and select **Accept**.

   You can also review the EULA in the **Guides & Manuals** tab in your phone's support page at Poly Support.
4 Select a system language.
5 Set your time zone ID.
6 Choose the system's base profile from the displayed list.
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 350 and 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 350 and 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 USB Optimized base profile.

Task

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*.

Task

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

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

3 Save the configuration file.

Poly CCX Phones Base Profiles

Poly CCX business media phones support Microsoft services when set to one of the supported 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.

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*.

USB Optimized Base Profile
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 350 phones, the USB Optimized base profile is an unsupported feature. Several functions for call handling using the phone's physical keys do not perform as expected. Microsoft certification, and later Microsoft Teams software updates, are required before users can avail of the phone's full functionality in this base profile.

Skype for Business Base Profile
This base profile provides an integration of Microsoft's Skype for Business Server or Skype for Business Online (3PIP).

Important: Support for Skype for Business is deprecated in UC Software 7.3.0 and later, and the Skype for Business base profile is now removed from CCX phone menus. Skype for Business support remains available and continues to receive maintenance updates on the UC Software 7.2.x series.

If you deploy your phones using the Skype for Business base profile, configure Skype for Business using Skype for Business Server or the Skype for Business Admin Center depending on your Skype deployment. For more information, see the Microsoft documentation website.

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

Set Microsoft Teams as Base Profile from Skype for Business

Configure the phone to run the Microsoft Teams application. Once configured with the Teams profile, you can access and modify device settings from the phone menu.

Task

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 **Microsoft Teams**.
6. Select Back and save the configuration.
   The phone restarts, and the Microsoft Teams profile loads.

Set Skype for Business as Base Profile from Microsoft Teams

Configure the phone to load the Skype for Business profile from the Teams interface.

Task

1. Select **Menu**.
2. Go to **Settings > Device Settings**.
3. Select **Admin Only**.
4. Select **Profile > Skype**.
5. Select Back and save the configuration.
   The phone restarts, and the Skype for Business profile loads.

Set Microsoft Teams as Base Profile from USB Optimized

Configure the phone to run the Microsoft Teams application. Once configured with the Teams profile, you can access and modify device settings from the phone menu.

Task

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 **Microsoft Teams**.
6. Select Back and save the configuration.
   The phone restarts, and the Microsoft Teams profile loads.

Set USB Optimized as Base Profile from Microsoft Teams

Configure the phone to load the USB Optimized profile from the Teams interface.

Task

1. Select **Menu**.
2. Go to **Settings > Device Settings**.
3. Select **Admin Only**.
4. Select **Profile > USB Optimized**.
5. Select Back and save the configuration.
   The phone restarts, and the USB Optimized profile loads.

CCX Phones with Microsoft Teams

This section provides information about deploying your CCX phones with Microsoft Teams.

Microsoft Teams Device Settings

You can access and modify device settings from the Microsoft Teams Portal or from the phone menu.

Note: When you set the base profile to Microsoft Teams, Microsoft controls the Microsoft Teams software experience and performance on Poly CCX business media phones.

Network Configuration Options

You can set some network configuration options from the Admin Settings menu on an individual phone.

Manually Set DHCP Settings

The network DHCP settings will be automatically configured based on the DHCP server settings. Optionally, you can manually configure DHCP settings for a single phone.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Only**.
3. Select **Network Configuration > DHCP Settings**.
4. Enter the following details:
   - Host Name
   - Domain Name
   - IP Address
   - Subnet Mask
   - Default Gateway
   - Primary DNS
   - Secondary DNS

Configure VLAN from the Phone

You can manually configure the VLAN settings from the local interface.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Only**.
3. Select **Network Configuration > VLAN**.
4. Enter the **VLAN Id**.
5. Tap the switch to enable **LLDP**.
6. Tap the switch to enable **CDP Compatibility**.
7. Select the required **DHCP VLAN Discovery**.
8. Select **DHCP VLAN Option**.

Wireless Network Connectivity (Wi-Fi)

Poly CCX 505 and CCX 600 business media phones support several wireless modes, security options, and radio controls.

Note: Poly CCX 505 and CCX 600 business media phones don't support connectivity to Wi-Fi networks that require web authorization.

Enabling Wi-Fi automatically disables the Ethernet port. You can't use Wi-Fi and Ethernet simultaneously to connect phones to your network. When you connect the system to your network over Wi-Fi, only audio-only calls are available. The phones don't support Wi-Fi captive portals or Wireless Display (WiDi).

Set Country of Operation

Select the country of operation to ensure the best performance in your location before you enable the Wi-Fi.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Only** and enter the administrator password (the default is 456).
3. Select **Wi-Fi** and select the country of operation.
4. Save the settings to apply your changes.

Set 802.1x Authentication for the Phone

You can manually configure the 802.1x authentication from the phone interface.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Only**.
3. Select **Network Configuration > 802.1x**.
4. Tap the switch for **802.1x Authentication** to enable manual configuration.
5. Enter the following details:
   - **EAP Method**
   - **Identity**
   - **Password**
   - **Anonymous ID**
   - **EAP-FAST In-Band Provisioning**

   EAP-FAST In-Band Provisioning is configurable only if you select **EAP Method** as **EAP-FAST**.

Download the 802.1x Certificates on CCX 400 Business Media Phones

You need to manually download the 802.1x certificates on your CCX 400.

Note: This process is not applicable for CCX 400 phones running CCX 6.2.11 and later.

Task

1. On the server, navigate to the Apache HTTP server root folder.
2. Place the certificates in the root folder.
3. On the phone screen, press the menu icon at the top left.
4. Go to **Settings > Device Settings**.
5. Select **Admin Only** and enter the administrator password (the default is `456`).
6. Select **Network Configuration > 802.1x**.
7. Tap the switch for 802.1x Authentication to enable manual configuration.
8. Tap CA certificates and enter the path of the certificate (http://<IP>/cert_file_name).

   The certificate downloads from the HTTP web server and the certificate file path displays in the CA certificates field.
9. Tap **OK**.

Set the PC Port for the Phone

You can manually set the PC port for the phone.

Task

1. Go to **Settings > Device Settings**.

2 Select **Admin Only**.
3 Select **Network Configuration > PC Port**.
4 Select one of the following options:

- Disabled
- Auto
- 10HD
- 10FD
- 100HD
- 100FD
- 1000FD

Set LAN Port Settings

You can manually set Local Area Network (LAN) port settings on the phone.

Task

1 Go to **Settings > Device Settings**.
2 Select **Admin Only**.
3 Select **Network Configuration > LAN Port Settings**.
4 Select one of the following options:

- Auto
- 10HD
- 10FD
- 100HD
- 100FD
- 1000FD

Change the Default Administrator Password

Update the phone's administrator password from the local interface.

Task

1 Go to **Settings > Device Settings**.
2 Select **Admin Only**.
3 Select **Admin Password**.
4 Enter the current admin password, enter a new password, and confirm the new password.

Using Poly OpenSIP Features with Microsoft Teams

Enhance your CCX phone's capabilities with features from Poly OpenSIP call application while configured in the Microsoft Teams base profile.

Phones in the Teams base profile support the following features:

- **Group paging** - Display a group paging button in the **Poly Control Panel** which enables users to send group pages within your open SIP calling network.
- **Failover calling** - Enable users to swap the phone to the Poly OpenSIP call application to use as a backup for placing calls.

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.

Note: This feature is not available on CCX 350 phones.

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

Task

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.

Group Paging with the Poly Control Panel

Configure the phone to include group paging as an option in the **Poly Control Panel**. This enables users to use Poly group paging with the Microsoft Teams base profile.

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

- Send a page to the default group 1 page group.
- Send a page to a single defined page group.
- Display the **Group Page List**, which enables users to select a group to page.

Enable Group Paging in the Poly Control Panel

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

Make sure you set `apps.android.appSwitcher.enabled="1"`.

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.

Task

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

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

3. 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.

Make sure you set `apps.android.appSwitcher.Paging.enabled="1"`. Make sure you have at least two page groups defined.

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

Task

1 Open the configuration file.
2 Configure the channel that the phone automatically opens when users select group paging from the **Poly Control Panel**.

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

3 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.

Make sure you set `apps.android.appSwitcher.Paging.enabled="1"`.

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

Task

1 Open the configuration file.
2 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"
```

3 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.

Task

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.

Microsoft Teams Device and Software Support

This section provides information on maintaining your devices and updating your phone's software.

Enable or Disable the System Web Interface

Enable or disable access to the phone's system web interface from the phone's settings.

Note: CCX 400 phones running software prior to UC Software 6.2.11 don't support access to a system web interface.

Task

1 Go to **Settings > Device Settings**.
2 Select **Admin Only**.
3 Select **Network Configuration**.
4 Toggle **Web User Interface** to enable or disable access to the system web interface.

Reset Custom Configurations

You can erase the phone configuration done through the system web interface or from the Device Settings on the phone to reset the customized **Debug** values to defaults.

Task

1 Go to **Settings > Device Settings**.
2 Select **Admin Only**.
3 Select **Debug > Reset Custom Config**.
4 When prompted Do you want to reset custom configuration?, select **Continue**.

Reset the Phone to Factory Defaults in Microsoft Teams

You can reset the device to factory default settings if your device experiences problems that you cannot resolve by troubleshooting the device logs.

Resetting the phone to defaults clears the flash parameters, user and cached data, and resets the administrator password to `456`. When the phone reboots, you must reset the administrator password following the onscreen prompts.

Task

1 Go to **Settings > Device Settings**.
2 Select **Admin Only**.
3 Select **Debug > Reset to Factory Defaults**.
4 When prompted Do you want to reset to factory defaults?, select **Continue**.

Updating Microsoft Teams

Manage Microsoft Teams updates for your CCX series phones through the Microsoft Teams admin portal.

Important: If you leverage mobile device management, make sure your compliance policies do not block CCX phones from being provisioned. CCX phones run the Microsoft Teams IP Phone application. This Android-based application presents itself as "Android (device administrator)". Exclude this name from any compliance policies that prevent usage.

For more information on updating Microsoft Teams on your CCX phones, see the Microsoft Teams website.

Manage your devices in Microsoft Teams

CCX Phones with Skype for Business

This section provides information about deploying your CCX phones with Skype for Business.

Important: Support for Skype for Business is deprecated in UC Software 7.3.0 and later, and the Skype for Business base profile is now removed from CCX phone menus. Skype for Business support remains available and continues to receive maintenance updates on the UC Software 7.2.x series.

Deploying Poly Phones with Skype for Business

Poly offers several methods to register your Poly phones with Skype for Business.

If you are using Poly phones shipped with Skype for Business-qualified UC Software and want to keep default settings with no change, you need only configure the network. If you want to customize default settings, complete the following tasks:

- Configure the Network
- Set up Poly UC Software
- Provisioning the Phones

Configure the Network

Configure the following network settings to register Poly devices with Skype for Business.

Task

1. Set up or verify Domain Name System (DNS) service (SRV) records to allow the devices to discover Skype for Business servers automatically.

   For information on creating and verifying DNS SRV records, see the latest documentation on Microsoft TechNet. If you're setting Microsoft Call Admission Control (CAC), refer to Microsoft Plan for call admission control in Skype for Business Server 2015 for required bandwidth guidelines.
2. Obtain a root certificate authority (CA) security certificate using one of the following methods:

Certificate Method	Description
Lightweight Directory Access Protocol (LDAP) Domain Name System (DNS)	Phones you register with Skype for Business are enable with this feature by default.
Dynamic Host Configuration Protocol (DHCP) Option 43	When provisioning phones from within an enterprise, you can use DHCP Option 43 to download a private CA root security certificate used by Skype for Business. The security certificate is required to support secure HTTPS and TLS connections. Along with DHCP Option 43, ensure that your devices can access Skype for Business Server Certificate Provisioning Web Service over HTTP (TCP 80) and HTTPS (TCP 443). **Note:** If you configure DHCP Option 43 in on-premises Skype for Business deployments, the phone displays only the PIN Authentication menu to users. For more details and troubleshooting information on DHCP Option 43, see Microsoft TechNet.
DHCP Option 66	Use this method if you're using a provisioning server or setting DHCP options using the following: • DHCP Option 161. If you're using devices with a Skype or Lync Base Profile, use Option 161 with the address (URL or IP address) of the provisioning server. You can set the provisioning server address or URL on the device menu.

3. Set up each user with a Skype for Business account and credentials.

Supported DHCP Sub-Options

The following table lists the individual sub-options and combination sub-options supported on the phones for DHCP Option 43.

DHCP Option 43 Sub-Options

Option	Result
Option 1 – Subnet mask	The phone parses the value from Option 43.
Option 2 – Time offset	The phone parses the value.
Option 3 – Router	The phone parses the value.
Option 4 – Time server	The phone parses the value.
Option 6 – Domain Name Server	The phone parses the value.
Option 7 – Domain Log server	The phone parses the value.
Option 15 – Domain Name	The phone parses the value.
Option 42 – Network Time Protocol server	The phone parses the value.
Option 66 – TFTP Server Name	The phone parses the value.
Sub-options configured in Option 43	
Options 1, 2, 3, 4, 5, 6, 7, 15, 42, and 66	The phone parses the value.

Set Up Poly UC Software

After you power your devices and set up the network, set up the Poly UC Software.

Note: To avoid placing the phone in a continuous reboot cycle, don't provision phones with UC Software from both a Microsoft server and your own provisioning server.

Task

1. Set up a provisioning server on your computer and create a root directory to hold all of the required UC Software, configuration files, and subdirectories. Name the directory to identify it as containing the UC Software release.
2. Download, save, and extract UC Software to the root directory you created.
3. After the UC Software directory is extracted, open the folder in your root directory.
4. Configure a Call Park Orbit Policy.

   You must configure a call park orbit policy to enable the call park feature. See Configuring Call Park on Microsoft TechNet.

Provisioning Skype for Business Phones

The method labeled `device.set` is an advanced method for users familiar with configuration files and uses centralized provisioning to set the Base Profile for multiple phones.

The Base Profile is a provisioning option available on Skype for Business-enabled devices. The Base Profile displays in the phone's menu system and varies by phone model.

The Base Profile automates registration with a default set of configuration parameters and settings. You can't modify or customize the Base Profile or feature settings. Use centralized provisioning for deployments of greater than 20 devices requiring only default Skype for Business settings.

After registering the phone with the Skype for Business Server, enable the system web interface to configure the phone using a web browser.

Centralized Provisioning

Use a central provisioning server when provisioning multiple phones to:

- Configure multiple devices automatically
- Facilitate automated software updates
- Receive automatic log files
- Add, remove, or manage features and settings to multiple phones simultaneously
- Create phone groups and modify features and settings for each phone group

Note: Using an existing server to deploy your provisioning server can affect performance of your Skype for Business deployment. Misconfiguration or nonstandard deployment of the Microsoft Internet Information Services (IIS) web server may affect your ability to obtain accurate Microsoft support.

Centralized Provisioning Methods

Use one of the following methods to centrally deploy multiple devices:

- Use Skype for Business Online or Microsoft Exchange Online to set up phones and configure features.
- Use device.* parameters to configure multiple devices and only if you're familiar with centralized provisioning and configuration files.

Set Up Phones with Skype for Business Online and Exchange Online

Skype for Business Online and Microsoft Exchange Online provide applications and services including email and social networking, Exchange Server, SharePoint, Yammer, MS Office web applications, and Microsoft Office software.

Poly offers Skype for Business Online and Exchange Online for:

- Poly CCX 400 business media phones
- Poly CCX 500 business media phones
- Poly CCX 505 business media phones
- Poly CCX 600 business media phones

If you need to configure media ports for Skype for Business Online deployments, see Skype for Business Online for specific port numbers.

When using Skype for Business Online and Microsoft Exchange Online, note the following:

- You must use TLS-DSK to authenticate the phones.

Task

1. Install and open the Skype for Business Online, Windows PowerShell Module.
2. Type the command: `Import-Module SkypeOnlineConnector`.
3. Connect to the Skype for Business tenancy using the command: `$session=New-CsOnlineSession -Credential $cred`.
4. When the Powershell credential request dialog displays, enter your Skype for Business user name and password.
5. Import the session with the command: `Import-PSSession $session -Verbose -AllowClobber`.
6. Set policies with the command: `CsIPPhonePolicies`.

Deploy UC Software from a Provisioning Server

Complete the following steps to deploy UC Software from a provisioning server.

Task

1. Locate `000000000000.cfg` in the folder after you unzip the software package.

2 Place these configuration files in your root provisioning directory, create a copy of each file, and rename them keeping the suffix .cfg.

   Using edited copies of the template files ensures that you have unedited template files containing the default values.

   If you plan to manually install a root CA security certificate, go to step 3. If not, skip to step 4.

3 Open the primary configuration file 000000000000.cfg.

   In the **CONFIG_FILES** field, enter the name of your Skype for Business configuration file and save.

   Ensure that multiple configuration file names are comma-separated.

   Configuration files you enter in the CONFIG_FILES field read from left to right. If you configured the same setting in two configuration files, the setting listed first on the applies first. Ensure that you don't have the same parameter in more than one configuration file.

   If you don't want to use the Microsoft Autodiscover service, use the following parameters to disable the feature and manually set the Skype for Business server address and SIP signaling port using:

   - Disable Autodiscover: `reg.1.serverAutoDiscovery=0`
   - Server: `reg.1.server.1.address=<server_address>`
   - Port: `reg.1.server.1.port=<port_number>`

4 Set the following parameters in the device config file (`device.cfg`) to bypass EULA during bulk provisioning and software upgrade:

   - `device.eulaAccepted.set="1"`
   - `device.eulaAccepted="1"`

5 Power on your phones.

   Your phones display the Skype for Business Sign In screen.

Set the Base Profile with device.* Parameters

This section shows you how to provision multiple devices using parameters in the device.cfg template configuration file included in your UC Software download.

Poly recommends using device.* parameters to configure multiple devices and only if you're familiar with centralized provisioning and configuration files.

The parameter values correspond to the options in the phone menu or the system web interface as follows:

- `Skype`—**Skype for Business**
- `USBOptimized`—**Microsoft USB Optimize**
- `MSTeams`—**Microsoft Teams**

Task

1 Locate the device.cfg template configuration file and place the device.cfg file on your provisioning server.

2 Locate and change the values of the following parameters:

   - `device.baseProfile= <Base Profile value>`
   - `device.set=1`
   - `device.baseProfile.set=1`

3 Rename and save the file.

4 Power on the phones.

5 Once bootup is complete, remove device.set from the template configuration file and save the file again after removing device.set.

Manual Provisioning Methods

You can use per-phone, manual provisioning methods to register Poly devices with Skype for Business.

All manual provisioning methods set the Base Profile of a phone to **Skype for Business**. The Base Profile is a feature on each phone that, when set to **Skype for Business**, automatically provisions the phone with the default parameters required to work with Skype for Business.

When you use configuration files to provision the phones with Skype for Business, the phone Base Profile is set to **Generic**. You do not need to set the Base Profile to **Skype for Business** when provisioning with configuration files.

Change the Base Profile from the Settings Menu

You can set the Base Profile to from the phone **Settings** menu.

Note: The setting location differs on a Poly phone with Microsoft Teams.

Task

1. Go to **Settings > Advanced > Administration Settings > Network Configuration > Base Profile** and select **Skype for Business**.
2. Select **Back > Save Configuration**.

   The phone automatically restarts and displays the **Sign In** screen. Users can now sign in.

Set the Base Profile Using the System Web Interface

You can use the system web interface to manually set a phone's Base Profile to **Skype for Business** or **Microsoft Teams**.

The system web interface is disabled by default when the phone registers with Skype for Business Server. You must manually enable the system web interface to configure phone settings. You cannot configure sign-in credentials using the system web interface.

Task

1. Power on your phones and allow them to complete the power-up process.
2. Get the IP address of each phone in your deployment by going 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 (default `456`) and click **Submit**.
5. On the Home page, navigate to the **Simple Setup** menu.
6. From the **Base Profile** drop-down list, choose **Skype for Business** or **Microsoft Teams**, and click **Save** at the bottom of the page.
7. In the confirmation dialog, choose **Yes**.

The phone automatically restarts, and users can now sign in.

Configuring In-Band Provisioning Settings

You must provision phones using either in-band provisioning or your provisioning server and not both.

Where settings conflict, Skype for Business in-band provisioning device settings take precedence over the same settings configured on your provisioning server. If you are using your own provisioning server, avoid phone update loops by configuring `lync.provisionDeviceParams.enabled=0` to disable the following in-band provisioning device settings sent from the Skype for Business Server or Skype for Business Online:

- EnableDeviceUpdate
- IPPhoneAdminPasswd
- LocalProvisioningServerAddress
- LocalProvisioningServerUser
- LocalProvisioningServerPassword
- LocalProvisioningServerType
- ucDiffServVoice

lync.provisionDeviceParams.enabled

1 (default) - Enable (accept) in-band provisioning device settings sent from Skype for Business.

0 - Disable (block) in-band provisioning device settings sent from Skype for Business.

Sign In Methods

The phone offers several options that allow users to log in to their phones.

Your phones support the following methods:

- **User ID** - Enable users to sign in with their user credentials on the Sign In screen. You cannot configure login credentials using the Web Configuration Utility.
- **PIN Authentication** - Use this to sign in on the phone or from the Web Configuration Utility. This option is available in on-premises Skype for Business deployments when you configure DHCP Option 43 and is not available for online deployments.
- **Web Sign In for Skype for Business** - This method enables secure sign-in from a browser on your computer or mobile device. The phone generates a unique pairing code used to sign in on a secure Office 365 website.
- **Single Sign-On Solutions (SSO)** - Allows you to use the same login credentials across multiple cloud-based applications such as Microsoft Exchange and Skype for Business.

When you change the active directory password, the phone de-registers from the Skype for Business server with a registration expiry value.

The maximum length of the user name or sign in address (Name + Domain) is limited to 45 characters.

While signing in to the phone, the phone displays sign-in progress messages such as **Discovering Skype for Business Server** or **Authentication in progress**.

Skype for Business Sign-in and Credential Parameters

The following parameters configure the type of sign in on the phones and user credentials.

reg.1.auth.loginCredentialType

Configure a login type and user credentials. You cannot log in to the phone with Microsoft credentials if the parameter `reg.1.auth.loginCredentialType` is set to the default value.

LoginCredentialNone (default)

usernameAndPassword - Set credentials to sign-in address, user name, domain, and password in the required format.

extensionAndPIN - Set credentials to extension and PIN.

reg.1.auth.useLoginCredentials

You can use this method in the configuration file to automatically sign in users after the phone powers up.

1 (default) - SSI Login credentials, BToE Sign in, and Web Sign types are available for authentication with the server.

0 - SSI Login credentials, BToE Sign in, and Web Sign types are not available for authentication with the server.

reg.1.auth.usePinCredentials

You can use this method in the configuration file to automatically sign in users after the phone powers up.

To use this sign-in method, you must enable DHCP Option 43 or `dhcp.option43.override.stsUri`.

1 - PIN authentication sign in method is available for authentication on the server.

0 - PIN authentication sign in method is not available for authentication on the server.

auth.unblock.period

If the authentication request attempts fail due to a server error, further authentication attempts are blocked for a defined number of minutes before reattempting.

30 minutes (default)

0 - 30

Example Sign In Configurations

You can set PIN authentication or SSI login credentials in the configuration file to log in users automatically after the phone powers up.

The following example sets PIN authentication user credentials in the configuration file:

- `reg.1.auth.usePinCredentials="1"`
- `reg.1.auth.loginCredentialType="extensionAndPIN"`
- `device.set="1"`
- `device.logincred.extension.set="1"`
- `device.logincred.extension="xxxx"`
- `device.logincred.pin.set="1"`
- `device.logincred.pin="xxxx"`

The following example sets SSI login credentials in the configuration file:

- `reg.1.auth.loginCredentialType="usernameAndPassword"`
- `reg.1.address="xxxx@domain.com"`
- `device.set="1"`
- `device.logincred.user.set="1"`
- `device.logincred.user="xxxx"`
- `device.logincred.password.set="1"`
- `device.logincred.password="xxxxx"`
- `device.logincred.domain.set="1"`
- `device.logincred.domain="domain"`

PIN Authentication

You can enable users to sign in to Skype for Business using PIN authentication.

To use PIN authentication, you must enable the Web Configuration Utility, which is disabled by default. For information on enabling the Web Configuration Utility, see Accessing the Web Configuration Utility. After you enable the Web Configuration Utility, you can enable PIN authentication using reg.1.auth.usePinCredentials.

If you configure DHCP Option 43 in on-premises Skype for Business deployments, the phone displays only the PIN Authentication menu to users. The PIN Auth menu does not display and is not available for Skype for Business Online.

PIN Authentication Parameters

The following parameters configure PIN Authentication.

device.logincred.extension

NULL (default) - The phones will not trigger registration.

0 to 32 - Enter a user phone extension number or string to a maximum of 32 characters. The phone reads this extension when you configure PIN-Auth as the phone registration method.

device.logincred.pin

NULL (default) - If the default value is set, the phones will not trigger registration.

0 to 32 -Enter a user phone PIN to a maximum of 32 characters. The phone reads this PIN when you configure PIN-Auth as the phone registration method.

reg.1.auth.useLoginCredentials

You can use this method in the configuration file to automatically sign in users after the phone powers up.

1 (default) - SSI Login credentials, BToE Sign in, and Web Sign types are available for authentication with the server.

0 - SSI Login credentials, BToE Sign in, and Web Sign types are not available for authentication with the server.

Web Sign In for Skype for Business

Web Sign In is enabled by default on phones registered with the Skype for Business server and is available for Skype for Business Online and On-Premise deployments.

Web Sign In enables users to securely login to Skype for Business on their phone from a computer or a mobile web browser. It provides users with a way to authenticate their Skype for Business credentials without entering their credentials on the phone. The phone displays on-screen instructions to help users proceed through the process. With the Web Sign In method, a user can sign in concurrently to a maximum of eight phones. If a user signs in on multiple phones and signs out from one phone, the user remains signed in on the remaining phones.

Users authenticate their accounts using a pairing code that is generated on the phone. The pairing code that the Web Sign In method generates expires within a few minutes after the Skype for Business server sends the code to the phone. Users must sign in before the pairing code expires.

Web Sign In supports Multi-Factor Authentication (MFA) on phones. If you're using MFA, you must use Web Sign In as the user sign-in method with phones. For more information on configuring MFA for Office 365, refer to Microsoft's Configure Azure Multi-Factor Authentication Settings.

Web Sign In for Skype for Business server is supported only when the Hybrid Modern Authentication (HMA) environment is enabled. To use the capability of HMA with Skype for Business On-Premise, Active Directory should be federated with Azure Active Directory (AAD). For more information to configure HMA in your environment, refer to Hybrid Modern Authentication for Skype for Business.

Web Sign In for Skype for Business Parameters

The following parameters configure Web Sign In for Skype for Business Online and On-Premises deployments.

feature.webSignIn.enabled

1 (default) - In Skype for Business Base Profile, the web sign in option is displayed on the phone for the user.

0 - In Skype for Business Base Profile, the web sign in option is not displayed on the phone for the user.

reg.1.auth.loginCredentialType

Specify the credential type the user must provide to log in. You cannot log in to the phone with Microsoft credentials if `reg.1.auth.loginCredentialType` is set to the default value.

`LoginCredentialNone` (default)

`onlineDeviceAuth` - Enables users to sign in to the phone using Web Sign In.

`usernameAndPassword` - Provide description of this value.

feature.remoteWebSignIn.enabled

0 (default) - The web UI does not provide the web sign-in option.

1 (default) - The web UI includes a web sign-in option.

Sign In Remotely using Web Sign-In for Skype for Business

You can sign in to Skype for Business remotely using the phone's Web Configuration Utility.

Task

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and select **Submit**.
3. Select **Settings > Skype for Business Sign In**.
4. Select **Web Sign-In** from **Authentication Type**.
5. Select **Sign In**.
   A URL and a sign-in code display.
6. Enter the URL into a web browser on your computer.
7. Enter the sign-in code and select **Continue**.
   The Skype for Business Authentication website displays.
8. Enter your Skype for Business login information.
   A confirmation message displays when the phone successfully signs in to Skype for Business.

Modern Authentication Supported Topologies

The following table lists supported Modern Authentication topologies.

Modern Authentication Supported Topologies

Technology Name	Skype for Business	Modern Authentication on Skype for Business	Microsoft Exchange	Modern Authentication on Microsoft Exchange	Supported?
Cloud Only	Online	On	Online	On	Yes
On Prem Only	On-Premise	On	On-Premise	On	Yes
Mixed 1	On-Premise	Off	Online	On	Yes
Mixed 2	Online	On	On-Premise	Off	Yes

Sign In with Better Together over Ethernet (BToE)

You can enable users to use this sign-in method with the Better Together over Ethernet (BToE) feature. The BToE feature enables users to place, answer, and hold audio calls from the phone and Skype for Business client on a computer.

This sign in method is available after the user downloads the BToE connector application then pairs their computer and phone. To download the application and for detailed instructions, see the user guide for your phone model.

Web Sign In for CAP with Skype for Business Online

When you enable Common Area Phone (CAP) mode with Online Web Sign In and set the phone to CAP Admin mode, you can sign in to the phone registered with Skype for Business Online and securely log in to Skype for Business from the phone or from a computer or mobile web browser.

This sign in method is not applicable when the phone is signed in as a guest user.

Disabling the Sign-In and Sign-Out Soft Keys

Use the following parameters to remove the sign-out soft key, or the **Sign In** and **Sign Out** soft keys.

feature.lync.hideSignInSignOut

0 (default) - The **Sign In** and **Sign Out** soft keys display on the **Home** screen and phone menus.

1 - The **Sign In** and **Sign Out** soft keys are removed from the Home screen and phone menus, and users are not able to sign in or out. Administrators can sign in and out with the system web interface.

feature.lync.hideSignOut

0 (default) - The **Sign Out** soft key displays on the **Home** screen and phone menus.

1 - The **Sign Out** soft key is removed from the **Home** screen and phone menus, and users are not able to sign out. Administrators can sign out of the phone from the **Advanced** menu or system web interface.

feature.lyncbtoe.autosignin.signoff.enabled

0 (default) - When the connection between the phone and and BToE application is terminated, the credentials cached on the phone remains as is and the phone continues to stay signed in.

1 - When the connection between the phone and BToE application is terminated, the credentials cached on the phone are removed and the phone triggers auto sign-off.

Note: The auto sign-off triggers only when the phone was previously signed in using via PC sign-in method.

softkey.feature.simplifiedSignIn

0 (default) - The **Sign In** and **Sign Out** soft keys are removed from the Home screen and display in the Features menu.

1 - The **Sign In** and **Sign Out** soft keys displays on the Home screen and phone menus.

Microsoft Exchange Integration

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

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

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

Skype for Business

Skype for Business and Lync Server provides a unified communications (UC) solution that enables customers, colleagues, and business partners to communicate instantly by voice, video, or messaging through a single interface, regardless of their location or network.

Note that the concurrent failover/fallback feature is not compatible in a Microsoft environment.

The features available when you are registered with Skype for Business Server vary with the Poly phone model and Poly UC Software version you are using. Poly UC Software supports the following devices with Skype for Business and Lync Server:

- Poly CCX business media phones

If you are using UC Software with Skype for Business and want to change default settings or customize your deployment, you must set up a provisioning server.

Poly UC Software enables you to register only a single phone line with Skype for Business Server. When you register a line on a Poly phone using Skype for Business Server you cannot register lines with another server.

Integrating with Microsoft Exchange

The phone offers several methods to integrate with Microsoft Exchange.

Use one of the following methods:

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

Provision the Microsoft Exchange Calendar

You can provision your phones with the Microsoft Exchange calendar.

Task

» Add the following parameters to one of your configuration files:

- `feature.exchangeCalendar.enabled=1`
- `exchange.server.url=https://<example URL>`

Enable Microsoft Exchange Calendar Using the System Web Interface

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

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

Task

1. Log in to the system web interface using admin credentials (default password `456`).
2. Go to **Settings > Applications > Exchange Applications**.
3. In the **Exchange Calendar** field, select **Enable**.
4. Enter the exchange web services URL using a Microsoft Exchange Server URL.
   For example `https://<mail.com>/ews/exchange.asmx`.
5. Select **Save**.
6. Select **Yes**.
   The Calendar icon displays on your phone screen.

Verify the Microsoft Exchange Integration

Verify that all of the Exchange services work properly.

Task

» Do one of the following:

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

Configuring the Microsoft Exchange Server

You can configure the following settings to use Microsoft Exchange services on your phones.

Visual Voicemail

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

Calendar Month View

On the Exchange server, you can enable the month view option for users to retrieve the calendar events for all the days in the month.

The **Month View** option is disabled by default.

Calendar Month View Parameters

The following parameters configure the month view.

calendar.monthView.enabled

0 (default) - Disables the **Month View** soft key.

1 - Enables the **Month View** soft key.

Synchronizing Call Logs

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

Call Log Synchronization Parameter

Use the following parameter to configure call logs.

feature.exchangeCallLog.enabled

1 (default) - The Exchange call log feature is enabled and the user call log history of Missed, Received, and outgoing calls can be retrieved on the phone.

You must also enable the parameter `feature.exchangeCalendar.enabled` to use the Exchange call log feature. If you disable `feature.exchangeCalendar.enabled` , also disable `feature.exchangeCallLog.enabled` to ensure call log functionality.

0 (default) - The Exchange call log feature is disabled and the user call logs history cannot be retrieved from the Exchange server.

ABS Adaptive Search

You can enable the Address Book Service (ABS) on the Exchange server.

There are three possible configurations.

- Outlook and ABS are both enabled by default. When both are enabled, the phone displays the Skype for Business Directory.
- If you disable Outlook and enable only ABS, the phone displays the Skype for Business Directory.
- If you enable Outlook and disable ABS, the Outlook Contact Search displays in Directories.

Phones registered with Skype for Business server display a one-touch **Join** button that allows you to join a Skype for Business conference in a federated environment, even if you haven't configured Transport Neutral Encapsulation Format (TNEF).

Microsoft Exchange Parameters

The following parameters configure Microsoft Exchange integration.

exchange.meeting.alert.followOfficeHours

1 (default) - Enable audible calendar alerts during business hours.

0 - Disable audible calendar alerts.

exchange.meeting.alert.tonePattern

positiveConfirm (default) - Set the tone pattern of the reminder alerts using any tone specified by `se.pat.*`.

exchange.meeting.alert.toneVolume

10 (default) - Set the volume level of reminder alert tones.

0 - 17

exchange.meeting.deleteUnlistedEvents

0 (default) - Remove events from the day view if they stop being reported by the server.

1 - Do not remove events from the day view if they stop being reported by the server.

exchange.meeting.allowScrollingToPast

0 (default) - Do not allow scrolling up in the Day calendar view to see recently past meetings.

1 - Allow scrolling up in the Day calendar view to see recently past meetings.

exchange.meeting.parseOption

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

Location (default)

All

LocationAndSubject

Description

Change causes a reboot.

exchange.meeting.phonePattern

NULL (default)

string

The pattern used to identify phone numbers in meeting descriptions, where "x" is a digit or an asterisk(*) and "|" separates alternative patterns (for example, xxx-xxx-xxxx|604.xxx.xxxx).

exchange.meeting.realConnectProcessing.outboundRegistration

Choose a line number to use to make calls on Polycom RealConnect technology.

2 (default)

1 - 34

Change causes system to restart or reboot.

exchange.meeting.realConnectProcessing.prefix.domain

Define the One-Touch Dial meeting invite prefix domain. Example: "`mypolycom.com`"

exchange.meeting.realConnectProcessing.prefix.value

Define the One-Touch Dial meeting invite prefix value.

exchange.meeting.realConnectProcessing.skype.enabled

0 (default) – Disable the Skype for Business meeting on Polycom RealConnect technology.

1 - Enable the Skype for Business meeting on Polycom RealConnect technology.

Change causes system to restart or reboot.

exchange.meeting.reminderEnabled

1 (default) - Meeting reminders are enabled.

0 - Meeting reminders are disabled.

exchange.meeting.reminderInterval

Set the interval at which phones display reminder messages.

300 seconds (default)

60 - 900 seconds

exchange.meeting.reminderSound.enabled

1 (default) - The phone makes an alert sound when users receive reminder notifications of calendar events. Note that when enabled, alert sounds take effect only if `exchange.meeting.reminderEnabled` is also enabled.

0 - The phone does not make an alert sound when users receive reminder notifications of calendar events.

exchange.meeting.reminderType

Customize the calendar reminder and tone.

2 (default) - The reminder is always audible and visual.

1 - The first reminder is audible and visual reminders are silent.

0 - All reminders are silent.

exchange.meeting.reminderWake.enabled

1 (default) - The phone wakes from low power mode after receiving a calendar notification.

0 - The phone stays in low power mode after receiving a calendar notification.

exchange.pollInterval

The interval, in milliseconds, to poll the Exchange server for new meetings.

30000 (default)

4000 minimum

60000 maximum

exchange.server.url

NULL (default)

string

The Microsoft Exchange server address.

feature.EWSAutodiscover.enabled

If you configure `exchange.server.url` and set this parameter to 1, preference is given to the value of `exchange.server.url`.

Generic Base Profile default is 0.

1 - Exchange autodiscovery is enabled and the phone automatically discovers the Exchange server using the email address or SIP URI information.

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

feature.exchangeCalendar.enabled

Generic Base Profile default is 0.

0 - The calendaring feature is disabled.

1 - The calendaring feature is enabled.

You must enable this parameter if you also enable `feature.exchangeCallLog.enabled`. If you disable `feature.exchangeCalendar.enabled`, also disable `feature.exchangeCallLog.enabled` to ensure call log functionality.

exchange.multipleCalendarEvents.enabled

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

0 - Only the next calendar event displays.

feature.exchangeContacts.enabled

Generic Base Profile default is 0.

1 - The Exchange call log feature is enabled and users can retrieve the call log histories for missed, received, and outgoing calls.

0 - The Exchange call log feature is disabled and users cannot retrieve call logs histories.

You must also enable the parameter `feature.exchangeCallLog.enabled` to use the Exchange call log feature.

feature.exchangeVoiceMail.enabled

Generic Base Profile default is 0.

1 - The Exchange voicemail feature is enabled and users can retrieve voicemails stored on the Exchange server from the phone.

0 - The Exchange voicemail feature is disabled and users cannot retrieve voicemails from Exchange Server on the phone.

You must also enable `feature.exchangeCalendar.enabled` to use the Exchange contact feature.

feature.exchangeVoiceMail.skipPin.enabled

0 (default) - Enable PIN authentication for Exchange Voicemail. Users are required to enter their PIN before accessing Exchange Voicemail.

1 - Disable PIN authentication for Exchange Voicemail. Users are not required to enter their PIN before accessing Exchange Voicemail.

feature.exchange2019.interop.enabled

0 (default) - Disabled

1 - The device sends a read notification for voicemail after playing to mark the voicemail has been read on the server.

feature.lync.abs.enabled

Generic Base Profile default is 0.

1 - Enable comprehensive contact search in the Skype for Business address book service.

0 - Disable comprehensive contact search in the Skype for Business address book service.

feature.lync.abs.maxResult

Define the maximum number of contacts to display in a Skype for Business address book service contact search.

12 (default)

5 - 50

feature.wad.enabled

Do not disable this parameter if you are using Skype Online or Web Sign-In.

1 (default) – The phone attempts to use Web auto-discovery and if no FQDN is available, falls back to DNS.

0 - The phone uses DNS to locate the server FQDN and does not use Web auto-discovery. Do not disable this parameter when using Skype for Business Online and Web Sign In.

feature.contacts.readonly

0 (default) - Skype for Business Contacts are editable.

1 - Skype for Business are read-only.

up.oneTouchDirectory

Generic Base Profile default is 0.

1 - The Skype for Business Search icon displays on the Home screen.

0 - The Skype for Business Search icon does not display on the Home screen.

Audio Features

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

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

Polycom NoiseBlock

Polycom NoiseBlock technology automatically mutes the microphone during audio-only and audio/video calls when a user stops speaking.

This feature silences noises that interrupt conversations such as paper shuffling, food wrappers, and keyboard typing. When a user speaks, the microphone is automatically unmuted.

Polycom NoiseBlock Parameters

Use the following parameters to configure NoiseBlock.

voice.ns.hf.block

1 (default) - Enables NoiseBlock.

0 - Disables NoiseBlock.

Supported Audio Codecs

The following table lists audio codecs supported by Poly CCX phones.

Audio Codecs and Priority

Phone	Audio Codec	Priority
Poly CCX	G.711 µ -law	6
	G.711a-law	7
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.722.1C (48kbps)	2
	G.729AB	8
	Opus*	0
	iLBC (13.33kbps, 15.2kbps)	0, 0

Supported Audio Codec Specifications

The following table summarizes the specifications for audio codecs supported on Poly phones.

Audio Codec Specifications

Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
G.711 µ -law	RFC 1890	64 kbps	80 kbps	8 ksps	20 ms	3.5 kHz
G.711 a-law	RFC 1890	64 kbps	80 kbps	8 ksps	20 ms	3.5 kHz
G.719	RFC 5404	32 kbps 48 kbps 64 kbps	48 kbps 64 kbps 80 kbps	48 ksps	20 ms	20 kHz
G.711	RFC 1890	64 kbps	80 kbps	16 ksps	20 ms	7 kHz

Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
G.722 Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.	RFC 3551	64 kbps	80 kbps	16 ksps	20 ms	7 kHz
G.722.1	RFC 3047	24 kbps 32 kbps	40 kbps 48 kbps	16 ksps	20 ms	7 kHz
G.722.1C	G7221C	24 kbps 32 kbps 48 kbps	40 kbps 48 kbps 64 kbps	32 ksps	20 ms	14 kHz
G.729AB	RFC 1890	8 kbps	24 kbps	8 ksps	20 ms	3.5 kHz
Opus	RFC 6716	8 to 24 kbps	24 to 40 kbps	8 ksps 16 ksps	20 ms	3.5 kHz 7 kHz
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
Siren 7	SIREN7	16 kbps 24 kbps 32 kbps	32 kbps 40 kbps 48 kbps	16 ksps	20 ms	7 kHz
Siren14	SIREN14	24 kbps 32 kbps 48 kbps	40 kbps 48 kbps 64 kbps	32 ksps	20 ms	14 kHz
Siren22	SIREN22	32 kbps 48 kbps 64 kbps	48 kbps 64 kbps 80 kbps	48 ksps	20 ms	22 kHz

Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
iLBC	RFC 3951	13.33 kbps 15.2 kbps	31.2 kbps 24 kbps	8 ksps	30 ms 20 ms	3.5 KHz
SILK	SILK	Skype 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	3.5 KHz 5.2 KHz 7 KHz 11 KHz

Note: The network bandwidth necessary to send the 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 for both the receive and transmit signals consumes about 100 kbps of network bandwidth (two-way audio).

Audio Codec Parameters

You can configure a set of codec properties to improve consistency and reduce workload on the phones.

Use the following parameters to specify audio codec priority on your phones.

- Permitted values to set audio codec priority are 1 - 35
- A value of 1 is the highest priority, 35 the lowest.
- If 0 or Null, the codec is disabled.
- A change to the default value does not cause a phone to restart or reboot

If a phone does not support a codec, the phone treats the value as 0, does not offer or accept calls using that codec, and continues to the codec next in priority.

`voice.codecPref.G711_A`

7 (default)

`voice.codecPref.G711_Mu`

6 (default)

`voice.codecPref.G719.32kbps`

0 (default)

`voice.codecPref.G719.48kbps`

0 (default)

`voice.codecPref.G719.64kbps`

0 (default)

`voice.codecPref.G722`

4 (default)

`voice.codecPref.G7221.24kbps`

0 (default)

voice.codecPref.G7221_C.24kbps

0 (default)

voice.codecPref.G7221.32kbps

5 (default)

voice.codecPref.G7221_C.48kbps

2 (default)

voice.codecPref.G729_AB

8 (default)

voice.codecPref.iLBC.13_33kbps

0 (default)

voice.codecPref.iLBC.15_2kbps

0 (default)

voice.codecPref.Lin16.8ksps

0 (default)

voice.codecPref.Lin16.16ksps

0 (default)

voice.codecPref.Lin16.32ksps

0 (default)

voice.codecPref.Lin16.44_1ksps

0 (default)

voice.codecPref.Lin16.48ksps

0 (default)

voice.codecPref.Siren7.16kbps

0 (default)

voice.codecPref.Siren7.24kbps

0 (default)

voice.codecPref.Siren7.32kbps

0 (default)

voice.codecPref.Siren14.24kbps

0 (default)

voice.codecPref.Siren14.32kbps

0 (default)

voice.codecPref.Siren14.48kbps

3 (default)

voice.codecPref.Siren22.32kbps

0 (default)

voice.codecPref.Siren22.48kbps

0 (default)

voice.codecPref.Siren22.64kbps

1 (default)

voice.codecPref.SILK.8ksps

0 (default)

voice.codecPref.SILK.12ksps

0 (default)

voice.codecPref.SILK.16ksps

0 (default)

voice.codecPref.SILK.24ksps

0 (default)

SILK Audio Codec Parameters

Use the following parameters to configure the SILK audio codec.

voice.audioProfile.SILK.8ksps.encMaxAvgBitrateKbps

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

20 kbps (default)

6 – 20 kbps

voice.audioProfile.SILK.12ksps.encMaxAvgBitrateKbps

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

25 kbps (default)

7 – 25 kbps

voice.audioProfile.SILK.16ksps.encMaxAvgBitrateKbps

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

30 kbps (default)

8 – 30 kbps

voice.audioProfile.SILK.24ksps.encMaxAvgBitrateKbps

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

40 kbps (default)

12 to 40 kbps

voice.audioProfile.SILK.encComplexity

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

2 (default)

0 to 2

voice.audioProfile.SILK.encDTXEnable

0 (default) – Disable Enable Discontinuous transmission (DTX).

1 - Enable DTX in the SILK encoder. Note that DTX reduces the encoder bitrate to 0bps during silence.

voice.audioProfile.SILK.encExpectedPktLossPercent

Set the SILK encoder expected network packet loss percentage.

A non-zero setting allows less inter-frame dependency to be encoded into the bitstream, resulting in increasingly larger bitrates but with an average bitrate less than that configured with voice.audioProfile.SILK.*.

0 (default)

0 to 100

voice.audioProfile.SILK.encInbandFECEnable

0 (default) - Disable inband Forward Error Correction (FEC) in the SILK encoder.

A non-zero value here causes perceptually important speech information to be sent twice: once in the normal bitstream and again at a lower bitrate in later packets, resulting in an increased bitrate.

voice.audioProfile.SILK.MaxPTime

Specify the maximum SILK packet duration in milliseconds (ms).

20 ms

voice.audioProfile.SILK.MinPTime

Specify the minimum SILK packet duration in milliseconds (ms).

20 ms

voice.audioProfile.SILK.pTime

The recommended received SILK packet duration in milliseconds (ms).

20 ms

Music on Hold

Music on Hold (MoH) enables you to play music when you place a call on hold.

You can specify on the provisioning server which music file the phone plays or upload a file using the phone's system web interface. When MoH is enabled, you can turn the music on or off while the call is on hold. If you place multiple calls on hold, only the first call placed on hold hears the music.

The default MoH file size is 540 KB and the maximum file size is 600 KB. You can increase the max file size to 1014KB using the parameter `res.quotas.tone`. The phone supports the following .wav audio file formats:

- mono G.711 (8 bits/sample, 8-khz sample rate)
- mono L16/16000 (16 bits/sample, 16-kHz sample rate)
- mono L16/48000 (16 bits/sample, 48-kHz sample rate)

Upload a Music File

You can upload a music file to the phone using the phone's system web interface.

Task

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password, and select **Submit**.
3. Go to **Preferences > Additional Preferences > Music On Hold**.
4. Select **MOH Status Enable** and **Save**.
5. Select **Add** and select a file from your computer or enter a URL.
6. Click **Save**.

Configuring Music on Hold

The following parameters configure Music on Hold.

feature.moh.enabled

Music on hold enables phone users to stream music when they place a caller on hold.

0 (default) - Music on hold is disabled.

1 - Music on hold is enabled and you must specify a music file in `feature.moh.filename`.

feature.moh.filename

Specify the file the music file you want the phone to play when users place an active call on hold.

NULL (default)

String, maximum of 256 characters

feature.moh.payload

Specify the payload for RTP packets when music on hold is playing. For best phone performance, set to 80. In PSTN calls using a media gateway that does not support a payload value of 80, set to 20.

80 (default)

20, 40, 60, 80

res.quotas.tone

Set the maximum sample tone file size.

1024 KB

600 - 1024 KB

Music on Hold Error Messages

If a music file fails to play, the phone displays one of the following messages to indicate the problem.

MoH Error Messages

Message	Cause
Download failed	Phone failed to download the MoH file because the current file was in use. MoH file size is 0 A network failure occurred during download.
File size exceeded the maximum	File size exceeded the maximum. You can configure the maximum file size using `res.quotas.tone`.
Unsupported file format	The file you are uploading is not a supported file format.
Network is down	A network failure occurred during download.

Headset and Speakerphone Parameters

You can use the parameters in the following list to enable and disable the headset or speakerphone and control other options for the headset and speakerphone.

up.analogHeadsetOption

Electronic Hookswitch (EHS) mode for the phone's analog headset jack.

2 (default) - Plantronics EHS-compatible headset is attached.

0 - No EHS-compatible headset is attached.

1 - Jabra EHS-compatible headset is attached.

3 - Sennheiser EHS-compatible headset is attached.

Change causes system to restart or reboot.

up.audioMode

Specify whether you want to use the handset or headset for audio.

0 (Default) - Use the handset for audio.

1 - Enabled - Use the headset for audio.

Phone Display Features

This section explains features you can configure for the phone's screen display and lists parameters you can use to configure these features.

Skype for Business User Interface on Poly Phones

The user interface for Poly phones match the theme used in the Skype for Business client.

This feature is enabled by default on supported phones with the Skype Base Profile or shipped with Skype for Business enabled.

Reverse Name Lookup

You can configure the phone to display incoming caller names, outgoing recipient names, and the source location where the phone obtains names.

The phone displays all Skype for Business participant names for the following functions:

- CCCP conference calls
- Response group calls
- Team calls
- Voicemail
- Placed, Received, and Missed call lists

If the phone cannot match the number of the incoming or outgoing name to a name in your organization, the phone displays the name given in the SIP signaling.

If a user saves a contact to the phone's local contact directory, the call list displays that name regardless of the priority you configure.

Reverse Name Lookup Parameter

The following parameter configure Reverse Name Lookup.

`up.rnl.priority`

Outlook,SIP,ABS,Local (default)

This parameter overrides `up.useDirectoryNames` in the Skype Base Profile.

Enter a comma-separated string, no spaces, for components you want to enable with Reverse Name Lookup. If you misconfigure the string, the parameter value falls back to the default priority order. The string isn't case-sensitive and can include any of the following values, listed here in the default priority order the phone looks for a matching name:

For example, if you configure "ABS,SIP,Outlook,Local", the phone tries to match the incoming number with contact names in the order of components you list.

If you don't configure the value SIP as one of the values, and the phone doesn't obtain the contact name using any one of the others values you configure, the phone uses the name given in the SIP signaling.

If you configure this parameter as disabled to avoid look up from Outlook, ABS, and local sources, then the phone uses the contact name given in the SIP signaling.

Time Zone Location Description

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

- device.sntp.gmtOffsetcityID If you are not provisioning phones manually from the phone menu or Web Configuration Utility and you are setting the device.sntp.gmtOffset parameter, then you must configure device.sntp.gmtOffsetcityID to ensure that the correct time zone location description displays on the phone menu and Web Configuration Utility. The time zone location description is set automatically if you set the device.sntp.gmtOffset parameter manually using the phone menu or Web Configuration Utility.
- tcpIpApp.sntp.gmtOffsetcityID If you are not provisioning phones manually from the Web Configuration Utility and you are setting the tcpIpApp.sntp.gmtOffset parameter, then you must configure tcpIpApp.sntp.gmtOffsetcityID to ensure that the correct time zone location description displays on the Web Configuration Utility. The time zone

location description is set automatically if you set the tcpIpApp.sntp.gmtOffset parameter manually using the Web Configuration Utility.

Time Zone Location Parameters

The following parameters configure time zone location.

Time Zone Location Parameter Values

Permitted Value	Time Zone Description
0	(GMT -12:00) Eniwetok,Kwajalein
1	(GMT -11:00) Midway Island
2	(GMT -10:00) Hawaii
3	(GMT -9:00) Alaska
4	(GMT -8:00) Pacific Time (US & Canada)
5	(GMT -8:00) Baja California
6	(GMT -7:00) Mountain Time (US & Canada)
7	(GMT -7:00) Chihuahua,La Paz
8	(GMT -7:00) Mazatlan
9	(GMT -7:00) Arizona
10	(GMT -6:00) Central Time (US & Canada)
11	(GMT -6:00) Mexico City
12	(GMT -6:00) Saskatchewan
13	(GMT -6:00) Guadalajara
14	(GMT -6:00) Monterrey
15	(GMT -6:00) Central America
16	(GMT -5:00) Eastern Time (US & Canada)
17	(GMT -5:00) Indiana (East)
18	(GMT -5:00) Bogota,Lima
19	(GMT -5:00) Quito
20	(GMT -4:30) Caracas
21	(GMT -4:00) Atlantic Time (Canada)
22	(GMT -4:00) San Juan
23	(GMT -4:00) Manaus,La Paz
24	(GMT -4:00) Asuncion,Cuiaba
25	(GMT -4:00) Georgetown
26	(GMT -3:30) Newfoundland
27	(GMT -3:00) Brasilia
28	(GMT -3:00) Buenos Aires
29	(GMT -3:00) Greenland
30	(GMT -3:00) Cayenne,Fortaleza
31	(GMT -3:00) Montevideo
32	(GMT -3:00) Salvador
33	(GMT -3:00) Santiago
34	(GMT -2:00) Mid-Atlantic
35	(GMT -1:00) Azores
36	(GMT -1:00) Cape Verde Islands
37	(GMT 0:00) Western Europe Time
38	(GMT 0:00) London,Lisbon
39	(GMT 0:00) Casablanca
40	(GMT 0:00) Dublin

Permitted Value	Time Zone Description
41	(GMT 0:00) Edinburgh
42	(GMT 0:00) Monrovia
43	(GMT 0:00) Reykjavik
44	(GMT +1:00) Belgrade
45	(GMT +1:00) Bratislava
46	(GMT +1:00) Budapest
47	(GMT +1:00) Ljubljana
48	(GMT +1:00) Prague
49	(GMT +1:00) Sarajevo,Skopje
50	(GMT +1:00) Warsaw,Zagreb
51	GMT +1:00) Brussels
52	(GMT +1:00) Copenhagen
53	(GMT +1:00) Madrid,Paris
54	(GMT +1:00) Amsterdam,Berlin
55	(GMT +1:00) Bern,Rome
56	(GMT +1:00) Stockholm,Vienna
57	(GMT +1:00) West Central Africa
58	(GMT +1:00) Windhoek
59	(GMT +2:00) Bucharest,Cairo
60	(GMT +2:00) Amman,Beirut
61	(GMT +2:00) Helsinki,Kyiv
62	(GMT +2:00) Riga,Sofia
63	(GMT +2:00) Tallinn,Vilnius
64	(GMT +2:00) Athens
65	(GMT +2:00) Damascus
66	(GMT +2:00) E.Europe
67	(GMT +2:00) Harare,Pretoria
68	(GMT +2:00) Jerusalem
69	(GMT +2:00) Kaliningrad (RTZ 1)
70	(GMT +2:00) Tripoli
71	(GMT +3:00) Moscow
72	(GMT +3:00) St.Petersburg
73	(GMT +3:00) Volgograd (RTZ 2)
74	(GMT +3:00) Kuwait,Riyadh
75	(GMT +3:00) Nairobi
76	(GMT +3:00) Baghdad
77	(GMT +3:00) Minsk, Istanbul
78	(GMT +3:30) Tehran
79	(GMT +4:00) Abu Dhabi,Muscat
80	(GMT +4:00) Baku,Tbilisi

Permitted Value	Time Zone Description
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
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

Capture Your Phone's Screen

You can capture your phone's current screen.

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

Task

1. Add the parameter `up.screenCapture.enabled` to your configuration.
2. Set the value to **1** and save.
3. On the device, go to **Settings > Basic > Preferences > Screen Capture**.
   Note you must repeat this step each time the device restarts or reboots.
4. Locate and record the phone's IP address at **Status > Platform > Phone > IP Address**.
5. Set the phone to the screen you want to capture.
6. In a web browser address field, enter `https://<phoneIPaddress>/captureScreen` where `<phoneIPaddress>` is the IP address you obtained from the phone.
7. Enter the username **Polycom** and the phone's current password.
   The web browser displays an image showing the phone's current screen. You can save the image as a .bmp or .jpeg file.

Related Links

Configuring the System Web Interface on page 55

Capture Your Device's Current Screen Parameters

Use the following parameters to get a screen capture of the current screen on your device.

`up.screenCapture.enabled`

0 (Default) - The Screen Capture menu is hidden on the phone.

1 - The Screen Capture menu displays on the phone.

When the phone reboots, screen captures are disabled from the Screen Capture menu on the phone.

Change causes system to restart or reboot.

`up.screenCapture.allowed`

0 (Default) - The Screen Capture feature is disabled.

1 - The Screen Capture feature is enabled.

Time and Date Wizard

Users signing into Skype for Business on the phone for the first time are prompted to set the time zone, time format, and date format before they start using the system.

This feature is enabled by default.

Time and Date Wizard Parameters

Use the following parameters to enable or disable the Time and Date Wizard.

`device.set`

0 (default) - Do not use any `device.xxx` fields to set any parameters.

1 - Use the `device.xxx` fields that have `device.xxx.set=1` . Set this to *1* only for the initial installation and set back to *0* after the initial installation.

device.lync.timeZone.set

0 (default) - Do not use the `device.xxx` value.

1 (default) - Use the `device.xxx` value.

For example, if `device.lync.timeZone.set = 1`, then use the value set for `device.lync.timeZone` .

device.lync.timeZone

1 (default) - Skype for Business Time Zone Control is enabled.

0 - Skype for Business Time Zone Control is disabled.

Setting up the Phone Theme

You can set the phone theme, labels, and colors that display on the user interface.

When the phone's Base Profile is set to Skype, the Skype for Business theme displays by default.

Theme Parameter

The following parameter configures the phone's theme.

up.uiTheme

Specifies the colors and icons used in the phone user interface. By default, the theme changes based on the set base profile. Poly doesn't recommend you change the default themes.
Default (default) - The phone displays the default Poly theme. Available for Generic and Skype for Business base profiles.

SkypeForBusiness - The phone displays the Skype for Business theme. Available for Generic and Skype for Business base profiles.

Phone Display Name

Configure the name that displays on the system, the connected monitor, and any devices wirelessly connected to the system.

The name you configure for the system, using any of the following parameters, displays in the subsequent priority order:

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

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

Display Name Parameters

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

bluetooth.device.name

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

NULL (default)

UTF-8 encoded string

reg.x.address

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

Null (default)

string address

reg.x.displayname

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

Null (default)

UTF-8 encoded string

reg.x.label

The text label that displays next to the line key for registration x.

The maximum number of characters for this parameter value is `256`; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters you use. Parameter values that exceed the phone's maximum display length are truncated by ellipses (...). The rules for parameter `up.cfgLabelElide` determine how the label is truncated.

Null (default)

UTF-8 encoded string

system.name

The system name that displays at the top left corner of the monitor, and at the top of the Global menu of the phone.

Enter a string, maximum 96 characters.

Number or Custom Label

You can choose to display a number, an extension, or a custom label on the Home Screen below the time and date.

Configure the Number or Label from the System

You can configure the display of the number or label on the Home screen from the system menu.

Task

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

Number and Label Parameters

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

homeScreen.placeACall.enable

0 - Does not display the label on the home screen.

homeScreen.customLabel

Specify the label to display on the phone's Home screen when `homeScreen.labelType="Custom"`. The label can be 0 to 255 characters.

Null (default)

homeScreen.labelLocation

Specify where the label displays on the screen.

StatusBar (default) - The phone displays the custom label in the status bar at the top of the screen.

BelowDate - The phone displays the custom label on the Home screen only, just below the time and date.

homeScreen.labelType

Specify the type of label to display on the phone's Home screen.

PhoneNumber (default)

- When the phone is set to use Lync Base Profile, the phone number is derived from the Skype for Business server.

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

PrimaryPhoneNumber – The status bar displays only the first phone number rather than all of the phone numbers.

None - Don't display a label.

reg.1.useteluriAsLineLabel

1 - If `reg.x.label`="Null" the tel URI/phone number/address displays as the label of the line key.

0 - If `reg.x.label`="Null" the value for `reg.x.displayName`, if available, displays as the label. If `reg.x.displayName` is unavailable, the user part of `reg.x.address` is used.

up.formatPhoneNumbers

1 (default) - Enables automatic number formatting.

0 - Disables automatic number formatting and numbers display separated by "-".

Direct Inward Dialing Number

The Direct Inward Dialing (DID) number assigned to the user on the Skype for Business server displays on the Lock, Home, and Incoming Call screens.

You can configure the format of the DID number to display on phones using parameter. You can also configure the phone to display DID numbers on phone screens of your choice with parameter.

Direct Inward Dialing Number Parameters

Use the following parameters to configure DID number.

up.DIDFormat

NumberAndExtension (default) – Display the DID number and extension.

NumberOnly – Display the DID number on the phone screen.

up.showDID

AllScreens (default) – Display the DID number on all the screens.

None – Disable DID number on phone.

LockedScreen – Display the DID number on the lockscreen.

StatusScreen – Display the DID number on the Statusscreen/Idle screen.

LockedAndStatusScreen – Display the DID number on the lock and Status/Idle screen.

Port Usage

This section lists ports used by Poly phones and ports you can configure.

Configuring Better Together over Ethernet (BToE) Firewall Ports for Poly Phones

The following table lists ports used by BToE application and the communication direction.

BToE Firewall Ports

Port Number	Type	Description	Direction
24802	UDP	Used for audio streaming	Phone (24802) <=> PC (24802)
6000	TCP	Used for Secure Shell (SSH) client connections to the BToE application (plink.exe)	PC (BToE service) (Dynamic) => PC (plink service) (6000) (Within PC)
Dynamic	TCP	plink.exe uses a dynamic port to connect to the phones	PC (Dynamic) => Phone (22)
22	TCP	Phones use this port to connect securely with computer applications	PC (Dynamic) => Phone (22)
2081	UDP	Phones use this port for discovery packet broadcasts	Phone(2081) => PC (2081)
24801	TCP	Phones and the BToE computer application communicate with each other using this non-secure port	Phone (plink service) => Phone (BToE service) (24801)
24804	TCP	Phones and the BToE computer application communicate with each other using this secure port connection.	Phone (24804) <=> PC (24804)

Inbound and Outbound Ports for Poly Phones with Skype for Business

This section provides port usage information when configuring network equipment to support Poly phones with Skype for Business.

For more information on port usage, visit the following articles on Microsoft TechNet:

- Port and protocol requirements for servers
- Skype for Business Online and Microsoft Teams

Inbound Ports for Poly Phones with Skype for Business

The following table lists the inbound IP ports currently used by Polycom UC Software running on the Poly phones with Skype for Business.

Inbound IP Ports

Inbound Port	Type	Protocol	Function	Default	Configurable Port Number
22	Static	TCP	SSH Administration	Off	No
80	Static	TCP	HTTP Pull Web interface, HTTP Push	Off	Yes
443	Static	TCP	HTTP Pull Web interface, HTTP Push	On	Yes
1023	Static	TCP	Telnet Diagnostics	Off	No
1024 - 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 - 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes
5060	Static	TCP/UDP	SIP signaling	On	No
5061	Static	TLS		On	No

Outbound Ports on Poly Phones with Skype for Business

The following table lists the outbound IP ports currently used by Polycom UC Software running on the Poly phones with Skype for Business.

Outbound IP Ports

Outbound Port	Type	Protocol	Function	Default	Configurable Port number
21	Static	TCP	FTP Provisioning, Logs	On	No
22	Static	TCP	SSH	On	No
53	Static	UDP	DNS	On	No
67	Static	UDP	DHCP Server	On	No
68	Static	UDP	DHCP Client		No
69	Static	UDP	TFTP Provisioning, Logs		No
80	Static	TCP	HTTP Provisioning, Logs, Web Interface		No
123	Static	UDP	NTP time server		No
389	Static	TCP/UDP	LDAP directory query		No

Outbound Port	Type	Protocol	Function	Default	Configurable Port number
443	Static	TCP	HTTPS Provisioning, Logs, Web Interface		No
514	Static	UDP	SYSLOG		No
636	Static	TCP/UDP	LDAP directory query		No
1024 - 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 - 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes
5060		TCP/UDP	SIP signaling	On	
5061		TCP	SIP over TLS signaling	On	
5222	Static	TCP	Polycom RealPresence Resource Manager: XMPP	On	No

Real-Time Transport Protocol (RTP) Port Parameters for Skype for Business

Use the following parameters to configure RTP packets and ports for the phones registered with Skype for Business.

`tcpIpApp.port.rtp.lync.audioPortRangeStart`

Determines the start port for the audio port range.

5350 (default)

1024 - 65436

`tcpIpApp.port.rtp.lync.audioPortRangeEnd`

Determines the end port for the audio port range.

5389 (default)

Min - 1024

Max - 65485

Client Media Port Ranges for QoE

To help deploy QoE, you can enable client media ports and configure unique port ranges on the Skype for Business Server.

Task

» Enable client media ports as shown in Configuring Port Ranges for your Microsoft Lync Clients in Lync Server 2013.

Configuring Security Options

Optimize security settings, such as changing the passwords for the phone, enabling users to lock their phones, and blocking administrator functions from phone users.

802.1X Authentication

Poly phones support standard IEEE 802.

1X authentication and the following EAP authentication methods:

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

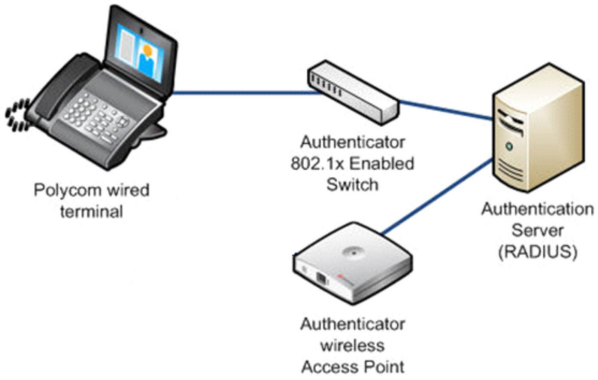


Figure 1: A typical 802.1X network configuration

802.1X Authentication Parameters

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

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

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

`device.net.dot1x.enabled`

Enable or disable 802.1X authentication

0 - Disabled

1 - Enabled

Change causes system to restart or reboot.

`device.net.dot1x.identity`

Set the identity (user name) for 802.1X authentication

String

Change causes system to restart or reboot

`device.net.dot1x.method`

Specify the 802.1X EAP method

EAP-None - No authentication

EAP-TLS,

EAP-PEAPv0-MSCHAPv2,

EAP-PEAPv0-GTC,

EAP-TTLS-MSCHAPv2,

EAP-TTLS-GTC,

EAP-FAST,

EAP-MD5

device.net.dot1x.password

Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS

String

Change causes system to restart or reboot.

device.net.dot1x.eapFastInBandProv

Enable EAP In-Band Provisioning for EAP-FAST

0 (default) - Disabled

1 - Unauthenticated, active only when the EAP method is EAP-FAST

device.pacfile.data

Specify a PAC file for EAP-FAST (optional)

Null (default)

0-2048 - String length

device.pacfile.password

The optional password for the EAP-FAST PAC file.

Null (default)

0-255 - String length

IEEE 802.1p/Q

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

- A valid VLAN ID is specified in the phone's network configuration.
- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or LLDP

IEEE 802.1p/Q Parameters

Use the following list to set values for IEEE 802.1p/Q parameters.

You can configure the user_priority specifically for RTP and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

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

- A valid VLAN ID specified in the phone's network configuration.

- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or CDP.

qos.ethernet.other.user_priority

Set user priority for packets without a per-protocol setting.

2 (Default)

0 - 7

qos.ethernet.rtp.video.user_priority

Set user-priority used for Video RTP packets.

5 (Default)

0 - 7

qos.ethernet.rtp.user_priority

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

5 (Default)

0 - 7

qos.ethernet.callControl.user_priority

Set the user-priority used for call control packets.

5 (Default)

0 - 7

Accessing the System Web Interface

When the Base Profile of a phone is set to **Skype**, access to the system web interface is disabled by default.

Administrators must enable access to a phone's system web interface from the phone menu system or using configuration parameters.

If a phone Base Profile is set to **Skype**, or you use the centralized provisioning method to enter user credentials to the configuration files, the phone displays a screen prompting an administrator to change the default Admin password (456). Poly strongly recommends that administrators change the default password. This password is not the Skype for Business Sign In password. The password you enter here is the same password administrators use to access the advanced settings on the phone menu and to log in to a phone's system web interface as an administrator.

Enable Access to the System Web Interface From the Phone Menu

When the phone's Base Profile is set to Skype, you can enable access to a phone's system web interface form the phone's menu system.

Task

1 On the phone, go to **Settings > Advanced**.
2 Enter the administrator password (the default is **456**).
3 Select **Administration Settings > Web Server Configuration**.
Web Server and Web Config Mode display.
4 Set **Web Server** to **Enabled**.
5 Set **Web Config Mode** to **HTTP Only**, **HTTPS Only**, or **HTTP/HTTPS** and tap the back button..

6 Select **Save Config** to save the web server configuration on the phone.

Configuring the System Web Interface

The security update for Skype for Business includes a device parameter and a corresponding device.set parameter.

Poly recommends using device.* parameters only if you are familiar with the centralized provisioning method and with Polycom UC Software.

Use the following parameters to enable and configure the system web interface.

`device.sec.coreDumpEncryption.enabled`

0 (default)

1

`device.sec.coreDumpEncryption.enabled.set`

0 (default)

1

`httpd.cfg.enabled`

Base Profile = Skype

0 (default) - The system web interface is disabled.

1 - The system web interface is enabled.

`httpd.cfg.secureTunnelRequired`

1 (default) - Access to the system web interface is allowed only over a secure tunnel (HTTPS) and non-secure (HTTP) is not allowed.

0 - Access to the system web interface is allowed over both a secure tunnel (HTTPS) and non-secure (HTTP).

`httpd.enabled`

Base Profile = Skype

0 (default) - The web server is disabled.

1 - The web server is enabled.

Related Links

Capture Your Phone's Screen on page 45

Securing Audio Using an MKI

For secure audio communications, phones offer support for the crypto header with or without an MKI in the SDP offer.

The following optional parameter allows you to include the crypto header in the SDP that uniquely identifies the SRTP stream within an SRTP session. The far end can choose to include a crypto with or without MKI.

`sec.srtp.mki.enabled`

1 (default) - The phone offers two cryptos in the SDP offer: one without an MKI, and one with a four-byte MKI parameter in the SDP message of the SIP INVITE / 200 OK.

0 - The phone offers only one non-MKI crypto in the SDL offer.

Administrator and User Passwords

You can change the default administrator and user passwords.

When you set the Base Profile to Skype or update your phones to UC Software 5.x.x or later, the phones display a message prompting you to change the default administrator password (`456`). You're required to change the administrator password to another password other than the default. This password isn't the Skype for Business user Sign In password. The default administrator password enables administrators to access advanced settings menu on the phone menu and to log in to a phone's system web interface as an administrator.

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

- The pop-up prompt when the phone first registers
- Phone menu
- System web interface
- Use the parameter `reg.1.auth.password` in the template configuration file

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

- Administrative password: `456`
- User password: `123`

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

Change the Default Administrator Password on the Phone

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

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

Task

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

Change the Default Passwords in the System Web Interface

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

Task

1. In your web browser, enter the phone's IP address into the URL field to access the system web interface.
2. Go to **Settings > Change Password**.
3. Update the passwords for the **Admin** and **User**.

Administrator and User Password Parameters

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

`sec.pwd.length.admin`

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

1 (default)

0 - 32

Change causes system to restart or reboot.

sec.pwd.length.user

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

2 (default)

0 - 32

Change causes system to restart or reboot.

up.echoPasswordDigits

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

0 - The phone displays only asterisks for the password characters.

device.auth.localAdminPassword

Specify a local administrator password.

0 - 32 characters

You must use this parameter with: `device.auth.localAdminPassword.set="1"`

device.auth.localAdminPassword.set

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

1 - Enables overwriting the local admin password when provisioning using a configuration file.

Device Lock for Skype for Business

You can configure phones to be protected with a lock code that enables users to access personal settings from different phones.

You must enable Device Lock on the Skype for Business server. After you enable Device Lock, you can enable or disable Device Lock and configure options for your phones using Poly parameters. You cannot enable or disable Device Lock using the Web Configuration Utility.

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

Administrators can configure phone behavior after six unsuccessful user unlock attempts. If users forget their lock code, they can reset it from the phone when signed in to their Skype for Business account. If users sign in to their Skype for Business account using the Web Sign-In method, they cannot reset their lock code from the phone.

Users must sign into the phone before using Device Lock. If a phone restarts or reboots after a user sets the lock code, the phone is locked after the restart or reboot. Users can lock the phone from the phone screen or Skype for Business client when the phone and computer are connected using BToE. If Device Lock is used in conjunction with BToE, the phone and computer always remain synchronized if either the phone or computer restarts or reboots. If the BToE connection is broken between phone and computer, the phone is locked.

You can also:

- Define authorized outbound emergency numbers from a locked device
- Set up a minimum lock code length on the Skype for Business server

Profile Photo on Device Lock Screen

When a user is signed in to their Skype for Business account, that user's Microsoft Exchange or public website profile photo displays on the Lock screen.

The profile photo appears when the Device Lock feature and the Microsoft Exchange Service are enabled. Profile photos set using Active Directory are not supported and do not display on the phone.

Adding Authorized Emergency Contacts on a Locked Device

You can configure emergency contact numbers that users can call on a locked device in one of two ways.

- Create a policy for emergency numbers on the Skype for Business Server. Note that this method must be supported by a voice routing trunk configuration.
- Create an authorized list for a line by configuring the value of the parameter phoneLock.authorized.x.value to a Tel URI or SIP URI, for example, `phoneLock.authorized.1.value="cwi57@cohovineyard.com"`.

When the Base Profile of the phone is set to Skype for Business, you can configure the phone to set the order of display for the authorized emergency numbers when the device is locked.

Device Lock for Skype for Business Parameters

The following parameters configure the Skype for Business Device Lock feature.

`feature.deviceLock.enable`

Enables or disables the Device Lock feature on the phone.

1 (default) - Device Lock is enabled.

0 - Device Lock is disabled.

`phoneLock.authorized.x.value`

Specify a registered line for 'x' and an authorized call list when the device is locked using a Tel URI or SIP URI, for example, `phoneLock.authorized.1.value="cwi57@cohovineyard.com"`.

`up.btoeDeviceLock.timeOut`

Configure a time delay after which the phone locks when the user locks the computer paired with the phone.

10 seconds (default)

0 - 40 seconds

`up.configureDeviceLockAuthList`

EmergencyNumberAtTop (default) - The E911 emergency number will be displayed followed by authorized numbers when the phone is locked.

EmergencyNumberAtBottom - The authorized numbers will be displayed followed by the E911 number when the phone is locked.

EmergencyNumberDisabled - Only the authorized numbers will be displayed when the phone is locked.

`up.deviceLock.createLockTimeout`

Specify the timeout in minutes after which the Create Lock Code screen disappears and the user is signed out.

0 (default) - No timeout for the Create Lock Code prompt.

0 - 3 minutes - If the user does not provide input to the Create Lock Code within the time you specify, the Create Lock Code screen disappears and the user is signed out of the phone.

`up.deviceLock.signOutOnIncorrectAttempts`

Specify whether to sign out the user from the phone after six unsuccessful attempts to unlock the phone.

0 (default) - After six unsuccessful unlock attempts, the phone displays a message indicating a countdown of 60 seconds after which the user can attempt to unlock the phone.

1 - After six unsuccessful unlock attempts, the user is signed out of the phone, must sign in again, and is prompted to create a new lock code.

Configuring Privacy Settings

Poly UC software enables you to block user-specific information such as SIP URI and telephone number leakage.

Privacy Configuration Parameter

Use the parameter below to configure how the phone handles user-specific information such as SIP URI and telephone number leakage.

`voIpProt.SIP.requestValidation.x.request`

Sets the name of the method for which validation is applied.

Null (default)

INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE

ALL - Phone does not honor the above request methods received from unknown sources.

Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.

Change causes system to restart or reboot.

Smart Login on Poly Phones

Smart Login determines if a network environment is capable of PIN Authentication.

If the STS-URI is not configured via DHCP Option43 or manually through configuration files, then PIN Authentication will not be enabled for the phone or in the Web Configuration Utility for a Skype for Business sign in.

Simple Certificate Enrollment Protocol

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

Simple Certificate Enrollment Protocol Parameters

Use the following parameters to configure Simple Certificate Enrollment Protocol (SCEP).

`SCEP.CAFingerprint`

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

null (default)

0 - 255 characters

`SCEP.certPoll.retryCount`

Specify the number of times to poll the SCEP server when the SCEP server returns a Certificate Enrollment Response Message with pkiStatus set to `pending`.

12 (default)

1 - 24

SCEP.certPoll.retryInterval

Specify the number of seconds to wait between poll attempts when the SCEP server returns a Certificate Enrollment Response Message with pkiStatus set to `pending`.

300 (default)

300 - 3600

SCEP.certRenewalRetryInterval

Specify the time interval to retry certificate renewal.

86400 seconds (default)

28800 - 259200 seconds

SCEP.certRenewalThreshold

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

80 (default)

50 - 100

SCEP.challengePassword

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

null (default)

0 - 255 characters

SCEP.csr.commonName

Specify the common name to use for CSR generation.

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

null (default)

0 - 64

SCEP.csr.country

Specify the country name to use for CSR generation.

null (default)

0 - 2

SCEP.csr.email

Specify the email address to use for CSR generation.

null (default)

0 - 64

SCEP.csr.locality

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

null (default)

0-64 characters

SCEP.csr.organization

Specify the organization name to use for CSR generation.

null (default)

0 - 64

SCEP.csr.organizationUnit

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

null (default)

0-64 characters

SCEP.csr.state

Specify the state name to use for CSR generation.

null (default)

0 - 128 characters

SCEP.enable

0 (default) - Disable the SCEP feature.

1 - Enable the SCEP feature.

SCEP.enrollment.retryCount

Specify the number of times to retry the enrollment process in case of enrollment failure.

12 (default)

1 - 24

SCEP.enrollment.retryInterval

Specify the time interval to retry the enrollment process.

300 seconds (default)

300 - 3600 seconds

SCEP.http.password

Specify the password that authenticates with the SCEP server.

null (default)

string, max 255 characters

SCEP.http.username

Specify the user name that authenticates with the SCEP server.

null (default)

string, max 255 characters

SCEP.url

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

null (default)

0 - 255 characters

SCEP.verifyWithScepCaCert

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

1 (default)

0 - Use settings from TLS Provisioning Profile.

Device Parameters

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

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

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

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

The <device/> parameters are designed to be stored in flash memory and for this reason, the phone does not upload <device/> parameters to the <MAC>-web.cfg or <MAC>-phone.cfg override files if you make configuration changes through the system web interface or phone interface. This design protects your ability to manage and access the phones using the standard set of parameters on a provisioning server after the initial software installation.

Changing Device Parameters

Keep the following in mind when modifying device parameters:

- Note that some parameters may be ignored. For example, if DHCP is enabled, it will still override the value set with device.net.ipAddress.
- Though individual parameters are checked to see whether they are in range, the interaction between parameters is not checked. If a parameter is out of range, an error message displays in the log file and the parameter is not be used.
- Incorrect configuration can put the phones into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, and server B has a configuration file that specifies that server A should be used.

To detect errors, including IP address conflicts, Polycom recommends that you test the new configuration files on two phones before initializing all phones.

Types of Device Parameters

The following parameters outline the three types of <device/> parameters, their permitted values, and the default value.

device.set

0 (default) - Don't use any device.xxx fields to set any parameters. Set this to 0 when you are not making changes to device parameters.

1 - Use the device.xxx fields that have device.xxx.set="1". Set this to 1 when you are making changes to device parameters.

Change may cause system to restart or reboot.

`device.xxx`

Configuration parameter.

String

Change may cause system to restart or reboot.

`device.xxx.set`

0 (default) - Don't use the `device.xxx`value.

1 - Use the `device.xxx` value.

For example, if `device.net.ipAddress.set="1"`, then use the value set for `device.net.ipAddress`.

Change may cause system to restart or reboot.

Parameter List Conventions

For each feature, Poly provides a list of parameters in XML that you can use to configure feature settings.

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

Using XML

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

When configuring the parameters as XML, you must enter parameter names as attributes of a well-formed XML syntax. You can organize parameters into any well-formed XML element structure.

A **parameter="value"** pair is equivalent to an XML **attribute="value"** pair. For example:

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

Parameter List Template and Examples

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

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

`parameter.name`

A parameter's description, applicability, or dependencies, as needed.

The parameter's permitted values, the default value, and the value's unit of measure, such as seconds, Hz, or dB.

An indication when a change in a parameter's value causes a phone restart or reboot.

Note: A note that highlights critical information you need to know.

The following sample parameter lists show a few example parameters and some XML representations showing how to use them.

`feature.acousticFenceUI.enabled`

0 (default) - Hide the Acoustic Fence configuration setting on the phone.

1 - Display the Acoustic Fence configuration setting on the phone.

Change causes system to reboot or restart.

XML Representation

```
<element feature.acousticFenceUI.enabled="1" />
```

reg.x.callsPerLineKey

Set the maximum number of concurrent calls for a single registration *x* that you specify. This parameter applies to all line keys using registration *x*. If registration *x* is a shared line, an active call counts as a call appearance on all phones sharing that registration.

This per-registration parameter overrides the global parameter `call.callsPerLineKey`.

24 (default)

1 - 24

1 - 8

XML Representation

```
<registration
    reg.1.callsPerLineKey="3"
    reg.2.callsPerLineKey="1"
    reg.3.callsPerLineKey="1"
/>
```

Device Parameters

Use the following <device/> parameters to configure some device settings.

Note: The default values for the <device/> parameters are set at the factory when the phones are shipped. For a list of the default values, see the latest Product Shipping Configuration Change Notice at Poly Engineering Advisories and Technical Notifications.

device.auth.localAdminPassword

Set the phone's local administrative password. The minimum length is defined by `sec.pwd.length.admin`.

String (32 character max)

device.auth.localUserPassword

Set the phone user's local password. The minimum length is defined by `sec.pwd.length.user`.

String (32 character max)

device.auxPort.enable

Enable or disable the phone auxiliary port.

0 - Disable the phone auxiliary port.

1 (default) - Enable the phone auxiliary port.

Change causes system to restart or reboot.

device.baseProfile

NULL (default)

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

USBOptimized - Optimizes the phone as a USB device.

MSTeams - Sets the base profile for Microsoft Teams deployments.

Change causes system to restart or reboot.

device.dhcp.bootSrvOpt

When the boot server is set to Custom or Custom+Option66, specify the numeric DHCP option that the phone looks for.

160 (default)

128 to 254

Change causes system to restart or reboot.

device.dhcp.bootSrvOptType

Set the type of DHCP option the phone looks for to find its provisioning server if `device.dhcp.bootSrvUseOpt="Custom"`.

IP (default) - The IP address provided must specify the format of the provisioning server.

String - The string provided must match one of the formats specified by `device.prov.serverName`.

Change causes system to restart or reboot.

device.dhcp.bootSrvUseOpt

Default - The phone looks for option number 66 (string type) in the response received from the DHCP server. The DHCP server sends address information in option 66 that matches one of the formats described for `device.prov.serverName`.

Custom - The phone looks for the option number specified by `device.dhcp.bootSrvOpt` and the type specified by `device.dhcp.bootSrvOptType` in the response received from the DHCP server.

Static - The phone uses the boot server configured through the provisioning server `device.prov.*` parameters.

Custom and Default - The phone uses the custom option first or use option 66 if the custom option is not present.

Change causes system to restart or reboot.

device.dhcp.dhcpVlanDiscOpt

Set the DHCP private option to use when `device.dhcp.dhcpVlanDiscUseOpt="Custom"`.

129 (default)

128 to 254

Change causes system to restart or reboot.

device.dhcp.dhcpVlanDiscUseOpt

Set how VLAN Discovery occurs.

Disabled - No VLAN discovery through DHCP.

Fixed (default) - Use predefined DHCP vendor-specific option values of 128, 144, 157 and 191 (`device.dhcp.dhcpVlanDiscOpt` is ignored).

Custom - Use the number specified by `device.dhcp.dhcpVlanDiscOpt`.

Change causes system to restart or reboot.

device.dhcp.enabled

Enable or disable DHCP.

If the phone can't communicate with the DHCP server, the phone's status bar reports network down. The phone communicates with the DHCP server every 5 minutes to receive or validate the IP Address..

0 - DHCP is disabled.

1 (default) - DHCP is enabled.

Change causes system to restart or reboot.

device.dhcp.option60Type

Set the DHCP option 60 type.

Binary - Vendor-identifying information is in the format defined in RFC 3925.

ASCII - Vendor-identifying information is in ASCII format.

Change causes system to restart or reboot.

device.dns.altSrvAddress

Sets the secondary server where the phone directs DNS queries.

Server Address

Change causes system to restart or reboot.

device.dns.domain

Set the phone's DNS domain.

String

Change causes system to restart or reboot.

device.dns.serverAddress

Sets the primary server where the phone directs DNS queries.

Server Address

Change causes system to restart or reboot.

device.hostname

Specify a hostname for the phone when using DHCP by adding a hostname string to the phone's configuration.

If `device.host.hostname.set="1"` and `device.host.hostname="Null"`, the DHCP client uses option 12 to send a predefined host name to the DHCP registration server using `Polycom_<MACaddress>`.

String —The maximum length of the host name string is ≤ 255 bytes, and the valid character set is defined in RFC 1035.

Change causes system to restart or reboot.

device.net.cdpEnabled

Determine if the phone attempts to determine its VLAN ID and negotiate power through CDP.

0 - Disabled

1 - Enabled

Change causes system to restart or reboot.

device.net.dot1x.anonid

EAP-TTLS and EAP-FAST only. Set the anonymous identity (user name) for 802.1X authentication.

String

Change causes system to restart or reboot.

device.net.dot1x.enabled

Enable or disable 802.1X authentication.

0 - Disabled

1 - Enabled

Change causes system to restart or reboot.

device.net.dot1x.identity

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

String

Change causes system to restart or reboot.

device.net.dot1x.method

Specify the 802.1X authentication method, where EAP-NONE means no authentication.

EAP-None

EAP-TLS

EAP-PEAPv0-MSCHAPv2

EAP-PEAPv0-GTC

EAP-TTLS-MSCHAPv2

EAP-TTLS-GTC

EAP-FAST

EAP-MD5

device.net.dot1x.password

Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.

String

Change causes system to restart or reboot.

device.net.etherModeLAN

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

Poly recommends that you don't change this setting.

0 - Auto (default)

1 - 10HD

2 - 10FD

3 - 100HD

4 - 100FD

5 - 1000FD

HD means half-duplex and FD means full duplex.

Change causes system to restart or reboot.

device.net.etherModePC

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

-1 - Disables the PC port

0 - Auto (default)

1 - 10HD

2 - 10FD

3 - 100HD

4 - 100FD

5 - 1000FD

HD means half-duplex and FD means full duplex.

Change causes system to restart or reboot.

device.net.etherStormFilter

1 - DoS storm prevention is enabled and received Ethernet packets are filtered to prevent TCP/IP stack overflow caused by bad data or too much data.

0 - DoS storm prevention is disabled.

Change causes system to restart or reboot.

device.net.etherStormFilterPpsValue

Set the corresponding packets per second (pps) for storm filter and to control the incoming network traffic.

17 to 40

38 (default)

device.net.etherStormFilterPpsValue.set

0 (default) - You can't configure the `device.net.etherStormFilterPpsValue` parameter.

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

device.net.ipAddress

Set the phone's IP address.

This parameter is disabled when `device.dhcp.enabled="1"`.

String

Change causes system to restart or reboot.

device.net.IPgateway

Set the phone's default router.

IP address

Change causes system to restart or reboot.

device.net.lldpEnabled

0 - The phone doesn't attempt to determine its VLAN ID.

1 - The phone attempts to determine its VLAN ID and negotiate power through LLDP.

Change causes system to restart or reboot.

device.net.lldp.extendedDiscovery

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

0 (default)

Change causes system to restart or reboot.

This parameter overrides `net.lldp.extendedDiscovery`.

device.net.lldpFastStartCount

Specify the number of consecutive LLDP packets the phone sends at the time of LLDP discovery, which are sent every one second.

5 (default)

3 to 10

device.net.subnetMask

Set the phone's subnet mask.

This parameter is disabled when `device.dhcp.enabled="1"`.

Subnet mask

Change causes system to restart or reboot.

device.net.vlanId

Set the phone's 802.1Q VLAN identifier.

Null - No VLAN tagging.

0 to 4094

Change causes system to restart or reboot.

device.prov.maxRedunServers

Set the maximum number of IP addresses to use from the DNS.

1 to 8

Change causes system to restart or reboot.

device.prov.password

Set the password for the phone to log in to the provisioning server, which may not be required.

If you modify this parameter, the phone reprovisions. The phone may also reboot if the configuration on the provisioning server has changed.

String

Change causes system to restart or reboot.

device.prov.redunAttemptLimit

Set the maximum number of attempts to attempt a file transfer before the transfer fails. When multiple IP addresses are provided by DNS, one attempt is considered to be a request sent to each server.

1 to 10

Change causes system to restart or reboot.

device.prov.redunInterAttemptDelay

Set the number of seconds to wait after a file transfer fails before retrying the transfer. When multiple IP addresses are returned by DNS, this delay only occurs after each IP has been tried.

0 to 300

Change causes system to restart or reboot.

device.prov.serverName

IP address

Domain name string

URL

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

device.prov.serverType

Set the protocol the phone uses to connect to the provisioning server. Active FTP is not supported for BootROM version 3.0 or later, and only implicit FTPS is supported.

FTP (default)

TFTP

HTTP

HTTPS

FTPS

Change causes system to restart or reboot.

device.prov.tagSerialNo

0 - The phone's serial number (MAC address) isn't included in the User-Agent header of HTTP/HTTPS transfers and communications to the microbrowser and web browser.

1 - The phone's serial number is included.

device.prov.upgradeServer

Specify the URL or path for a software version to download to the device. The phone will use the path specified in this parameter, if it is a non-NULL value, to look for the sip.ld software file. Otherwise, it will use the path specified in the APP_FILE_PATH attribute in the master configuration file.

NULL (default)

String

0 to 255 characters

device.prov.user

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

If you modify this parameter, the phone reprovisions, and it may reboot if the configuration on the provisioning server has changed.

String

device.sec.configEncryption.key

Set the configuration encryption key used to encrypt configuration files.

String

For more information, see the section on Configuration File Encryption.

Change causes system to restart or reboot.

device.sec.coreDumpEncryption.enabled

Determine whether to encrypt the core dump or bypass the encryption of the core dump.

0 - Encryption of the core dump is bypassed.

1 (default) - the core dump is encrypted.

device.sec.TLS.customDeviceCert1.privateKey
device.sec.TLS.customDeviceCert2.privateKey

Enter the corresponding signed private key in PEM format (X.509).

Size constraint is 4096 bytes for the private key.

device.sec.TLS.customDeviceCert1.publicCert
device.sec.TLS.customDeviceCert2.publicCert

Enter the signed custom device certificate in PEM format (X.509).

Size constraint is 8192 bytes for the device certificate.

device.sec.TLS.customDeviceCert1.set
device.sec.TLS.customDeviceCert2.set

Use to set the values for parameters `device.sec.TLS.customDeviceCertX.publicCert` and `device.sec.TLS.customDeviceCertX.privateKey`.

Size constraints are 4096 bytes for the private key and 8192 bytes for the device certificate.

0 (default) - Disabled

1 - Enabled

device.sec.TLS.profile.caCertList1 device.sec.TLS.profile.caCertList2

Choose the CA certificate(s) to use for TLS Platform Profile 1 and TLS Platform Profile 2 authentication:

Builtin - The built-in default certificate

BuiltinAndPlatform - The built-in and Custom #1 certificates

BuiltinAndPlatform2 - The built-in and Custom #2 certificates

All - Any certificate (built in, Custom #1 or Custom #2)

Platform1 - Only the Custom #1 certificate

Platform2 - Only the Custom #2 certificate

Platform1AndPlatform2 - Either the Custom #1 or Custom #2 certificate

device.sec.TLS.profile.cipherSuite1 device.sec.TLS.profile.cipherSuite2

Enter the cipher suites to use for TLS Platform Profile 1 and TLS Platform Profile 2

String

device.sec.TLS.profile.cipherSuiteDefault1
device.sec.TLS.profile.cipherSuiteDefault2

Determine the cipher suite to use for TLS Platform Profile 1 and TLS Platform profile 2.

0 - The custom cipher suite is used.

1 - The default cipher suite is used.

device.sec.TLS.profile.deviceCert1 device.sec.TLS.profile.deviceCert2

Choose the device certificate(s) for TLS Platform Profile 1 and TLS Platform Profile 2 to use for authentication.

Builtin

Platform1

Platform2

device.sec.TLS.profileSelection.dot1x

Choose the TLS Platform Profile to use for 802.1X.

PlatformProfile1

PlatformProfile2

device.sec.TLS.profileSelection.provisioning

Set the TLS Platform Profile to use for provisioning.

PlatformProfile1

PlatformProfile2

Change causes system to restart or reboot.

device.sec.TLS.profileSelection.syslog

Set the TLS Platform Profile to use for syslog.

PlatformProfile1

PlatformProfile2

Change causes system to restart or reboot.

device.sec.TLS.prov.strictCertCommonNameValidation

0 - Disables common name validation.

1 (default) - Provisioning server always verifies the server certificate for the `commonName/SubjectAltName` match with the server hostname that the phone is trying to connect.

device.sec.TLS.syslog.strictCertCommonNameValidation

0 - Disables common name validation.

1 - Syslog always verifies the server certificate for the `commonName/SubjectAltName` match with the server hostname that the phone is trying to connect.

device.sec.TLS.syslog.strictCertCommonNameValidation

0 - Disables common name validation.

1 (default) - Verify the 802.1x server certificate for the `commonName/SubjectAltName` match with the server hostname that the phone is trying to connect.

device.sntp.gmtOffset

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

-43200 to 46800

device.sntp.gmtOffsetcityID

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

NULL (default)

0 to 126

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

device.sntp.serverName

Enter the SNTP server where the phone obtains the current time.

IP address

Domain name string

device.syslog.facility

Determine a description of what generated the log message.

0 to 23

For more information, see RFC 3164.

device.syslog.prependMac

0

1 - The phone's MAC address is prepended to the log message sent to the syslog server.

Change causes system to restart or reboot.

device.syslog.renderLevel

Specify the logging level for the lowest severity of events to log in the syslog. When you choose a log level, the log includes all events of an equal or greater severity level, but it excludes events of a lower severity level.

0 or 1 - SeverityDebug(7).

2 or 3 - SeverityInformational(6).

4 - SeverityError(3).

5 - SeverityCritical(2).

6 - SeverityEmergency(0).

Change causes system to restart or reboot.

device.syslog.serverName

Set the syslog server IP address or domain name string.

IP address

Domain name string

device.syslog.transport

Set the transport protocol that the phone uses to write to the syslog server.

None - Transmission is turned off but the server address is preserved.

UDP

TCP

TLS

Certificates

If you need to set up a remote worker, you must manually install a certificate to the phone.

You also have the option to create your own XML configuration file and upload it to a phone using the Web Configuration Utility.

You can manually install certificates on a per-phone basis only. You must use Base64 format.

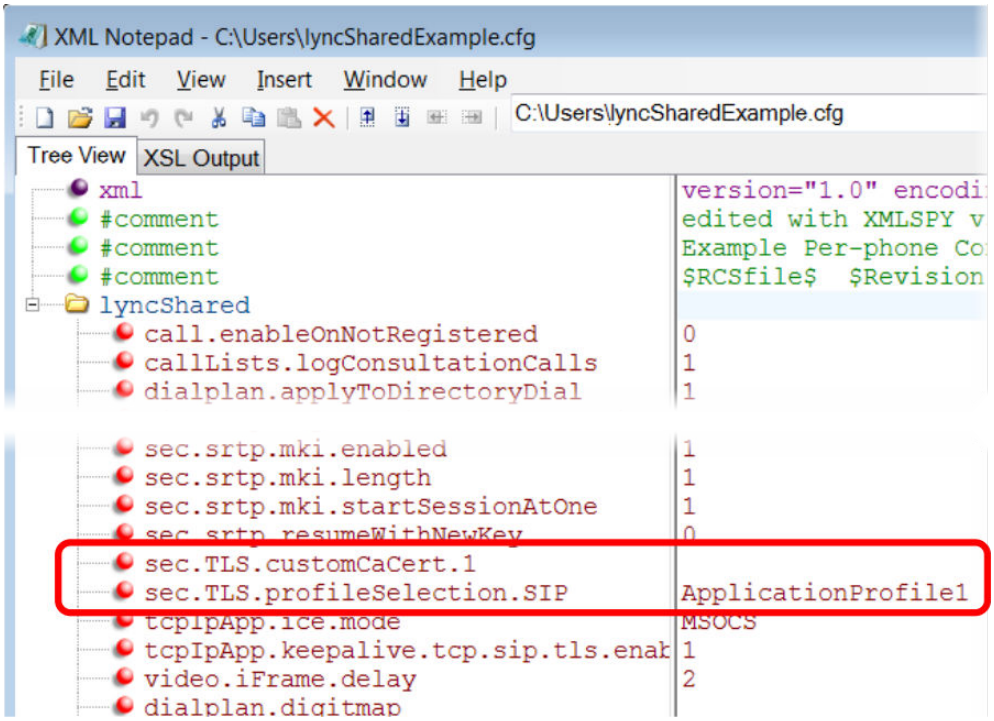
When phones are signed in and the software is downgraded, the phones will be in the signed-in state until the User Certificates are valid.

If you are setting up your network and you want more information on certificate options see Configure the Network.

Install a Certificate Using Configuration Files

You can manually install a certificate using configuration parameters in the template files available with UC Software.

1. Enter the following two parameters to a configuration file in your Skype for Business directory.
2. Enter the certificate and application profile as values for the two parameters:
   - `sec.TLS.customCaCert.1=<enter the certificate>`
   - `sec.TLS.profileSelection.SIP=<ApplicationProfile1>`

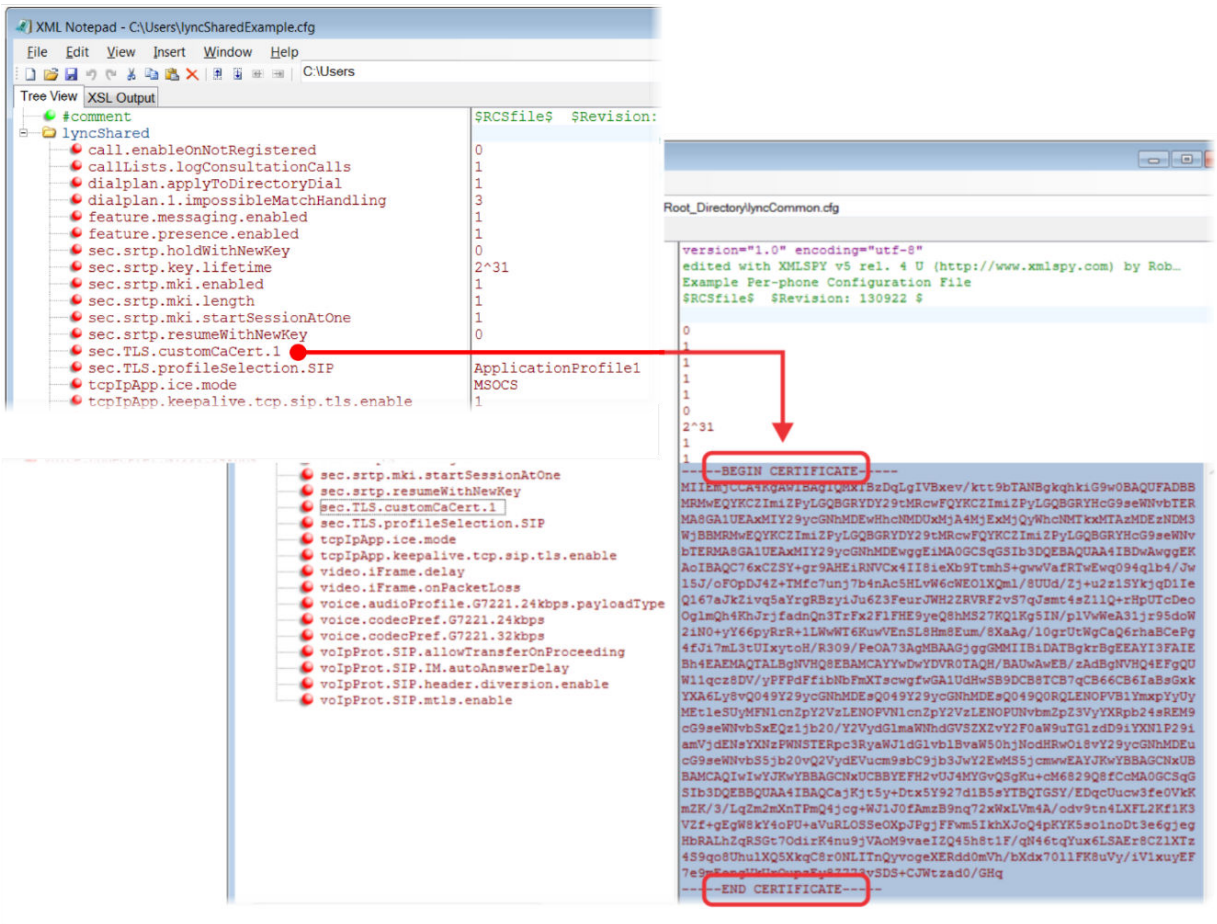


You can also enter the certificate by doing one of the following:

- Add the two parameters in an XML file you create with an XML editor.
- Add the two parameters to an existing configuration file you are using.

Task

» Enter the root CA certificate, in Base64 format, in `sec.TLS.customCaCert.1` and set the application profile in `sec.TLS.profileSelection.SIP` .



You have successfully installed a security certificate.

Manually Install a Certificate with the System Web Interface

You can use the system web interface to install a certificate manually.

Task

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and select **Submit**.
3. Go to **Utilities > Import & Export Configuration**.
4. Under **Import Configuration**, click **Choose File**.
5. In the dialog, choose the XML configuration file you created and click **Import**.
   The XML configuration file is successfully loaded to the phone.
6. To verify that the file is loaded, go to **Menu > Settings > Status > Platform > Configuration**.

Online Certificate Status Protocol

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

Online Certificate Status Protocol Parameter

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

device.sec.TLS.OCSP.enabled

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

0 (default) OCSP is disabled.

1 – OCSP is enabled

Change causes system to restart or reboot.

Directories and Contacts

You can configure phones with a local contact directory and link contacts to speed dial buttons.

Additionally, call logs stored in the Missed Calls, Received Calls, and Placed Calls call lists let you view user phone events like remote party identification, time and date of call, and call duration. This section provides information on contact directory, speed dial, and call log parameters you can configure on your phone.

Unified Contact Store

Administrators can unify users' contacts with Microsoft Exchange Server to enable users to access and manage contacts from any application or device synchronized with the Exchange Server including Poly phones, Skype for Business client, Outlook, or Outlook Web Application from a mobile device.

For example, if a user deletes a contact from a phone, the contact is also deleted on the Skype for Business client. Note users can manage (move, copy) contacts across Groups only on the Skype for Business client and Group contacts on the phone stay unified.

When an administrator enables Unified Contact Store, users can:

- Add a contact
- Delete a contact
- Add and delete a Distribution List (DL) group
- Manage contacts or groups

To set up this feature, administrators must use a PowerShell command using the instructions on the Microsoft TechNet web site Planning and deploying unified contact store in Lync Server 2013.

Configuring Contacts

The following parameter enables the contact directories.

up.queryContactInfo

Enable or disable the parameter to retrieve the details of a specific contact from the Active Directory.

0 (default) - Disabled

1 - Enabled

Call Lists

The phone records and maintains user phone events to a call list, which contains call information such as remote party identification, time and date of the call, and call duration.

The list is stored on the provisioning server as an XML file named <*MACaddress*>-calls.xml. If you want to route the call list to another server, use the `CALL_LISTS_DIRECTORY` field in the primary configuration file. All call lists are enabled by default.

The phone maintains all the calls in three separate user accessible call lists: Missed Calls, Received Calls, and Placed Calls. Users can clear lists manually on their phones, or delete individual records or all records in a group (for example, all missed calls).

Call List Parameters

Use the following parameters to configure call lists.

callLists.collapseDuplicates

Generic Base Profile - 1 (default)

1 - Consecutive incomplete calls to/from the same party and in the same direction are collapsed into one record in the calls list. The collapsed entry displays the number of consecutive calls.

0 - Each call is listed individually in the calls list.

callLists.logConsultationCalls

Generic Base Profile - 1 (default)

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

1 - Each consultation call is listed individually in the calls list.

feature.callList.enabled

1 (default) - Allows you to enable the missed, placed, and received call lists on all phone menus including the Home screen and dialpad.

0 - Disables all call lists.

feature.callListMissed.enabled

0 (Default) - The missed call list is disabled.

1 - The missed call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

feature.callListPlaced.enabled

0 (Default) - The placed call list is disabled.

1 - The placed call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

feature.callListReceived.enabled

0 (Default) - The received call list is disabled.

1 - The received call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

feature.exchangeCallLog.enabled

If Base Profile is:

Generic - 0 (default)

1 - The Exchange call log feature is enabled, user call logs are synchronized with the server, and the user call history of Missed, Received, and outgoing calls can be retrieved on the phone.

You must also enable the parameter `feature.callList.enabled` to use the Exchange call log feature.

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

Local Contact Directory Parameters

The following parameters configure the local contact directory.

`contactPhotoIntegration.hideMyPhoto`

Don't show the signed-in user's photo on the line key but still show other users' photos.

0 (default) - Disable the Hide My Photo feature.

1 - Enable the Hide My Photo feature.

`dir.local.contacts.maxNum`

Set the maximum number of contacts that can be stored in the Local Contact Directory. The maximum number varies by phone model, refer to section 'Maximum Capacity of the Local Contact Directory'.

Change causes system to restart or reboot.

`dir.local.readonly`

0 (default) - Disable read-only protection of the local Contact Directory.

1 - Enable read-only protection of the local Contact Directory.

`feature.directory.enabled`

0 - The local contact directory is disabled.

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

`dir.search.field`

Specify whether to sort contact directory searches by first name or last name.

0 (default) - Last name.

1 - First name.

`feature.pauseAndWaitDigitEntryControl.enabled`

1 (default) - Enable processing of control characters in the contact phone number field. When enabled, "," or "p" control characters cause a one-second pause.

For example, a "," or "p" control character causes a one-second pause. A ";" or "w" control character causes a user prompt that allows a user-controlled wait. Subsequent digits entered to the contact field are dialed automatically.

0 - Disable processing of control characters.

`up.regOnPhone`

0 (default) - Contacts you assign to a line key display on the phone in the position assigned.

1 - Contacts you assign to a line key are pushed to the attached expansion module.

Change causes system to restart or reboot.

Outlook Contact Photo Integration

You can configure the phone to display profile photos for the registered line and all Skype for Business contacts, if a photo is set for the Skype for Business or Microsoft Exchange account.

When enabled, a profile photo shows for contacts on all contact-related screens, including the Call, Recent Calls, and Directory search screens, as space permits. Set the parameter `feature.contactPhotoIntegration.enabled` = 1 to enable outlook photos to display on the phone.

Contact Photo Integration Limitations

The following are limitations on the phone with the Outlook Photo Integration feature:

- The phone cannot access contact photos for non-federated accounts, from image URLs, or imported from Active Directory.

Outlook Contact Photo Parameters

Use the following parameters to configure Skype for Business or Microsoft Exchange profile photos to display on the phone for contacts on supported contact screens.

`feature.contactPhotoIntegration.enabled`

Set to retrieve and display Outlook profile photos for contacts on the phone.

1 (default) - Retrieves profile photos from Outlook and displays the photos for contacts.

0 - Does not show Outlook contact photos.

`contactPhotoIntegration.videoMute`

Set to display the profile photo for the signed-in user's video mute icon.

1 (default) - Shows the signed-in user's profile photo when on video mute.

0 - Shows the generic video mute icon.

Call Controls

This chapter shows you how to configure call control features.

Call Forwarding with Skype for Business

The Skype for Business server automatically sends call forwarding functionality in-band to the phones.

With Call Forwarding enabled on the Skype for Business server, you can override Microsoft settings from a provisioning server using the Poly parameters in the following list or from the system web interface.

Disabling call forwarding on the Microsoft server also disables call forwarding on the phone. To disable call forwarding sent in-band from the Microsoft server, disable the settings for call forwarding and simultaneous ring on the Microsoft server.

`feature.forward.enable`

1 (default) - Enables call forwarding from the local interface.

0 - Disables call forwarding from the main menu.

`homeScreen.forward.enable`

1 (default) - Displays the **Forward** icon on the **Home** screen.

0 - Removes the **Forward** icon from the **Home** screen.

softkey.feature.forward

1 (default) - Displays the **Forward** softkey.

0 - The **Forward** softkey doesn't display.

To configure the `softkey.feature.forward` parameter, you must configure `feature.enhancedFeatureKeys.enabled="1"` .

Enhanced Feature Line Key (EFLK)

This feature enables users with Microsoft-registered phones to assign contacts to specific line keys on the phone or an expansion module connected to the phone.

EFLK is disabled by default. After you enable ELFK, users can enable and disable the feature from the phone menu.

Phones display registrations and contacts in the following order:

- Registration
- Enhanced Feature Key (EFK) as line key
- Skype for Business favorites
- Favorites (Local contacts)

After you enable EFLK on the server, the user must sign into the phone and enable Custom Line Keys from the phone menu. The option to customize line keys is not available during active calls. After a user enables custom line keys on the phone, contacts on the phone's local contact directory are not available.

- Assign a Skype for Business contact to a line
- Clear a contact assigned to a line key or clear all customizations
- Delete a line key and the contact assigned to it
- Insert an empty line above or below a line key

Note the following points when using EFLK:

- Changes users make in Customized mode do not affect contacts in Default Mode.
- Deleting a contact from the Skype for Business client does not delete the contact from the phone.
- If a customized contact exists in both Boss Admin and self-contacts, then Boss Admin relation will be given higher precedence.

User customizations are uploaded to the phone and server as a .csv file in the following format:

- `<MACaddress>-<sign-in address>.csv`

The user .csv customization files cannot be edited manually. To apply a common customization to multiple phones, administrators can rename any user file by replacing the `<MACaddress>` part of the user file name with `<000000000000>-<sign-in address>.csv` . You must use centralized provisioning to share custom .csv files.

EFLK Limitations

Note the following limitations when using EFLK:

- The .csv file is always stored in the root directory and you can’t use a sub-directory.
- The phone doesn’t load the .csv file when checking the server for updates using check sync.
- The user can't configure Speed Dials and Enhanced Feature Key (EFK) as line key.
- You can configure 100 contacts only.

Configuring EFLK

Use the following parameters to configure the Enhanced Feature Line Key feature for devices registered with Skype for Business.

feature.flexibleLineKey.enable

0 (default) - The EFLK feature is disabled.

1 - The EFLK feature is enabled and Line Key Customization is added to the phone at **Settings > Basic > Line Key Customization**.

Busy Options to Manage Incoming Calls

Busy Options enables users to manage incoming calls when a call or conference is already in progress.

After you enable and configure the Busy Options on the Skype for Business server, Busy Options settings take effect on all Skype for Business call devices and clients. You can enable one of the following predefined settings on the devices:

- **BusyonBusy**: Rejects an incoming call and sends a notification to the caller stating that the user is busy on another call.
- **VoicemailonBusy**: Forwards an incoming call to voicemail, when the user is either busy or does not answer the call.

Call Transfer Parameters

Use the following list to specify call transfer behavior.

`call.defaultTransferType`

Set the transfer type the phone uses when transferring a call.

Generic Base Profile: Consultative (default) - Users can immediately transfer the call to another party.

Centralized Conference Control Protocol (CCCP)

CCCP is enabled by default when the phone Base Profile is set to Skype.

CCCP enables users to initiate conference calls with Skype for Business contacts from their phone, manage conference participants, enable announcements, and lock a conference. Users can manage a maximum of 24 Skype for Business conference calls at a time on their phone. However, users can have only one active conference call in progress on their phone.

Centralized Conference Control Protocol (CCCP) Parameters

The following parameters configure CCCP.

Dial Plans

This section on dial plans includes information on dial plan normalization, multiple emergency number dial plans, parameters you can configure on your provisioning server, and examples of supported and unsupported dial plans.

Dial Plan Normalization

Dial Plan Normalization enables you to configure dial plans on the Skype for Business server or on your provisioning server.

For more information on regular expressions used on Skype for Business server, see .NET Framework Regular Expressions on Microsoft Developer Network.

Multiple Emergency Number Dial Plan

When registering phones with Skype for Business, you can configure multiple emergency numbers on the Skype for Business server.

When you correctly configure the multiple emergency numbers on the Skype for Business server, users can make calls to the emergency numbers from the Skype for Business client or from a phone, even when the phone is locked.

Phones receive emergency numbers through in-band provisioning and can conflict with the emergency dial string and mask. When a phone receives both multiple emergency numbers and emergency dial string and mask, the client and phone use multiple emergency numbers.

For instructions on creating a multiple emergency number dial plan, see Configure Multiple Emergency Numbers in Skype for Business 2015 on Microsoft TechNet.

Dial Plan, Dial Plan Normalization, and Digit Map Parameters

Poly does not support all regular expression dial plans.

The following parameters configure supported dial plans with Skype for Business Server.

`dialplan.x.digitmap`

x.T

In the above expression, enter the phone number for "x". Enter the timeout in seconds for "T".

Specify the digit map used for the dial plan using a string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. This parameter enables the phone to automatically initiate calls to numbers that match a digit map pattern.

The string is limited to 2560 bytes and 100 segments of 64 bytes, and the following characters are allowed in the digit map.

- A comma (,), which turns dial tone back on.
- A plus sign (+) is allowed as a valid digit.
- The extension letter 'R' indicates replaced string.
- The extension letter 'Pn' indicates precedence, where 'n' range is 1-9.
  1—Low precedence

  9—High precedence

`dialplan.x.digitmap.timeOut`

Specify a timeout in seconds for each segment of digit map. After you press a key, the phone waits the number of seconds you specify to match the digits to a dial plan and dial the call.

4 seconds (default)

String of positive integers separated by | for example 3 | 3 | 3 | 3 | 3 | 3

Note: If there are more digit maps than timeout values, the default value is used. If there are more timeout values than digit maps, the extra timeout values are ignored.

`dialplan.x.lyncDigitmap.timeOut`

This parameter applies to lines registered with Skype for Business or Lync Server.

Specify a timeout in seconds for each segment of a digit map. After you press a key, the phone waits the number of seconds you specify to match the digits to a dial plan and dial the call.

4 seconds (default)

0 to 99 seconds

Note: If there are more digit maps than timeout values, the default value is used. If there are more timeout values than digit maps, the extra timeout values are ignored.

Note also that if you configure a value outside of the permitted range, the default value is used.

`dialplan.userDial.timeOut`

Specify the time in seconds that the phone waits before dialing a number you enter while the phone is on hook. This parameter applies only when its value is lower than `up.IdleTimeOut`.

4 seconds (default)

0 to 99 seconds

reg.x.applyServerDigitMapLocally

1 - Enable dial plan normalization. Dial plan normalization rules are downloaded from the Microsoft Server and processed on the phone.

0 - Disable dial plan normalization. Dial plan rules are processed by the Microsoft Server.

up.IdleTimeOut

Set the number of seconds that the phone is idle for before automatically leaving a menu and showing the idle display.

During a call, the phone returns to the Call screen after the idle timeout.

40 seconds (default)

0 to 65535 seconds

Change causes system to restart or reboot.

Supported Dial Plans

Poly phones support Skype for Business External Access Prefix functionality.

Examples of supported dial plans include the following:

- Support for multiple combination of braces (): ^91(727|813)([2-9]\d{6})$@+9$1$2@0
- Support for 'ext': ^64(\d{2})$@+86411845933$1;ext=64$1@0

Supported Dial Plans

Number	Element	Meaning	Example	Description of Example
1	^	Match at beginning of string	^123	Match the digits 123 at the beginning of the string
2	()	Captures the matched subexpression	(456)	Capture what is between the parentheses into a numbered variable, starting at 1 which can be accessed as $n, for example, $1
3	*	Specifies zero or more matches	\d(*)	
4	+	Specifies one or more matches	\d(+)	
5	?	Specifies zero or one matches	\d(+)	
6	{n}	Specifies exactly n matches	\d {4}	Match 4 digits
7	Vertical Bar (Pipe)	Matches any one of the terms separated by the (vertical bar) character when all characters are surrounded by brackets or square brackets	(1|2|3) or [1|2|3]	Match either 1, 2, or 3.

Number	Element	Meaning	Example	Description of Example
8	\d	Matches any decimal digit	^\d	Match any decimal digit (at the beginning of a string)
9	$	The match must occur at the end of the string	^(123)$	Match exactly digits 123 (and not 1234)

PSTN Gateway on Failover

When a phone becomes unregistered due to an outage and can't reach the Skype for Business server for a specified time interval, the phone fails over to an alternate PSTN gateway server.

You can view the PSTN failover details in the Web Configuration Utility.

When you enable this feature, calls switch to the configured PSTN gateway in the event of an outage. However, if the phone fails over, only basic call-related functions and soft keys are available.

Make sure the value of call.enableOnNotRegistered and reg.x.srtp.simplifiedBestEffort parameter is set to `1`.

Note: The failover feature does not work if you enable the hybrid line registration feature.

Ensure the Direct Inward Dialing number registered on the Skype for Business server and the number used for the PSTN gateway are same.

PSTN Gateway Failover Parameters

The following parameters configure phones to fail over to an alternate PSTN gateway in the event of an outage or if the phones can't reach the Skype for Business server.

`feature.sfbPstnFailover.enabled`

Enable or disable for phones to fail over to a PSTN gateway during an outage.

0 (default) - Disabled

1 - Enabled

Change causes system to restart or reboot.

`reg.x.server.y.address`

If this parameter is set, it takes precedence even if the DHCP server is available.

Null (default) - SIP server does not accept registrations.

IP address or hostname - SIP server that accepts registrations.

This parameter is only applicable during a failover to PSTN gateway in Skype for Business deployments.

`reg.x.server.y.pstnServerAuth.userId`

Specify the user identification for the PSTN gateway.

Null (default)

String (maximum of 255 characters)

`reg.x.server.y.pstnServerAuth.password`

Specify the PSTN user's password.

Null (default)

String (maximum of 255 characters)

Presence Status

You can enable users to monitor the status of other remote users and phones.

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 in order to override or mask automatic status updates to others and can receive notifications when the status of a remote line changes.

Poly phones support a maximum of:

Presence Status Parameters

Use the following parameters to enable Presence and display the **MyStatus** and **Buddies** soft keys on the phone.

`feature.presence.enabled`

0 (default) - Disable the presence feature—including buddy managements and user status.

1 - Enable the presence feature with the buddy and status options.

`pres.idleSoftkeys`

1 (default) - The MyStat and Buddies presence idle soft keys display.

0 - The MyStat and Buddies presence idle soft keys do not display.

`pres.reg`

The valid line/registration number to use for presence. If the value is not a valid registration, this parameter is ignored.

1 (default)

1 - 34

Local Call Recording

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

You can play back recorded audio on the phone or using an audio application on the computer. To use this feature, you must enable USB port.

Audio calls are recorded in .wav format and include a date/time stamp. The phone displays the recording time remaining on the attached USB device, and users can browse all recorded files using the phone's menu.

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

Local Call Recording Parameter

Use the following parameter to configure local call recording.

`feature.callRecording.enabled`

0 (default) - Disable audio call recording.

1 - Enable audio call recording.

Change causes system to restart or reboot.

Local Digit Map

The local digit map feature allows the phone to automatically call a dialed number you configure.

Digit maps are defined by a single string or a list of strings. If a dialed number matches any string of a digit map, the call is automatically placed. If a dialed number matches no string—an impossible match—you can specify the phone's behavior. If a number ends with #, you can specify the phone's behavior, called trailing # behavior. You can also specify the digit map timeout, the period of time after you dial a number that the call is placed. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of RFC 3435.

Local Digit Maps Parameters

Use the following parameters to configure the local digit map.

`dialplan.1.applyToCallListDial`

Choose whether the dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus.

1 (default) - Enable

0 - Disable

Change causes system to restart or reboot.

`dialplan.1.applyToDirectoryDial`

Generic Base Profile – 0 (default)

0— The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

1—The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

Change causes system to restart or reboot.

`dialplan.1.applyToForward`

Generic Base Profile – 0 (default)

0—The dial plan does not apply to forwarded calls.

1—The dial plan applies to forwarded calls.

Change causes system to restart or reboot.

`dialplan.applyToTelUriDial`

Choose whether the dial plan applies to URI dialing.

1 (default) - Enable

0 - Disable

Change causes system to restart or reboot.

`dialplan.applyToUserDial`

Choose whether the dial plan applies to calls placed when the user presses Dial.

1 (default) - Enable

0 - Disable

Change causes system to restart or reboot.

dialplan.applyToUserSend

Choose whether the dial plan applies to calls placed when the user presses Send.

1 (default) - Enable

0 - Disable

Change causes system to restart or reboot.

dialplan.1.conflictMatchHandling

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

0 (default for Generic Profile) - Disable

1 (default for Skype Profile) - Enable

dialplan.1.digitmap.timeOut

Specify a timeout in seconds for each segment of the digit map using a string of positive integers separated by a vertical bar (|). After a user presses a key, the phone waits this many seconds before matching the digits to a dial plan and dialing the call.

(Default) `3 | 3 | 3 | 3 | 3| 3`

If there are more digit maps than timeout values, the default value 3 is used. If there are more timeout values than digit maps, the extra timeout values are ignored.

Change causes system to restart or reboot.

dialplan.1.digitmap

Specify the digit map used for the dial plan using a string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. This parameter enables the phone to automatically initiate calls to numbers that match a digit map pattern.

The string is limited to 2560 bytes and 100 segments of 64 bytes, and the following characters are allowed in the digit map.

- A comma (,), which turns dial tone back on.
- A plus sign (+) is allowed as a valid digit.
- The extension letter 'R' indicates replaced string.
- The extension letter 'Pn' indicates precedence, where 'n' range is 1-9.
  1—Low precedence

  9—High precedence

Change causes system to restart or reboot.

dialplan.applyToDirectoryDial

Generic Base Profile – 0 (default)

0— The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

1—The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.

Change causes system to restart or reboot.

dialplan.applyToForward

Generic Base Profile – 0 (default)

0—The dial plan does not apply to forwarded calls.

1—The dial plan applies to forwarded calls.

Change causes system to restart or reboot.

dialplan.filterNonDigitUriUsers

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

0 (default) - Disable

1 - Enable

Change causes system to restart or reboot.

dialplan.1.impossibleMatchHandling

0 —The digits entered up to and including the point an impossible match occurred are sent to the server immediately.

1—The phone gives a reorder tone.

2 —Users can accumulate digits and dispatch the call manually by pressing Send.

3 — No digits are sent to the call server until the timeout is configured by `dialplan.impossibleMatchHandling.timeout` parameter.

If a call orbit number begins with a pound (#) or asterisk (*), you need to set the value to 2 to retrieve the call using off-hook dialing.

Change causes system to restart or reboot.

dialplan.removeEndOfDial

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

1 (default) - Enable

0 - Disable

Change causes system to restart or reboot.

dialplan.routing.emergency.outboundIdentity

Choose how your phone is identified when you place an emergency call.

NULL (default)

10-25 digit number

SIP

TEL URI

If using a URI, the full URI is included verbatim in the P-A-I header. For example:

- `dialplan.routing.emergency.outboundIdentity = 5551238000`
- `dialplan.routing.emergency.outboundIdentity= sip:john@emergency.com`
- `dialplan.routing.emergency.outboundIdentity = tel:+16045558000`

dialplan.routing.emergency.preferredSource

Set the precedence of the source of emergency outbound identities.

ELIN (default)— the outbound identity used in the SIP P-Asserted-Identity header is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN).

Config— the parameter `dialplan.routing.emergency.outboundIdentity` has priority when enabled, and the LLDP-MED ELIN value is used if `dialplan.routing.emergency.outboundIdentity` is NULL.

dialplan.routing.emergency.1.description

Set the label or description for the emergency contact address.

x=1: Emergency, Others: NULL (default)

string

x is the index of the emergency entry description where x must use sequential numbering starting at 1.

Change causes system to restart or reboot.

dialplan.routing.emergency.x.server.y

Set the emergency server to use for emergency routing (`dialplan.routing.server.1.address` where x is the index).

x=1: 1, Others: Null (default)

positive integer

x is the index of the emergency entry and y is the index of the server associated with emergency entry x. For each emergency entry (x), one or more server entries (x,y) can be configured. x and y must both use sequential numbering starting at 1.

Change causes system to restart or reboot.

dialplan.routing.emergency.1.value

Set the emergency URL values that should be watched for. When the user dials one of the URLs, the call is directed to the emergency server defined by `dialplan.routing.server.1.address`.

x=15: 911, others: Null (default)

SIP URL (single entry)

x is the index of the emergency entry description where x must use sequential numbering starting at 15.

dialplan.routing.server.1.address

Set the IP address or hostname of a SIP server to use for routing calls. Multiple servers can be listed starting with x=1 to 3 for fault tolerance.

Null (default)

IP address

hostname

Blind transfer for 911 or other emergency calls may not work if registration and emergency servers are different entities.

Change causes system to restart or reboot.

dialplan.routing.server.1.port

Set the port of a SIP server to use for routing calls.

5060 (default)

1 to 65535

Change causes system to restart or reboot.

dialplan.routing.server.1.transport

Set the DNS lookup of the first server to use and dialed if there is a conflict with other servers.

DNSnaptr (default)

TCPpreferred

UDPOnly

TLS

TCPOnly

For example, if `dialplan.routing.server.1.transport` = "UDPOnly" and `dialplan.routing.server.2.transport` = "TLS", then UDPOnly is used.

Change causes system to restart or reboot.

dialplan.userDial.timeOut

Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook.

0-99 seconds

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

dialplan.1.lyncDigitmap.timeOut

This parameter applies to lines registered with Skype for Business or Lync Server.

Specify a timeout in seconds for each segment of a digit map. After you press a key, the phone waits the number of seconds you specify to match the digits to a dial plan and dial the call.

4 seconds (default)

0 to 99 seconds

Note:
If there are more digit maps than timeout values, the default value is used. If there are more timeout values than digit maps, the extra timeout values are ignored.

If you configure a value outside of the permitted range, the default value is used.

dialplan.TranslationInAutoComp

1 (default) - The translated string displays in the auto-complete list.

0 - The translated string does not display in the auto-complete list.

dialplan.applyToPstnDialing

Apply the dial plan to the Public Switch Telephony Network (PSTN).

0 (default) - Disable

1 - Enable

dialplan.applyToRemoteDialing

0 (default) - Disable

1 - Enable

dialplan.digitmap

0 (default) - Disable the line switching in dial plan to switch the call to the dial plan matched line.

1 - Enable the line switching in dial plan to switch the call to the dial plan matched line.

This is not applicable for off-hook dialing.

dialplan.userDial.timeOut

Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook.

Generic Base Profile (default) – 0

Lync Base Profile (default) – 4

0-99 seconds

0-99 seconds

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

International Dialing Prefix

Enter a plus (+) symbol before you dial an international phone number to identify to the switch that you are dialing an international phone number.

International Dialing Prefix Parameters

The following parameters configure the international dialing prefixes.

call.internationalDialing.enabled

This parameter applies to all numeric dial pads on the phone, including for example, the contact directory.

1 (default) - Disable the key tap timer that converts a double tap of the asterisk "*" symbol to the "+" symbol to indicate an international call. By default, this parameter is enabled so that a quick double tap of "*" converts immediately to "+". To enter a double asterisk "**", tap "*" once and wait for the key tap timer to expire to enter a second "*".

0 - When you disable this parameter, you cannot dial "+" and you must enter the international exit code of the country you are calling from to make international calls.

Change causes system to restart or reboot.

call.internationalPrefix.key

The phone supports international call prefix (+) with both "0" and "*".

0 (default) - Set the international prefix with "*".

1 - Set the international prefix with "0".

Enhanced 911 (E.911)

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

The phone supports the following methods:

- LLDP-MED

- DHCP via option 99
- LIS compliant with RFC 5985

Configuring the source of location information allows the phone to share its location details in the invite sent when a 911 call is made to ensure the 911 operator dispatches emergency services to the correct address.

Enhanced 911 (E.911) Parameters

Use the following parameters to configure E.911.

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

`feature.E911.locationInfoSchema`

HYBRID (default) - SIP invites use an XML schema as per the RFC4119 and RFC5139 standards.

RFC 4119 - SIP invites use an XML schema as per the RFC4119 standards.

RFC5139 - SIP invites use an XML schema as per the RFC5139 standards.

`feature.E911.HELD.server`

NULL (default)

Set to the URL to request the location information from the server. For example, https://host.domain.com/held/request.

0 - 255 characters

`feature.E911.HELD.username`

NULL (default)

Set the user name used to authenticate to the LIS.

0 - 255 characters

`feature.E911.HELD.password`

NULL (default)

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

0 - 255 characters

`feature.E911.HELD.identity`

Set the vendor-specific element to include in a location request message. For example, 'companyID'.

NULL (default)

String 255 character max

`feature.E911.HELD.identityValue`

Set the value for the vendor-specific element to include in a location request message.

NULL (default)

String 255 character max

feature.E911.locationRetryTimer

Specify the retry timeout value in seconds for the location request sent to the Location Information Server (LIS).

The phone does not retry after receiving location information received through the LIS.

60 seconds (default)

60 - 86400 seconds

feature.E911.HELD.nai.enable

0 (default) – The NAI is omitted as a device identity in the location request sent to the LIS.

1 - The NAI is included as a device identity in the location request sent to the LIS.

locInfo.source

Specify the source of phone location information. This parameter is useful for locating a phone in environments that have multiple sources of location information.

LLDP (default for Generic Base Profile) – Use the network switch as the source of location information.

CONFIG - Use location information defined in the configuration.

LIS – Use the location information server as the source of location information. Generic Base Profile only.

DHCP – Use DHCP as the source of location information. Generic Base Profile only.

locInfo.x.label

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter a label for the location.

Null (default)

0 -255

locInfo.x.country

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter the country where the phone is located.

Null (default)

0 -255

locInfo.x.A1

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

locInfo.x.A3

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter the city where the phone is located.

Null (default)

0 -255

locInfo.x.PRD

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter the leading direction of the street location.

Null (default)

0 -255

locInfo.x.RD

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

locInfo.x.STS

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

locInfo.x.POD

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter the trailing street direction. For example, southwest.

Null (default)

0 -255

locInfo.x.HNO

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

locInfo.x.HNS

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

locInfo.x.LOC

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter any additional information that identifies the location.

Null (default)

0 -255

locInfo.x.NAM

To use this parameter, set `locInfo.source` to `CONFIG`.

Enter a proper name to associate with the location.

Null (default)

0 -255

locInfo.x.PC

To use this parameter, set `locInfo.source` to `CONFIG`.

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

Null (default)

0 -255

feature.E911.enabled

0 (default) - Disable the E.911 feature.

1 - Enable the E.911 feature.

The INVITE sent for emergency calls from the phone includes the geolocation header defined in RFC 6442 and PIDF presence element as specified in RFC3863 with a GEOPRIV location object specified in RFC4119 for in Open SIP environments.

feature.E911.HELD.requestType

Any (default) - Send a request to the Location Information Server (LIS) to return either 'Location by Reference' or 'Location by Value'. Note this is not the 'Any' value referred to in RFC 5985.

Civic - Send a request to the LIS to return a location by value in the form of a civic address for the device as defined in RFC 5985.

RefID - Send a request to the LIS to return a set of Location URIs for the device as defined in RFC 5985.

voIpProt.SIP.header.priority.enable

0 (default) – Do not include a priority header in the E.911 INVITE message.

1 - Include a priority header in the E.911 INVITE message.

voIpProt.SIP.header.geolocation-routing.enable

0 (default) – Do not include the geolocation-routing header in the E.911 INVITE message.

1 - Include the geolocation-routing header in the E.911 INVITE message.

voIpProt.SIP.header.switchInfo.enable

The phone gathers the MAC address and port information from LLDP and sends that data to the server, which determines phone location based on "Location" configurations.
0 (default) - The register message does not include the custom header `X-switch-info`.

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

`feature.E911.HELD.secondary.server`

Set to the URL to request the location information from the server. For example, https://host.domain.com/held/request.

NULL (default)

0-255

`feature.E911.HELD.secondary.username`

Set a user name to authenticate to the secondary Location information Server (LIS).

NULL (default)

String

0-255

`feature.E911.HELD.secondary.password`

Set a password to authenticate to the secondary LIS.

NULL (default)

String

`feature.E911.usagerule.retransmission`

0 (default) - The recipient of this location object is not permitted to share the enclosed location information, or the object as a whole, with other parties.

1 - Distributing this location is permitted.

Configuring Boss-Admin

The Boss-Admin feature enables a Boss to assign and share a line with an Admin, a delegate who can manage calls efficiently on behalf of the Boss. Boss-Admin is supported with Skype for Business, Lync 2013, and Lync 2010.

The Boss can add and remove admins, monitor call status, view which admins answered a call, and pick up calls put on hold. Admins can place, answer, hold, and transfer calls, monitor call status, set ringtones on the Boss line, and send a call to voicemail or intercom. Phones in a Boss-Admin group can receive up to five incoming calls at the same time.

A boss can assign up to 25 admin lines to their phone; Admins cannot assign themselves as a delegate to a line on a boss' phone. The maximum number of bosses an Admin phone can be assigned varies by phone model and depends on the number of line keys available on the phone.

A boss can add or remove Admins from the Skype for Business client application on a computer or from the phone. Bosses can add and edit Admins from the phone using the contact list and to set up the call forwarding and simultaneous call ringing. You can view Enhanced Boss-Admin status in the system web interface for your device.

Note: Enhanced Boss-Admin is enabled by default.

Maximum Number of Boss Lines

The following table lists the maximum number of Boss lines that can be assigned to an Admin phone.

Maximum Number of Boss Lines Assigned to an Admin Phone

Phone Model	Maximum Bosses Assigned
Poly CCX 400 business media phones	23 of 24 lines
Poly CCX 500 business media phones	23 of 24 lines
Poly CCX 600 business media phones	23 of 24 lines

Viewing Delegates on Boss's Phone

When a Boss delegates an Admin, you can view the delegate's key icon on the Boss's phone.

The following figure illustrates Admins on a Boss's phone.

Safe Transfer for Boss-Admin

A safe transfer transfers a call to another party and allows you to continue monitoring the call with the option to resume before the call goes to voicemail.

If the call is answered by the other party, you are disconnected from the call.

Configuring Safe Transfer

The following parameters configure safe transfer for the Boss-Admin feature.

`feature.lyncSafeTransfer.enabled`

1 (default) - Enable safe transfer and display of the **Safe Transfer** soft key.

0 - Disable safe transfer and display of the **Safe Transfer** soft key.

Boss-Admin Parameters

Use the following parameters to configure Boss-Admin.

`up.enhancedbossadmin`

1 (default)- Enable Enhanced Boss-Admin.

0 - Disable Enhanced Boss-Admin.

Change causes system to restart or reboot.

Using the Phones as Shared Devices

Poly phones registered with Skype for Business offer several ways to share phones and phone lines among users.

Skype for Business User Profiles

You can enable users to access their personal settings from any phone in the organization registered to Skype for Business.

For example, users can access their contact directory and speed dials – as well as other phone settings – even if they temporarily change work areas. This feature is particularly useful for remote and mobile workers who do not use a dedicated work space and conduct business in multiple locations. The user profile feature is also useful if an office has a common conference phone from which multiple users need to access their personal settings.

You must decide whether to require users to always log in to a phone or not. If you do not require users to log in, users have the option to use the phone as is – without access to their personal settings – or they can log in to display their personal settings. You can also specify if, after the device restarts or reboots, a user is automatically logged out.

You can choose to define default credentials. If you specify a default user ID and password, the phone automatically logs itself in each time an actual user logs out or the device restarts or reboots. When the device logs itself in using the default login credentials, a default profile displays, and users retain the option to log in and view their personal settings.

You can configure the phones so that anyone can call authorized and emergency numbers when not logged in to a phone using the parameter dialplan.routing.emergency.outboundIdentity.

Poly recommends that you create a single default user password for all users. You can reset a user's password by removing the password parameter from the override file. This causes the phone to use the default password in the <*user*>.cfg file.

To set up the user profile feature, you must:

- Create a phone configuration file or update an existing file to enable the feature's settings, and configure attributes for the feature.
- Create a user configuration file in the format <*user*>.cfg to specify each user's password and registration and other user-specific settings that you want to define.

Create a User Profile Configuration File

You can create a configuration file with user-specific profile details and provision multiple phones with that file.

Task

1. Create a configuration file for the phone and place it on the provisioning server.
2. Add the prov.login* parameters you want to use to your configuration.
3. Copy the prov.login* parameters you want to use for each user and enter user-specific values.

Create a User Configuration File

Create a user-specific configuration file that stores user names, passwords, and registrations.

After a user logs in with their user ID and password (The default password is 123), users can:

- Log in to a phone to access their personal phone settings.
- Log out of a phone after they finish using it.
- Place a call to an authorized number from a phone that is in the logged out state.
- Change their user password.

If a user changes any settings while logged in, the settings save and display the next time the user logs in. When a user logs out, the user's personal phone settings no longer display.

Task

1. On the provisioning server, create a user configuration file for each user to log in to the phone.

   The name of the file is the user's ID to log in to the phone. For example, if the user's login ID is *user100*, the name of the user's configuration file is user100.cfg.
2. In each <*user*>.cfg file, you can add and set values for the user's login password (optional).
3. Add and set values for any user-specific parameters, such as:

   - Registration details (for example, the number of lines the profile displays and line labels).
   - Feature settings (for example, browser settings).

     Note: If you add optional user-specific parameters to <*user*>.cfg, add only those parameters that will not cause the phone to restart or reboot when the parameter is updated.

Stored User Settings

If a user updates their password or other user-specific settings using the Main Menu on the phone, the updates are stored in <*user*>-phone.cfg, not <*MACaddress*>-phone.cfg.

If a user updates their contact directory while logged in to a phone, the updates are stored in <*user*>-directory.xml. Directory updates display each time the user logs in to a phone. An up-to-date call lists history is defined in <*user*>-calls.xml. This list is retained each time the user logs in to their phone. Configuration parameter precedence (from first to last) for a phone that has the user profile feature enabled is:

- <*user*>-phone.cfg
- Web Configuration Utility
- Configuration files listed in the primary configuration file (including <*user*>.cfg)
- Default values

Hot Desking

You can configure your phone to allow a hot desking or guest user to sign in on top of a host user signed in to a phone or a common area phone (CAP).

You must enable this feature on both the Skype for Business server and on your provisioning server using the `feature.HotDesking.enable` parameter. When you enable this feature, a **Guest** soft key displays on the phone. By default, this feature is enabled on the provisioning server. However, the user can choose to enable or disable the feature from the phone.

Note: When the phone is CAP enabled, users do not have permission to enable or disable Hot Desking.

Hot Desking Sign-In Methods

If the user disables Hot Desking from the phone, the user setting overrides the Skype for Business server setting and the feature is disabled. The guest user can sign in to the host phone by pressing the **Guest** soft key. After pressing the **Guest** soft key, the guest user can sign in with one of the following methods even if the phone is CAP-enabled or locked:

- User ID
- Pin Authentication
- Via PC
- Online Web Sign In

When the guest user signs in to the phone, the host/CAP user is logged out automatically and the guest user icon displays on the phone. After the guest user has signed in to the phone, the following details of the previously signed-in host/CAP user are not accessible:

- Call Logs
- Voicemail
- Calendar
- Local Contact Directory

Host Desking Feature Limitations

The menu options that are not accessible to the guest user are as follows:

- Headset Settings
- Background
- Screen Saver
- Presence
- Location Info
- Diagnostic logs
- Picture frame
- Power Saving
- Reset to Factory
- Clear browser data
- Network Configuration

Automatic Sign-Out Scenarios

When the guest user signs out of the phone, all the basic settings of the guest user are removed and the phone is set with original settings of the host user.

The following scenarios enable the phone to sign out the guest user automatically and sign in back with the previously signed in user:

- **Timeout**

  This feature supports hot desking timeout, the period of time after which the phone shall sign in to the host user when being idle in hot desking mode. This timeout is applicable only when the guest user has signed in successfully.

  - When the phone is idle for hot desking timeout configured on the server.
    When the guest user is signed in and does not perform any activity and the timeout interval configured on the server reached the value, the guest user is signed out.
  - User taps the guest soft key and does not sign in using any sign in methods.
    The timeout interval for hot desking is set to 2 minutes by default. However, the host user does not need to wait for 2 minutes. The host user can sign in by pressing the **Host** soft key on the phone screen.
- **BToE Mode**

  When a guest user is signed in to the phone and the phone is in BToE mode, the following scenarios lead to sign in the host user after logging out the guest user automatically:

  - Guest user unpairs the BToE pairing from the device.
  - Guest user unpairs the BToE pairing using BToE client.
  - Guest user signs out from the paired Skype for Business client.

When the phone is in idle state and any one of these scenarios occur, the phone signs out the guest user.

Hot Desking Parameters

The following parameters configure Hot Desking.

`feature.HotDesking.enabled`

1 (default) - Enable Hot Desking.

0 - Disable Hot Desking.

`feature.ResetHostSettings.enabled`

1 (default) – Enables the settings when the device switched to guest mode.

0 – Disables the settings when device switched to guest mode.

Common Area Phone (CAP)

You can configure your phone with Common Area Phone (CAP) to restrict user's access to configuration settings on phones deployed in common areas, typically lobbies, employee lounges, and conference rooms.

You enable CAP Mode on a per-phone basis and CAP Mode is independent of any other configuration you make on the Skype server or apply to the Skype user account.

After you enable this feature using `feature.CAP.enabled=1`, CAP Mode and CAP Admin Mode are available on the phone. By default, CAP Mode is enabled and CAP Admin Mode is disabled.

While a phone is running in CAP Mode, users can access only basic settings and features. You can make more features available by enabling parameters for the corresponding feature, listed below.

Features Available in CAP Mode

Soft Key / Menu	CAP Mode Default	Parameters to Enable
Status/DND	Disabled	`feature.doNotDisturb.enable` `softkey.feature.mystatus`
Call Forward	Disabled	`feature.forward.enable`

Soft Key / Menu	CAP Mode Default	Parameters to Enable
Device Lock	Disabled	`feature.deviceLock.enable`

Exchange Call Logs	Disabled	`Local logs: feature.callList.enabled`
		`Exchange call logs:`
		`feature.callList.enabled`
		`feature.exchangeCallLog.enabled`
		`feature.EWSAutodiscover.enabled`

Local Contact Directory	Disabled	`feature.directory.enabled`

Exchange Calendar	Disabled	`feature.EWSAutodiscover.enabled`
		`feature.exchangeCalendar.enabled`
		`homeScreen.calendar.enable`

Exchange Contacts	Disabled	`feature.EWSAutodiscover.enabled` `feature.exchangeContacts.enabled`

Exchange Voicemail/ Messages	Disabled	`feature.voicemail.enabled`
		`feature.EWSAutodiscover.enabled`
		`feature.exchangeVoiceMail.enabled`
		`feature.exchangeSipVMPlay.enabled`

Redial	Disabled	`homeScreen.redial.enable`

You can use the phone's administrator password to enable CAP Admin Mode. CAP Admin Mode provides access to all phone settings available from the phone interface. In addition, in CAP Admin Mode, the phone displays Sign In / Sign Out soft keys that allow you to sign users in or out of the phone. Alternatively, you can sign into a phone in CAP Mode without enabling CAP Admin Mode from the Common Area Phone provisioning portal at `https://aka.ms/skypecap` .

Any CAP-enabled phone that is not signed in with a Skype account and is left idle for three minutes displays a notice that the phone is not in use.

The following settings are available in CAP Admin Mode.

- Basic Settings
- Sign In/Sign Out
- My Status (under **Features > Presence > My Status**)

Disable CAP Admin Mode

You can disable the Common Area Phone (CAP) Admin Mode from the phone.

Task

1. On the phone, navigate to **Settings > Advanced**, and enter the default password.
2. Select **Administration Settings > Common Area Phone Settings > CAP Admin Mode**.
3. Choose **Disable**.

CAP Web Sign In

After you enable the CAP feature and the phone is in CAP Mode, you can generate a code on the phone that you use to log into the Common Area Phone Provisioning Portal, a Microsoft web service that enables you to sign in multiple phones using any tenant account without the need to authenticate as a user on each phone.

You can log into the Common Area Provisioning Portal at https://aka.ms/skypecap using any account having administrator rights to the Microsoft tenant. Note that your Skype deployment must use Modern Authentication to access CAP web

sign-in. For more information, see Skype for Business topologies supported with Modern Authentication on Microsoft Technet.

CAP Web Sign In is not supported with On-premises Skype for Business deployments.

Note: Sign in using accounts that are designated only for the Common Area locations. The CAP portal is designed only for Common Area Phone accounts. Provisioning a CAP phone from the Provisioning Portal changes that phone's Active Directory user account password to a random string generated by Microsoft. For this reason, do not use the Provisioning Portal to sign in to a phone on behalf of an end user.

Sign In to a CAP-Enabled Phone

You can sign out of a CAP-enabled phone using a code sent to the phone by the Common Area Provisioning Portal.

Task

1. While signed out of the phone, select Web Sign-in (CAP).
   The phone displays a code.
2. In the provisioning portal, enter the code in the field beside the user name and press Provision.
   The user's password is reset to a random string and the phone is signed in.

Common Area Phone Parameters

The following parameters configure the Common Area Phone (CAP) feature.

Use of CAP requires UC Software 5.7.0 or later.

`feature.CAP.enabled`

0 (default) - Disable Common Area Phone.

1 - Enable Common Area Phone.

Skype for Business Device and Software Support

This section provides information on maintaining your devices and updating UC Software.

Microsoft Quality of Experience Monitoring Server Protocol (MS-QoE)

Microsoft Quality of Experience Monitoring Server Protocol (MS-QoE) enables you to monitor the user's audio quality and troubleshoot audio problems.

QoE reports contain only audio metrics and do not contain video or content sharing metrics. This feature also enables you to query the QoE status of a phone from the Web Configuration Utility.

All parameters for enabling or disabling QoE are included in the in-band provisioning parameters sent from the Skype for Business server.

Note: Poly supports only those elements listed in section Supported Skype for Business QoE Elements.

For a list of all parameters that report QoE data, see Microsoft [MS-QoE] PDF at [MS-QoE]: Quality of Experience Monitoring Server Protocol.

To help deploy QoE, you can enable client media ports and configure unique port ranges on the Skype for Business Server. For details, see Configuring Port Ranges for your Microsoft Lync Clients in Lync Server 2013.

Set QoE Parameters on the Skype for Business Server

Set the following QoE parameters on the Skype for Business Server.

Task

» Use the following parameters to set Quality of Experience settings on the Skype for Business server.

EnableQoE

Set to 'True' to enable QoE on the server and automatically assign the URI to which QoE reports are published.

If set to 'False' no QoE reports are published.

Note that the URI maps to the in-band element '`qosUri`'. To get the current value of `EnableQoE`, run the command `Get-CsQoEConfiguration` in Skype for Business Server Powershell.

EnableInCallQoS

Set to 'True' to enable in-call QoE on the server.

If set to 'False', only end-call QoE reports are sent. `EnableInCallQoS` maps to the in-band element '`enableInCallQoS`'.

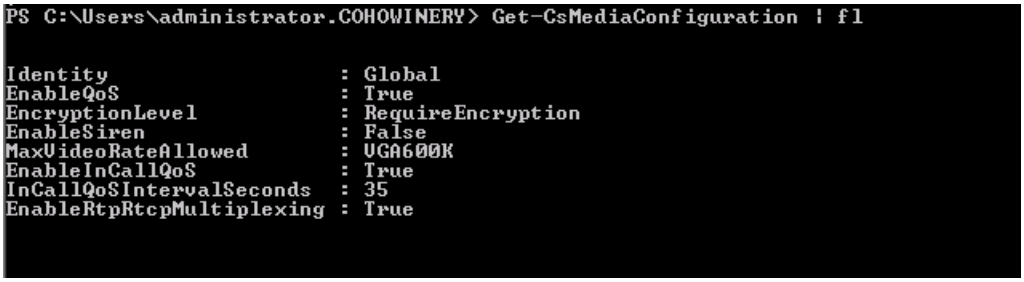
InCallQoSIntervalSeconds

Set the time interval in seconds to publish in-call QoE reports only if there is a transition in call quality. If no change in call quality is detected, no report is sent at the interval time you set. `InCallQoSIntervalSeconds` maps to the in-band element `inCallQoSIntervalSeconds`.

voice.qualityMonitoring.rtcpxr.enable

Set to 1 (default) to allow the phone to collect RTCP XR metrics.

The following figure illustrates the QoE parameter values you need to set.



Enable In-Call QoE within your Skype Environment

When you enable in-call QoE, you do not need to wait until the end of the call to view call quality data.

In-call QoE is off by default and you can enable it on Windows PowerShell using the following command:

```
Set-CsMediaConfiguration -Identity Global -EnableInCallQoS:$TRUE -
InCallQoSIntervalSeconds x (where x is a digit from 1 to 65535)
```

Query QoE Status from the System Web Interface

Users and administrators can query the in-band QoE status, interval, and URI from a phone's system web interface.

Task

1. Enter the IP address of the phone into a web browser and log in as Administrator or User.
2. Go to **Diagnostics > Skype for Business Status > Quality of Experience**.

QoE Parameters

Use the following parameters to configure MS-QoE from a provisioning server.

`voice.qoe.event.lossrate.threshold.bad`

Defines the threshold for the network loss rate. Total packets lost for an interval/total packets expected for the interval *256 as stated in RFC 2611, section 4.7.1.

38 (default) - Approximately a 15% packet loss.

0 to 100

`voice.qoe.event.lossrate.threshold.poor`

Defines the threshold for the network loss rate. Total packets lost for an interval/total packets expected for the interval *256 as stated in RFC 2611, section 4.7.1.

25 ms (default) - Approximately a 10% packet loss.

0 to 100

`voice.qoe.event.networkmos.threshold.bad`

Defines the threshold for Network MOS as follows:

The average of MOS-LQO wideband, as specified by [ITUP.800.1] section 2.1.2, based on the audio codec used and the observed packet loss and inter-arrival packet jitter.

19 (default) - Indicates a MOS score of 1.9.

10 - 50 - Indicates a MOS score between 1 - 5.

networkMOS > 2.9 signifies good quality

networkMOS > 2.9 < 1.9 signifies poor quality

networkMOS < 1.9 signifies bad quality

`voice.qoe.event.networkmos.threshold.poor`

Defines the threshold for Network MOS as follows:

The average of MOS-LQO wideband, as specified by [ITUP.800.1] section 2.1.2, based on the audio codec used and the observed packet loss and inter-arrival packet jitter.

29 (default) - Indicates a MOS score of 2.9.

10 - 50 - Indicates a MOS score between 1 - 5.

networkMOS > 2.9 signifies good quality

networkMOS > 2.9 < 1.9 signifies poor quality

networkMOS < 1.9 signifies bad quality

Supported Skype for Business QoE Elements

This section lists supported Microsoft Quality of Experience (QoE) elements.

For a list of all parameters that report QoE data, see Microsoft [MS-QoE] PDF at [MS-QoE]: Quality of Experience Monitoring Server Protocol.

Supported Skype for Business QoE Elements

Parent Element	Child Elements/Attributes
VQReportEvent	VQSessionReport

Parent Element	Child Elements/Attributes
VQSessionReport	SessionId Endpoint DialogInfo MediaLine
Endpoint	Name v2:OS v2:VirtualizationFlag CorrelationID FromURI ToURI Caller LocalContactURI RemoteContactURI LocalUserAgent RemoteUserAgent LocalPAI RemotePAI ConfURI v2:CallPriority v2:MediationServerBypassFlag v2:TrunkingPeer v2:RegisteredInside CallID FromTag ToTag Start End
MediaLine	Description InboundStream OutboundStream
Description	Connectivity Security Transport LocalAddr RemoteAddr v3:ReflexiveLocalIPAddress v3:MidCallReport
LocalAddr, RemoteAddr, RelayAddr	IPAddr Port SubnetMask v2:MACAddr
Connectivity	Ice IceWarningFlags (Five flags supported) RelayAddress

Parent Element	Child Elements/Attributes
InboundStream, OutboundStream	Network Payload QualityEstimates
Network	Jitter PacketLoss BurstGapLoss Delay Utilization
Jitter	InterArrival InterArrivalMax
Packetloss	LossRate LossRateMax
BurstGapLoss	BurstDensity BurstDuration GapDensity GapDuration
Delay	RoundTrip RoundTripMax
Utilization	Packets
Payload	Audio
Payload.Audio	PayloadType PayloadDescription SampleRate v4:JitterBufferSizeAvg v4:JitterBufferSizeMax v4:JitterBufferSizeMin v4:NetworkJitterAvg v4:NetworkJitterMax v4:NetworkJitterMin

Parent Element	Child Elements/Attributes
Signal	SignalLevel NoiseLevel InitialSignalLevelRMS RecvSignalLevelCh1 RecvNoiseLevelCh1 RenderSignalLevel RenderNoiseLevel RenderLoopbackSignalLevel VsEntryCauses EchoEventCauses EchoPercentMicIn EchoPercentSend SendSignalLevelCh1 SendNoiseLevelCh1
QualityEstimates.Audio	RecvListenMOS RecvListenMOSMin NetworkMOS
NetworkMOS	OverallAvg OverallMin
NetworkConnectivityInfo	Traceroute

Manually Pairing with BToE

This feature enables users to manually pair their phone with their computer using the Poly Better Together over Ethernet Connector application.

This feature is supported for CCX 400, CCX 500, and CCX 600 phones.

When you enable this feature users can select **Auto** or **Manual** pairing mode in the system web interface or in the **Features** menu on the phone. However, the manual pairing feature no longer requires you to connect the Ethernet cable from your computer to the PC port on your phone. By default, BToE and BToE pairing are enabled for phones registered with Skype for Business. When an administrator disables BToE pairing, users cannot pair their phone with their computer using BToE. When the phone is set to manually pair with your computer connected to a reachable network, the phone generates a pairing code that users must enter into the Poly BToE Connector application to pair.

Note: You can pair and unpair the phone with the BToE application installed in a Citrix Virtual Desktop Infrastructure.

The following table lists the supported UC Software version for the corresponding BToE Connector application for Manual Pairing.

Supported UC Software Version for Manual Pairing

Software Version	BToE Application Version	Manual Pairing	Automatic Pairing
CCX 5.9.12	BToE version 4.3.0	Yes	Yes
CCX 6.2.11	BToE version 4.3.0	Yes	Yes

BToE Widget

By default, users can access BToE settings from the phone menu at **Settings > Features > BToE**.

You can configure a BToE widget to display on the phone's Home screen that allows direct user access to BToE settings. Enabling the BToE widget does not remove access via the phone menu.

BToE Widget Parameters

The following parameters configure the BToE Widget.

`homeScreen.BToE.enable`

1 (default) - Displays the BToE widget on the phone's home screen.

0 - Does not display the BToE widget on the phone's home screen.

Enable or Disable BToE PC Pairing from the Phone

You can enable or disable the BToE PC Pairing feature for Better Together over Ethernet from the phone.

Task

1. On the phone, go to **Settings > Advanced** and enter the administrator password.
2. Select **Administration Settings > BToE PC Pairing**.
3. Select **Enable** or **Disable**.

Enable or Disable BToE PC Pairing from the System Web Interface

You can enable or disable the BToE PC Pairing feature from the system web interface.

Task

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password, and select **Submit**.
3. Go to **Settings > Skype for Business Settings > BToE PC Pairing**.
4. Check or uncheck **Enable BToE PC Pairing**.
5. Click **Save**.

TLS Feature Support for BToE

Poly BToE application supports Transport Layer Security (TLS)

Poly BToE application authenticates the following:

- Poly UC Software can use TLS to authenticate phones using the BToE application.
- TLS takes precedence over SSH.
- If TLS connection fails between the phone and Poly BToE Connector application, then the connection falls back to SSH.

Rebooting the Phone at a Scheduled Time

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

Scheduled Reboot Parameters

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

`prov.scheduledReboot.enabled`

0 (default)— Disables scheduled reboot.

1—Enables scheduled reboot.

`prov.scheduledReboot.periodDays`

Specify the time in days between scheduled reboots.

1 day (default)

1–365 days

prov.scheduledReboot.time

Specify a time to reboot the Poly phone. Use the 24 hour time format (hh:mm).

03:00 (default)

prov.scheduledReboot.timeRandomEnd

If this parameter is set to a specific time, the scheduled reboot occurs at a random time between the time set for `prov.scheduledReboot.time` and `prov.scheduledReboot.timeRandomEnd`. The time is in 24-hour format.

0–5 hours

hh:mm

Updating Poly UC Software

You can update UC Software on a per-phone basis from the phone's local interface or through the system web interface.

Update UC Software Manually

You can use an USB flash drive to update the software and configure the phone.

When you configure the phone using a USB drive, the configuration on the USB overrides all previous configurations. When the USB drive is removed, the system returns to the previous configuration.

Task

1. Download and unzip UC Software to a directory on your provisioning server.
2. On the phone, go to **Settings > Advanced**, enter the administrator password (default `456`).
3. Go to **Network Configuration > Provisioning Server > DHCP Menu > Boot Server**.
4. In the Boot Server menu, choose **Static** if you are testing or provisioning a few phones, or choose **Option 66** if you are provisioning in a large environment and want phones to use a boot server defined in DHCP.

   If you choose **Option 66**, skip step 5 and go to step 6.
5. Go back to **Provisioning Server** and do the following:
   - Choose a server type in the **Server Type** field.
   - Enter the server address. For example,

     ```
     http://server.domain.com/41X
      or
     ftp://ftp.domain.com/41X
     ```
   - Enter your server user name and server password, if required.
6. Press **Back** until you are prompted to save your settings.
7. Choose **Save Configuration** to save your settings.

   The phone reboots.

For details on how to update the phone software using the Web Configuration Utility, see Feature Profile 67993: Using the Software Upgrade Option in the System Web Interface.

Automatic UC Software Updates

By default, the phones poll the Skype for Business Server for software updates and automatically download updated software if it's available. This automatic software update feature is available on all devices registered with Skype for Business Server using UC Software 5.0.0 and later.

An information dialog displays on the phone when a software update becomes available. The dialog provides three options:

- **Reboot** - Select to restart the phone and automatically update the phone's software.
- **Cancel** - Select to cancel the automatic software update. When you select Cancel, a **DevUpdt** softkey displays on the phone's home screen. Press **DevUpdt** at any time to update your phone's software.
- **Details** - Select to view information about current and available software.

When a software update is available and the phone is inactive for a long period of time, the phone automatically reboots and updates the phone's software.

Configuring Automatic Software Updates

The following parameters configure automatic software updates and polling of the provisioning server.

`device.prov.lyncDeviceUpdateEnabled`

0 - The automatic device update is disabled and the phone does not receive software updates from the server.

1 - The automatic device update is enabled and the phone receives software updates from the server.

Change causes system to restart or reboot.

`device.prov.lyncDeviceUpdateEnabled.set`

0 (default) - Disable automatic device update for all devices.

1 - Enable automatic device update for all devices and use `device.prov.lyncDeviceUpdateEnabled`.

Change causes system to restart or reboot.

`lync.deviceUpdate.popUpSK.enabled`

0 (disable) - Disable the Information popup that indicates when an automatic software update is available.

1 - Enable the Information popup that indicates when an automatic software update is available.

Change causes system to restart or reboot.

`lync.deviceUpdate.serverPollInterval`

7200 seconds (default) - The time interval in seconds that the phone sends a software update request to the Skype for Business Server.

min=1800 seconds

max=28800 seconds

Change causes system to restart or reboot.

`lync.deviceUpdate.userInactivityTimeout`

900 seconds [15 minutes] (default) - Sets the user inactivity timeout period after which the phone's software is automatically updated.

Min=300 seconds

Max=1800 seconds

Change causes system to restart or reboot.

prov.polling.enabled

You can choose to automatically poll the provisioning server for software updates.

1 (default) - the phone automatically polls the server for software updates.

0 - Disable automatic polling.

prov.polling.mode

Choose the polling mode.

abs (default) - The phone polls every day at the time specified by `prov.polling.time`.

rel - The phone polls after the number of seconds specified by `prov.polling.period`.

random - The phone polls at random between a starting time set in `prov.polling.time` and an end time set in `prov.polling.timeRandomEnd`.

Note that if you set the polling period in `prov.polling.period` to a time greater than 86400 seconds (one day) polling occurs on a random day within that polling period (meaning values such as 86401 are over 2 days) and only between the start and end times. The day within that period is determined by the phone MAC addresses and does not change with a reboot. The time within the start and end is calculated again with every reboot.

prov.polling.period

The polling period in seconds.

86400 (default)

integer > 3600

The polling period is rounded up to the nearest number of days in absolute and random mode you set in .

In relative mode, the polling period starts once the phone boots.

If random mode is set to a time greater than 86400 (one day) polling occurs on a random day based on the phone MAC address.

prov.polling.time

Specify the polling start time in absolute or random polling mode you choose with `prov.polling.mode`.

03:00 (default)

hh:mm

prov.polling.timeRandomEnd

The polling stop time when the polling mode is set to random.

NULL (default)

hh:mm

Network Configuration

Poly UC Software enables you to make custom network configurations.

Wireless Network Connectivity (Wi-Fi)

To ensure the best performance in your location, set a proper country code with the device.wifi.country parameter before enabling Wi-Fi.

Note: If device.wifi.country is not set, the phone will operate in a world safe mode restricting Wi-Fi channels and power.

You can configure Wi-Fi options to display in the phone's basic settings menu to enable users to manually add a Wi-Fi network. You can also configure the phone to display the Wi-Fi icon on the phone's status bar and home screen.

Enabling Wi-Fi automatically disables the Ethernet port. You can't use Wi-Fi and Ethernet simultaneously to connect phones to your network. When you connect the system to your network over Wi-Fi, only audio-only calls are available. The phones don't support Wi-Fi captive portals or wireless display (WiDi).

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

Enable Wi-Fi

You can wirelessly connect phones to your network using Wi-Fi, which is disabled by default.

When you enable Wi-Fi, the system reboots.

Task

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

Configure Wireless Network Settings with EAP

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

Task

1. Go to **Settings > Advanced > Administrator Settings > Network Configuration > Network Interfaces > Wi-Fi Menu**.
2. Turn Wi-Fi to **On**.
   The phone reboots.
3. After the phone reboots, go to **Settings > Advanced > Administration Settings > Network Configuration > Network Interfaces > Wi-Fi Menu** to view available networks.
4. Configure the following wireless network settings:
   - **A** Select the SSID name of the wireless network.
   - **B** Select the security type of the wireless network.
   - **C** Optional: If you have an enterprise-based network, enter the **User ID** and **Password**.
   - **D** Select one of the following EAP- Method types for authentication:
     - EAP-PEAP-MSCHAPv2
     - EAP-TTLS-MSCHAPv2
     - EAP-PWD
     - EAP-TLS
5. Select a network and press **Connect**.

Wi-Fi Parameters

The parameters you configure depend on the security mode of your organization and whether or not you enable DHCP.

CCX 600 business media phones include a security-restrictive worldwide Wi-Fi country code setting.

The CCX 600 business media phones support the following Wi-Fi security modes:

- WPA PSK
- WPA2 PSK
- WPA2 Enterprise

device.wifi.country

NULL (default)

Two-letter country code

device.wifi.dhcpEnabled

Enable or disable DHCP for Wi-Fi.

0 (default) - Disable

1 - Enable

device.wifi.ipAddress

Enter the IP address of the wireless device if you are not using DHCP.

0.0.0.0 (default)

String

device.wifi.ipGateway

Enter the IP gateway address for the wireless interface if not using DHCP.

0.0.0.0 (default)

String

device.wifi.psk.key

Enter the hexadecimal key or ASCII passphrase.

0xFF (default)

String

device.wifi.psk.keyType

Set the Pre-Shared Key (PSK) type.

0 (default) - Passphrase.

1 - Hexadecimal key.

device.wifi.securityMode

Specify the wireless security mode.

NULL (default)

WPA-PSK

WPA2-PSK

WPA2-Enterprise

device.wifi.ssid

Set the Service Set Identifier (SSID) of the wireless network.

SSID1 (default)

SSID

device.wifi.subnetMask

Set the network mask address of the wireless device if not using DHCP.

255.0.0.0 (default)

String

device.wifi.wpa2Ent.method

Set the Extensible Authentication Protocol (EAP) to use for 802.1X authentication.

Null (default)

EAP-PEAPv0/MSCHAPv2

EAP-TTLS-MSCHAPv2

EAP-PEAPv0-NONE

EAP-TTLS-NONE

EAP-PWD

EAP-TLS

device.wifi.wpa2Ent.password

The WPA2-Enterprise password.

device.wifi.wpa2Ent.user

The WPA2-Enterprise user name.

feature.wifiUserSettings.enabled

1 (default) – Display Wi-Fi menu options on the phone menu.

0 – Wi-Fi menu options do not display on the phone menu.

homeScreen.wifi.enable

1 (default) – Display the Wi-Fi icon on the phone's Home screen.

0 – Do not display the Wi-Fi icon on the phone's Home screen.

status.wifi.icon.enable

1 (default) – Display the Wi-Fi icon on the status bar of the phone's screen. Users can access Wi-Fi settings by selecting the Wi-Fi icon.

0 – Do not display the Wi-Fi icon on the status bar.

Configuring Bluetooth

You can enable Bluetooth to allow users to connect and pair compatible Bluetooth devices such as a mobile phone, tablet, laptop, or headset with Poly CCX.

Bluetooth is disabled by default. You must configure the following parameters to enable Bluetooth and allow devices to find and pair with your CCX:

- `feature.bluetooth.enabled`
- `bluetooth.radioOn`

After you enable Bluetooth, you can pair and cache a maximum of six Bluetooth devices with the CCX phone and connect a maximum of two devices at a time, or pair the Poly CCX phone with one of your devices.

When you pair your Bluetooth headset to the phone, you can use your headset to manage call audio. When you pair the phone to your PC, tablet, or mobile phone, you can use the phone to answer a call, end a call, or reject a call.

Note that using a Bluetooth headset can affect voice quality on the phone due to inherent limitations with Bluetooth technology. You may not experience the highest voice quality when using a Bluetooth headset while the 2.4 GHz band is enabled or while you are in an environment with many other Bluetooth devices.

Note: Bluetooth is available on Poly CCX 500, CCX 505, and CCX 600 business media phones only. This feature is not available on Poly CCX 350 or CCX 400 business media phones.

Bluetooth Parameters

Use the parameters in the following list to configure Bluetooth.

`bluetooth.device.discoverable`

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

0 - This device is not discoverable for Bluetooth pairing.

`bluetooth.device.name`

NULL (default)

UTF-8 string

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

`bluetooth.discoverableTimeout`

Set the time in seconds after which other devices can discover this device over Bluetooth.

0 (default) - Other devices can always discover this device over Bluetooth.

0 - 3600 seconds

`bluetooth.pairedDeviceMemorySize`

Set the maximum number of devices that can be paired and cached as paired on the phone.

10 (default)

0 - 10

`bluetooth.radioOn`

0 - The Bluetooth radio transmitter/receiver is off.

1 (default) - The Bluetooth radio is on. You must turn on the Bluetooth radio to allow devices to connect over Bluetooth.

`feature.bluetooth.enabled`

For high security environments.

1 (default) – Enable Bluetooth and the Bluetooth phone screen icon.

0 - Disable Bluetooth and the Bluetooth phone screen icon.

Supported Bluetooth Profiles

To pair devices via Bluetooth, ensure that paired devices use Bluetooth profiles supported by Poly phones.

Poly CCX phones support the following Bluetooth application profiles:

- Headset Profile (HSP) (both Gateway and Device)
- Hands-Free Profile (HFP) (both Gateway and Device)
- Advanced Audio Distribution Profile (A2DP) (Both Source and Sink)

Extended Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is used by network devices to advertise their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

LLDP is enabled by default.

Media Endpoint Discover (MED) capabilities include:

- Network policy discover
- Endpoint location identification discovery
- Extender power discovery required for endpoint

Configuring LLDP Fast Start Count

Fast start count enables a device to initially advertise itself over the network at a fast rate for a limited time when an LLDP-MED endpoint has been newly detected or connected to the network.

`device.net.lldpFastStartCount`

Configure the fast-start LLDP packets that the phone sends when booting up or when the network comes up.

5 (default)

3 - 10

If fast-start packet count is configured > 10, the value resets to 10. If the fast-start packet count is < 3, the value resets to 3. If you configure an invalid value-for example, a negative value, string, or character-the value resets to default 5.

Web Proxy Auto Discovery (WPAD)

The Web Proxy Auto-Discovery Protocol (WPAD) feature enables Poly phones to locate the URL of a Proxy Auto-Configuration (PAC) file you configure.

You can configure WPAD using configuration parameters on your provisioning server, DHCP Option 252, or the DNS-A protocol mechanism to discover the PAC file location. When using a provisioning server or DHCP, the phone looks for the file name you specify. If using DNS-A, the phone looks only for the wpad.dat file.

PAC File Search Priority
Poly phones search for PAC files in the following priority order:

- Provisioning server. Example: `feature.wpad.curl="http://server.domain.com/proxy.pac`
- DHCP Option 252. For instructions, see *Creating an Option 252 entry in DHCP* on Microsoft TechNet: https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc995090(v=technet.10)?redirectedfrom=MSDN
- DNS-A. For instructions, see *Creating a WPAD entry in DNS* on Microsoft TechNet: https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc995062(v=technet.10)?redirectedfrom=MSDN

Supported HTTP/HTTPS Web Proxy Services
When the web proxy server is successfully configured and operational, the phones route the following HTTP/HTTPS web proxy services to the web proxy server:

Generic Services

- HTTP/HTTPS Provisioning
- Core File Upload

Skype for Business Services

- Registration Services
- Address Book Service (ABS)
- Location Information Server (LIS)
- Device Update (To ensure reliable software updates, device update is direct in case a proxy is not available.)
- Server Log Upload
- Exchange Web Services

View Web Proxy Diagnostics on the System Web Interface

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

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

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

Task

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

Web Proxy Configuration Parameters

The following parameters configure web proxy settings.

`feature.wpad.enabled`

Set to enable web proxy.
0 (default) - Disables web proxy.

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

Change causes system to restart or reboot.

`feature.wpad.curl`

Enter the PAC file location.

Change causes system to restart or reboot.

`feature.wpad.proxy`

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

0 to 255 characters

Change causes system to restart or reboot.

feature.wpad.proxy.username

Enter the user name to authenticate with the proxy server.

0 to 255 characters

Change causes system to restart or reboot.

feature.wpad.proxy.password

Enter the password to authenticate with the proxy server.

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

0 to 255 characters

Change causes system to restart or reboot.

Data Center Resiliency

Data center resiliency ensures that minimum basic call functions remain available in the event of a server shutdown or Wide Area Network (WAN) outage.

The phones you register with Skype for Business on-premises are enabled with this feature by default and no additional configuration is required.

In the event of an unplanned server shutdown or outage, phone behavior changes to the following:

- The phone displays a scrolling banner message 'Limited functionality due to outage'.
- Your presence status displays as 'Unknown'.
- The presence status of your contacts displays as 'Unknown'.
- You cannot change your presence status.
- You cannot add or delete Skype for Business contacts.
- Phones in the locked state display a message on the Sign In menu 'Limited functionality due to outage'.
- You can access current Call Forwarding settings in read-only mode.

TURN / ICE Parameters

Use parameters in this list to configure Traversal Using Relays Around NAT (TURN) and Interactive Connectivity Establishment (ICE).

tcpIpApp.ice.ConnCheckInetvalPairs

Time interval in milliseconds to serialize first attempt of connectivity check of identified ICE candidate pairs per call.

25 - 100

tcpIpApp.ice.ConnCheckInetvalRetries

Time interval in milliseconds to serialize the retry attempts of connectivity check for identified pairs per call.

25 - 100

tcpIpApp.ice.MaxRetries

The maximum number of retry attempts performed on each ICE connectivity check pair identified in case of a request timeout or failure.

5 (default)

2 - 25

tcpIpApp.ice.mode

MSOCS (default)

Disabled

Standard

tcpIpApp.ice.NetworkMode

TCPUDP (default) – Gathers all the possible UDP and TCP ICE candidates.

TCPOnly – Gathers all the TCP candidates along with UDP host candidates.

UDPOnly - Gathers all the UDP candidates.

tcpIpApp.ice.password

Enter the password to authenticate to the TURN server.

NULL (default)

tcpIpApp.ice.ReflexiveChecksRequired

1 (default) - TCP and UDP reflexive candidates will be collected in candidate gathering process.

0 - TCP and UDP reflexive candidates will not be collected in candidate gathering process.

tcpIpApp.ice.stun.server

Enter the IP address of the STUN server.

NULL (default)

tcpIpApp.ice.stun.udpPort

The UDP port number of the STUN server.

3478 (default)

1 - 65535

tcpIpApp.ice.tcp.enabled

1 (default) - Enable TCP.

0 - Disable TCP.

tcpIpApp.ice.turn.server

Enter the IP address of the TURN server.

NULL (default)

tcpIpApp.ice.turn.tcpPort

443 (default)

1 - 65535

tcpIpApp.ice.turn.udpPort

The UDP port number of the TURN server.

443 (default)

65535

tcpIpApp.ice.username

Enter the user name to authenticate to the TURN server.

NULL (default)

Updating Poly UC Software

You can update UC Software on a per-phone basis from the phone's local interface or through the system web interface.

Update UC Software Manually

You can use an USB flash drive to update the software and configure the phone.

When you configure the phone using a USB drive, the configuration on the USB overrides all previous configurations. When the USB drive is removed, the system returns to the previous configuration.

Task

1. Download and unzip UC Software to a directory on your provisioning server.
2. On the phone, go to **Settings > Advanced**, enter the administrator password (default `456`).
3. Go to **Network Configuration > Provisioning Server > DHCP Menu > Boot Server**.
4. In the Boot Server menu, choose **Static** if you are testing or provisioning a few phones, or choose **Option 66** if you are provisioning in a large environment and want phones to use a boot server defined in DHCP.

   If you choose **Option 66**, skip step 5 and go to step 6.
5. Go back to **Provisioning Server** and do the following:
   - Choose a server type in the **Server Type** field.
   - Enter the server address. For example,

     ```
     http://server.domain.com/41X
      or
     ftp://ftp.domain.com/41X
     ```
   - Enter your server user name and server password, if required.
6. Press **Back** until you are prompted to save your settings.
7. Choose **Save Configuration** to save your settings.

   The phone reboots.

For details on how to update the phone software using the Web Configuration Utility, see Feature Profile 67993: Using the Software Upgrade Option in the System Web Interface.

Troubleshooting

This section provides information on troubleshooting CCX business media phones.

General Troubleshooting Tasks

If you experience issues with your CCX phone, review the following troubleshooting information to try to resolve your issue.

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.

Task

1. Disconnect the power, then reconnect power to the Poly phone.
2. Do one of the following:
   - On CCX 350 phones, as soon as the Poly logo appears, press and hold the 1, 3, and 5 keys simultaneously.
   - 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, or CCX 600 phones, as soon as the Poly logo appears 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.

Troubleshooting Microsoft Teams

Refer to the following topics to help you diagnose and fix issues with your CCX business media phones when using Microsoft Teams.

For more information on troubleshooting Microsoft Teams or to get additional support, see Welcome to Microsoft Teams at Microsoft Docs.

System Logs

System log files assist when troubleshooting issues.

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

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

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

Set the Logging Level for a Phone

You can enable logging and set the logging level for general logs from the **Admin Settings** menu on an individual CCX phone.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Settings** and enter the administrator password (the default is 456).
3. Select **Debug**.
4. Tap the switch for **Logging** to enable the feature.
5. Tap **Log Level**, and select a severity level.

Set Log Levels from the System Web Interface

You can set log levels from the system web interface.

Task

1. Enter the IP address of the phone into a web browser and log in as Administrator or User.
2. Go to **Settings > Logging**.
3. In **Server Log Level**, select a log level.

Capture Your Phone's Screen

You can take a snapshot of a phone's screen to record any troubleshooting issues.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Only**.
3. Select **Debug**, and tap the switch to enable **Screen Capture**.
4. In a web browser, enter `https://<phoneIPaddress>/captureScreen` into the address field, where `<phoneIPaddress>` equals your phone's IP address.
5. If prompted, enter the login credentials.
   The web browser displays an image showing the phone's current screen. You can save the image as a BMP or JPEG file.

Troubleshooting Skype for Business

Refer to the following topics to help you diagnose and fix issues with your CCX business media phones when using Skype for Business.

For more information on troubleshooting Skype for Business or to get additional support, see Skype for Business at Microsoft Docs.

System Logs

System log files assist when troubleshooting issues.

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

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

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

Upload Logs to the Skype for Business Server

To help troubleshoot phone issues for phones registered with Skype for Business, you can allow users to upload logs to the Skype for Business server from the phone or Web Configuration Utility. Users can also set log levels for the phone.

This feature is available on the phones registered with Skype for Business Server On-premises or Online and with Microsoft Lync 2013 or 2010 Server.

Logs are uploaded to the Skype for Business Server at the following location, which you can specify in the Skype for Business topology builder or at initial installation:

```
<LYNC_SERVER_LOG_PATH>\1-WebServices-1\DeviceUpdateLogs\Client\CELog
```

Phones support Core File Uploads to help log phone crashes. The logs are uploaded to the Skype for Business server in tar.gz format. The Skype for Business server must support tar.gz format to decrypt the log file uploaded to server.

Upload Logs Parameters

Use the following parameters to configure log uploading to the Skype for Business server.

`feature.logUpload.enabled`

1 (default) - Enable users to upload logs to the Skype for Business server from the phone.

0 - Do not allow users to upload log files to the Skype for Business server.

`Log.render.file`

When you enable this option, the phone first writes log files directly into its flash memory. The contents of the flash memory upload to a provisioning server after a predetermined period of time or when the flash memory becomes full. Poly recommends not changing this parameter.

1 (default) – Disabled

0 – The phone is prevented from uploading its contents from memory to the server. Disabling the ability to upload log files is recommended only when necessary to reduce data traffic when the phone starts or reboots.

Send Logs from the Phone

To help troubleshoot issues, you can send logs from the phone to the Skype for Business server.

Task

» Go to **Settings > Basic > Diagnostic Logs > Upload Logs**.
The files are uploaded to the server as plain text.

Send Diagnostic Logs from the System Web Interface

To help troubleshoot issues, you can send diagnostic logs to the Skype for Business server from the system web interface.

This option is available when logged in as Administrator or User.

Task

1 Enter the IP address of the phone into a web browser and log in as Administrator or User.
2 Go to **Diagnostics > Upload Logs**.
The files are uploaded to the server as plain text.
3 View uploaded URLs at **Skype for Business Status > Skype for Business Parameters** and one of the following locations:

- Update Server Internal URL for on-premises deployments.
- Update Server External URL online deployments.

Logging Levels

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

Two types of logging are supported:

- Level, change, and render
- Schedule

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

Logging Levels

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

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

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

Set the Logging Level for a Phone

You can enable logging and set the logging level for general logs from the **Admin Settings** menu on an individual CCX phone.

Task

1. Go to **Settings > Device Settings**.
2. Select **Admin Settings** and enter the administrator password (the default is 456).
3. Select **Debug**.
4. Tap the switch for **Logging** to enable the feature.
5. Tap **Log Level**, and select a severity level.

Set Log Levels from the System Web Interface

You can set log levels from the system web interface.

Task

1. Enter the IP address of the phone into a web browser and log in as Administrator or User.
2. Go to **Settings > Logging**.
3. In **Server Log Level**, select a log level.

Support

NEED MORE HELP?

poly.com/support

Poly Worldwide Headquarters

345 Encinal Street
Santa Cruz, CA 95060
United States