poly

Polycom UC Software with Skype for Business

PLANTRONICS + POLYCOM. NOW TOGETHER AS poly

Contents

Getting Started

Topics:

This guide provides general guidance on installing and provisioning with Polycom UC Software and shows you how to deploy Polycom devices in Microsoft environments.

Support for Lync 2010 is limited to testing of basic call scenarios. Microsoft support of Lync and Skype for Business is documented on Microsoft's website. Microsoft does not currently support IP phones on Lync 2010. For information, see IP Phones on Microsoft Support.

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
- Open SIP networks and VoIP endpoint environments

UC Software Device Compatibility

Polycom UC Software supports the following devices with Skype for Business:

- Polycom® VVX® 201 business media phones
- Polycom® VVX® 250 business IP phones (on-premise only)
- Polycom® VVX® 300, 301, 310, 311 business media phones
- Polycom® VVX® 350 business IP phones (on-premise only)
- Polycom® VVX® 400, 401, 410, 411 business media phones
- Polycom® VVX® 450 business IP phones (on-premise only)
- Polycom® VVX® 500 and 501 business media phones
- Polycom® VVX® 600 and 601 business media phones
- Polycom® SoundStructure® VoIP interface phones

If you are using previous versions of UC Software to register SoundStructure VoIP Interface with Lync Server, see *Polycom SoundStructure VoIP Interface for Use with Microsoft Lync Server* at Polycom SoundStructure on [Polycom Support](#).

Polycom VVX phones and SoundStructure VoIP interface support Skype for Business and Lync Server 2013. Note that Microsoft now supports multiple clients:

- Skype for Business 2016 (v16.x)
- Lync 2013 / Skype for Business 2015 (v15.x)

Microsoft Qualified Phones

Polycom offers devices with an Open SIP or a Skype Base Profile. Polycom also offers devices already configured for use with Skype for Business on-premises deployments or Skype for Business Online. These devices include Microsoft-qualified UC Software with a feature license included and enable you to start up the phone and register with default settings.

Feature Licenses

Polycom devices purchased and shipped with a Skype or Lync Base Profile include a Poly feature license to register with Skype for Business, Lync Server, and Office 365.

If you do not purchase devices with a configured Skype or Lync Base Profile, you can use Polycom phones in a Skype for Business, Lync Server, or Office 365 environment for trial purposes, without purchasing a license, for a maximum of 30 days.

For information about purchasing a Polycom feature license, talk to your reseller or sales representative.

Skype for Business Topologies

Polycom support for a Skype for Business topology varies by environment.

Supported Skype for Business Topologies

The following table lists Polycom support for each Skype for Business topology.

Note that VVX business IP phones support on-premises topologies only.

Polycom-Supported Skype for Business Topologies

Topology	Active Directory	Skype for Business	Exchange
On-premises	On-premises	On-premises	On-premises
Hybrid Voice/Cloud Connector Edition	On-premises	Online	Online
Office 365 Multi-tenant (O365MT)	Online	Online	Online

Topology	Active Directory	Skype for Business	Exchange
Hybrid (Split-Domain)	On-premises	On-premises	Online
	On-premises	Online	Online
	On-premises	Online	On-premises

Prerequisites - On-Premises Deployments

You need to modify some settings of Skype for Business before you set up devices for an on-premises Skype for Business deployment.

Ensure that you complete the following tasks:

- Set the server log levels to capture only low-level events. For information on setting logging levels, see Set-CsUCPhoneConfiguration on Microsoft Docs.
- Disable automatic device update by setting:
    - `Set-CsIPPhonePolicy -EnableDeviceUpdate $False` For more information see Set-CsIPPhonePolicy on Microsoft TechNet.
    - `device.prov.lyncDeviceUpdateEnabled.set="1"`
    - `device.prov.lyncDeviceUpdateEnabled="0"`

UC Software File Formats for Skype for Business

offers UC Software for Skype for Business in two file formats:

- Combined or Split **sip.ld**.
- offers UC Software in CAB file format. This Microsoft Windows archive file format, recommended by Microsoft for customer premises equipment (CPE), safely compresses data and embeds digital certificates.

Skype for Business On-Premises and Online Features

The following table lists Polycom UC Software support for Skype for Business on-premises and Online features.

Polycom with Skype for Business Online Feature Support

Skype for Business Feature	Polycom with Skype for Business On-Premises	Polycom with Skype for Business Online
Resiliency - Branch Office		na
Resiliency - Data Center Outage	✓	na
Call Park	✓	x

Skype for Business Feature	Polycom with Skype for Business On-Premises	Polycom with Skype for Business Online
PIN Authentication	✓	x
Attendant Console	✓	x
Cross Pool	✓	x
Media Bypass	✓	x
Response Groups	✓	x
Private Line	✓	x
Web Sign In	x	✓
Common Area Phone (CAP)	✓	✓
Host Desking	✓	✓
Enhanced Feature Line Key (EFLK)	✓	✓
Enhanced 911 (E.911)	✓	✓
Web Proxy Auto Discovery	✓	✓
Quality of Service for Audio Calls	✓	✓
Device Lock	✓	✓
Distribution Lists	✓	✓
Quality of Experience (QoE)	✓	✓
User Log Upload	✓	✓
BToE Manual Pairing	✓	✓
Device Update	✓	✓
In-band Provisioning	✓	✓
Call Handling	✓	✓
Call Forward	✓	✓
Call Transfer	✓	✓
Conference Calls	✓	✓
Local Call Logs	✓	✓

Skype for Business Feature	Polycom with Skype for Business On-Premises	Polycom with Skype for Business Online
Exchange Call Logs	✓	✓
Federated Calls	✓	✓
Simultaneous Ring	✓	✓
Dual Tone Multi Frequency	✓	✓
Emergency 911	✓	✓
Call Admission Control	✓	✓
Monitoring (Device Inventory)	✓	✓
Delegates	✓	✓
Team Call	✓	✓
Message Waiting Indicator	✓	✓
Exchange Integration	✓	✓
Exchange Calendar		
Extended Presence	✓	✓
Visual Voicemail	✓	✓
Boss-Admin	✓	✓

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Polycom Support Site is the entry point to online product, service, and solution support information including **Licensing & Product Registration**, **Self-Service**, **Account Management**, **Product-Related Legal Notices**, and **Documents & Software** downloads.

- The Polycom Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.

- The Polycom Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.

- The Polycom Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.

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

Deploying Poly Phones with Skype for Business

Topics:

- [Configure the Network](#)
- [Set Up Polycom UC Software](#)
- [Provisioning Skype for Business Phones](#)
- [Configuring In-Band Provisioning Settings](#)

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

As of UC Software 5.3.0, Poly phones ordered with the Skype SKU are shipped with Skype for Business-qualified software that enables you to start up the phone and register with default settings.

Note: 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 complete the task Set Up the Network. If you want to customize default settings, complete all three tasks.

Configure the Network

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

Procedure

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

   For information on creating and verifying DNS SRV records, see the latest documentation on [Microsoft TechNet](#).

2. Optional: If you are setting Microsoft Call Admission Control (CAC) refer to Microsoft Plan for call admission control in Skype for Business Server 2015 for required bandwidth guidelines.

3. 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)	Devices running UC Software 5.3.0 or later that you are registering with Skype for Business automatically fetch the root certificate using a LDAP DNS query. Phones you register with Skype for Business are enabled with this feature by default and no additional configuration is required.
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. In conjunction 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 are using a provisioning server or setting DHCP options using the following: • DHCP Option 160. If you are 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.

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

Also set up PIN Authentication type if you are using any of the following devices in your deployment: VVX 201, 300/310, 301/311, 400/410, 401/411, 500/501, 600/601 business media phones, VVX 250, 350, and 450 business IP phones, and SoundStructure VoIP Interface.

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	Result
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 Polycom UC Software

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

Make sure you have an XML editor, such as XML Notepad, installed on your computer to update the provisioning. Your provisioning, or boot server must support one of the FTP, FTPS, TFTP, HTTP, or HTTPS protocols, FTP being the most common. FileZilla Server is a free FTP solution.

All UC Software versions are available on the Polycom UC Software Support Center.

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.

Procedure

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. Decide if you are provisioning your phones from Skype for Business Server or using your own provisioning server.

    Deploying UC Software in CAB file format provisions the phones and enables default feature functionality, including the automatic software update feature. However, if you want to change or customize default functionality of the phone features, you need to set up and edit UC Software configuration files on your own provisioning server and send the custom settings to the phones.
3. Download, save, and extract UC Software to the root directory you created.

    • If you are deploying UC Software from Skype for Business Server, download the CAB file version of UC Software.

    • If you are deploying phones from your own provisioning server, download the split or combined version of UC Software in XML format.
4. After the UC Software directory is extracted, open the folder in your root directory.
5. 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.
6. (Optional) To use the BToE feature, download the Polycom BToE connector application and enable BToE.

For complete instructions on setting up BToE, see the latest *Polycom VVX Business Media Phones for Skype for Business - User Guide* on [Polycom UC Software for Microsoft Deployments](#).

Provisioning Skype for Business Phones

Polycom offers several centralized provisioning methods for mass provisioning and several per-phone provisioning methods. This section outlines a few options that may help you decide which method is best for your Skype for Business deployment.

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 that simplifies the process of registering your devices with Skype for Business. 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 cannot modify or customize the Base Profile or feature settings. Because you can provision only a single phone at a time from the local phone menu, use centralized provisioning for deployments of greater than 20 devices requiring only default Skype for Business settings.

If you are using Polycom UC Software 5.1.1 or later, the per-phone Web Configuration Utility is disabled by default and you cannot register phones using the Web Configuration Utility. If you want to configure phone options using a phone's Web Configuration Utility after registering the phone with the Skype for Business Server, you must enable access to the Web Configuration Utility.

For complete information on provisioning with Polycom UC Software, see the *Polycom UC Software Administrator Guide* on [Polycom UC Software for Microsoft Deployments](#).

Manual Provisioning Methods

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

All manual provisioning methods set the Base Profile of a phone to **Skype**. The Base Profile is a feature on each phone that, when set to **Skype**, 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** when provisioning with configuration files.

Manually Reboot the Phone

When you change the Base Profile using any of these methods, the phone reboots.

If the phone does not reboot, you can manually reboot by powering off/on the phone or manually rebooting the phone from the Settings menu.

Procedure

1. Go to **Settings > Advanced**.
2. Enter the password (default 456).
3. Press **Enter**.
4. Choose **Reboot Phone**.

When the phone completes the reboot cycle, the Sign In screen displays.

Set the Base Profile of VVX Phones to Skype Using MKC During Startup

You can set the Base Profile of a phone to **Skype** during the phone startup cycle in two ways: by using an MKC method during startup or from the phone boot Setup menu.

The MKC during startup is the fastest manual provisioning method.

If your phones are not brand new and directly from the manufacturer, ensure that you reset the phones to factory default settings before setting the Base Profile manually.

Procedure

1. Power on the phone or restart it after you have reset the phone to factory default settings.
2. A few seconds into the device's startup cycle, the phone displays the message 'Starting Application', press Cancel to interrupt and a Cancel soft key.

   Press the **Cancel** soft key.
3. When the phone displays three soft keys—Start, Setup, and About—press and hold **1, 4, 9** on the phone keypad for about 3 seconds to enter the MKC.
4. Press and hold the MKC keys to cause the Base Profile Password menu to display.

   Enter the password (default 456) to change the Base Profile and press **Ok**.

   The **Base Profile** menu displays.
5. Press the **Edit** soft key, use the keypad keys to set the Base Profile to **Skype**, and press **Ok** > **Exit**.
6. Highlight **Save & Reboot** and press the **Select** soft key.

   The phone reboots and displays the Sign In screen. Users can now sign in.

Set the Base Profile of VVX Phones to Skype from the Setup Menu During Startup

When you boot up the phone, you can set the Base Profile to **Skype** using the Setup menu available during the phone startup process.

Procedure

1. Power on the phone or restart after you have reset the phone to factory default settings.
2. A few seconds into the device power-up cycle, the phone displays the message 'Starting Application, press Cancel to interrupt' and a Cancel soft key.

   Press the **Cancel** soft key.
3. When the phone displays three soft keys—Start, Setup, and About—press the **Setup** soft key, enter the password (default 456), and press **Ok**.

   The phone displays a diagram of keypad keys you can use to navigate the Setup menu. You will need to use these keys in the next few steps.
4. Press the **Setup** soft key and the Setup menu displays.
5. Using the keypad keys, scroll down, highlight **Base Profile**, and select the **Edit** soft key.
6. Using the keypad keys, set the Base Profile to **Skype**, and press **Ok > Exit.**
7. Highlight **Save & Reboot** and press the **Select** soft key.
8. The phone reboots and displays the Sign In screen.

   Users can now sign in.

Set the Base Profile of VVX Phones Using MKC

This section shows you two ways to set the Base Profile to **Skype** from the Settings menu when the phone is idle, and how to sign in and register a line.

Procedure

1. Press the phone's **Home/Menu** key.
2. From the idle screen, press and hold the following key combinations **1, 4, 9** on the phone keypad for about 3 seconds.
3. Press and hold the MKC keys to cause the Base Profile screen to display.

   Enter the password (default 456) and press **Enter**.
4. In the **Base Profile** menu, select **Skype**.

   The phone automatically restarts and displays the Sign In screen. Users can now sign in using one of the Sign In Methods.

   If the phone does not restart, choose **Settings > Basic > Restart**, or power the phone off and then on.

If your phone supports PIN authentication, you will be prompted for authentication. Otherwise, you will be prompted for Skype for Business sign-in credentials.

Related Links
Sign In Methods on page 23

Set the Base Profile from the Settings Menu

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

Procedure

1. Go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration**, and set Base Profile to **Skype**.
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 Web Configuration Utility

You can use the Web Configuration Utility to manually set a phone's Base Profile to **Skype**.

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

Procedure

1. Provide power to your phones and allow the phones 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 Web Configuration Utility 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**, 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.

Related Links

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.
- Download UC Software in CAB file format and place the software on Skype for Business Server. Default feature settings are applied to all your phones.
  - This method requires you to set up your own provisioning server. Setting up your own provisioning server enables you to customize feature settings using the template configuration files included in the UC Software download. With this method, users can sign in with their credentials from the phone's interface.
- Use `device.*` parameters to configure multiple devices and only if you are 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.

Polycom offers Skype for Business Online and Exchange Online for:

- VVX 201, 300/310, 301/311, 400/410, 401/411, 500/501, and 600/601 business media phones

---

Note: VVX 250, 350, and 450 business IP phones do not support Skype for Business Online. VVX business IP phones support Skype for Business on-premises only.

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.
- The phones support use of ZTP staging for software upgrades.

You can configure and manage VVX business media phones from the Office 365 online interface without the need for a separate provisioning server. After you set up phones, the first time users log in to a phone, users are prompted by a menu to set the time zone.

Procedure

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 Skype for Business Server

If you downloaded UC Software files in CAB format, complete the following procedure to deploy UC Software from Skype for Business Server.

Procedure

1. Download and save UC Software in CAB file format to your computer.

   You can obtain all Microsoft-compatible UC Software from UC Software for Microsoft Deployments.
2. Go to Skype for Business Server and copy the CAB file to a C: drive directory.
3. Use the Skype for Business Server Management Shell to go to a particular directory.
4. In the Skype for Business Server Management Shell, run the following import command:

   ```
   Import-CsDeviceUpdate -Identity service:1-WebServices-1 -FileName
   UCUpdates.cab
   ```

5. In the Skype for Business Control Panel, go to **Clients** > **Device Update** to view UC Software versions available on Skype for Business Server.
6. Go to **Clients** > **Action** > **Approve** to approve the UC Software.

Deploying UC Software from a Provisioning Server

Setting up your own provisioning server enables you to customize feature settings using the template configuration files included in the UC Software download.

All configuration files are saved in compressed ZIP file format and you must unzip (extract) the files before use.

Poly provides the UC Software download in two file formats:

- **Split files**. Enable you to choose UC Software for specific phone models. The split files are smaller in size with faster update times, and they reduce internal network traffic during reboots and updates.
- **Combined file**. A large directory that contain software files for all Poly phone models.

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.

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

Procedure

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 boot-up is complete, remove `device.set` from the template configuration file and save the file again after removing `device.set`.

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.

Related Links

[Quality of Service for Audio and Video Calls](#) on page 138

Sign In Methods

Topics:

You can configure users to sign in or out of the phone using one of 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.

  As of UC Software 5.1.1, this sign in method is available on the SoundStructure VoIP Interface.

- **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.

- **Sign In with Better Together over Ethernet (BToE)** - If you use the BToE feature in your deployment, you can sign in to the phone from the PC client when the phone and computer are connected through the BToE application.

- **CAP Web Sign In** - Use this method to securely sign in from a browser on your computer or mobile device when CAP Admin Mode is enabled on the phone. The phone generates a unique pairing code you use to sign in to the CAP Provisioning Portal 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**. VVX 201 business media phones do not display these messages due to screen size limitations.

Related Links
[Set the Base Profile of VVX Phones Using MKC](#)

Configuring a Skype for Business Sign In Method and Credentials

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 (default) - 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.

You can enable PIN authentication for VVX business media phones, VVX business IP phones, and SoundStructure VoIP Interface registered with Skype for Business.

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.

Note: Polycom VVX 250, 350, and 450 business IP phones support On-Premises deployments only.

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.

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.

Procedure

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 click **Submit**.
3. Select **Settings**.
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 the 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

Technology Name	Skype for Business	Modern Authentication on Skype for Business	Microsoft Exchange	Modern Authentication on Microsoft Exchange	Supported?
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 and video 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 Common Area Phone (CAP) mode is enabled along with Online Web Sign In and the phone is set to CAP Admin mode, you can sign in to the phone registered with Skype for Business Online and securely login 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.

Sign-In and Sign-Out Soft Keys Parameters

If your phones are used as shared devices in your organization, you can remove the sign-out soft key to prevent users from signing others out.

Or, you can remove both 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 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 Web Configuration Utility.

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 Web Configuration Utility.

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

Topics:

- [Skype for Business](#)
- [Integrating with Microsoft Exchange](#)
- [Configuring the Microsoft Exchange Server](#)

If you have a Skype for Business, Office 365, Lync Server 2010 or 2013 deployment, you can integrate with Microsoft Exchange Server.

You can set up visual voicemail, call log synchronization, Outlook contact search, and Skype for Business Address Book Service (ABS) adaptive search. Each of these features is enabled by default on Poly phones registered with Skype for Business.

After the phone is connected with the Exchange Server, you can:

- Verify the status of Exchange Server services on each phone.
- View the status of each service in the Web Configuration Utility.

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:

- VVX 201, 300 series, 400 series, 500 series, and 600 series business media phones
- VVX 250, 350, and 450 business IP phones
- SoundStructure VoIP Interface 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

You can integrate with Microsoft Exchange using one of the following methods:

- Exchange Server auto-discover
- Provision the phone with the Microsoft Exchange address
- Web Configuration Utility

Note: If you enter the Skype for Business credentials to the configuration file, phone users must enter credentials to the phone **Sign In** screen.

Provision the Microsoft Exchange Calendar

You can provision your phones with the Microsoft Exchange calendar.

Procedure

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

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

Enable Microsoft Exchange Calendar Using the Web Configuration Utility

You can use the Web Configuration Utility to manually enable your phones with the Microsoft Exchange calendar.

Enable the access to the Web Configuration Utility on the phone registered with Skype for Business.

This is useful for troubleshooting if auto-discovery is not working or is mis-configured. Enabling Microsoft Exchange Calendar through the Web Configuration Utility can only be performed on one phone at a time.

Procedure

1. Log in to the Web Configuration Utility as an Admin (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`.

   In this example, the URL part `<mail.com>` is specific to an organization.
5. At the bottom of the browser page, click **Save**.
6. When the confirmation dialog displays, click **Yes**.

   Your Exchange Calendar is successfully configured and the Calendar icon displays on your phone screen.

Verify the Microsoft Exchange Integration

You can verify if all of the Exchange services are working.

Procedure

» Do one of the following:

- On the phone, go to **Settings** > **Status** > **Diagnostics** > **Warnings**.
- From the Web Configuration Utility, go to **Diagnostics** > **Skype for Business Status** > **Exchange Client**.

Configuring the Microsoft Exchange Server

You can configure the following settings to take advantage of Microsoft Exchange services on your phones.

Note: For help with Lync Server 2010, refer to Microsoft Configure Exchange Services for the Autodiscover Service.

For help with Lync Server 2013, refer to Microsoft Configuring Unified Messaging on Microsoft Exchange Server to work with Lync Server 2013.

Visual Voicemail

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

If you disable `feature.exchangeVoiceMail.enabled`, the Message Center and Skype for Business Voice mail menus display the message: Skype for Business Server only plays voicemail and you cannot download voicemails or play locally on the phone.

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.

Address Book Service (ABS) Adaptive Search

You can enable the ABS service on the Exchange server.

There are three possible configurations.

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

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

Microsoft Exchange Parameters

The following parameters configure Microsoft Exchange integration.

exchange.meeting.alert.followOfficeHours

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

0 - Disable audible calendar alerts.

exchange.meeting.alert.tonePattern

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

exchange.meeting.alert.toneVolume

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

0 - 17

exchange.meeting.allowScrollingToPast

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

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

exchange.meeting.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 and "|" separates alternative patterns (for example, xxx-xxx-xxxx|604.xxx.xxxx).

exchange.meeting.realConnectProcessing.outboundRegistration

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

2 (default)

1 - 34

Change causes system to restart or reboot.

exchange.meeting.realConnectProcessing.prefix.domain

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

exchange.meeting.realConnectProcessing.prefix.value

Define the One-Touch Dial meeting invite prefix value.

exchange.meeting.realConnectProcessing.skype.enabled

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

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

Change causes system to restart or reboot.

exchange.meeting.reminderEnabled

1 (default) - Meeting reminders are enabled.

0 - Meeting reminders are disabled.

exchange.meeting.reminderInterval

300 seconds (default)

60 - 900 seconds

Set the interval at which phones display reminder messages.

exchange.meeting.reminderSound.enabled

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

0 - The phone does not make an alert sound when users receives 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 seconds, 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.`

Lync Base Profile default is 1.

Generic Base Profile default is 0.

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

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

feature.exchangeCalendar.enabled

Available for:

- VVX 300/301, 310/311, 400/401, 410/411, 500/501, 600/601 and 1500 business media phones
- VVX 250, 350, and 450 business IP phones
- CX5500 Unified Conference Station

Lync Base Profile default is 1.

Generic Base Profile default is 0.

0 - The calendaring feature is disabled.

1 - The calendaring feature is enabled.

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

feature.exchangeContacts.enabled

Lync Base Profile default is 1.

Generic Base Profile default is 0.

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

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

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

feature.exchangeVoiceMail.enabled

Lync Base Profile default is 1.

Generic Base Profile default is 0.

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

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

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

feature.exchangeVoiceMail.skipPin.enabled

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

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

feature.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

Lync Base Profile default is 1.

Generic Base Profile default is 0.

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

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

feature.lync.abs.maxResult

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

12 (default)

5 - 50

feature.wad.enabled

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

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

0 - The phone uses DNS to locate the server FQDN and does not use Web auto-discovery. 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

Lync Base Profile default is 1.

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.

up.oneTouchVoiceMail1

Lync Base Profile default is 1.

Generic Base Profile default is 0.

0 - The phone displays a summary page with message counts. The user must press the Connect soft key to dial the voicemail server.

1 - The phone dials voicemail services directly (if available on the call server) without displaying the voicemail summary.

Microsoft Exchange Calendar Using OAuth Support

Polycom UC software enables you to access the Microsoft Exchange calendar using the OAuth 2.0 service.

You must include the following parameters in the phone configuration file to access Microsoft Exchange calendar:

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

Microsoft Exchange Calendar using OAuth Support Parameters

Use the following parameters to access the Microsoft Exchange calendar.

`device.logincred.domain`

Authenticates user credentials.

String (maximum of 255 characters)

`device.logincred.user`

Authenticates the user name from the Exchange server.

String (maximum of 255 characters)

`device.logincred.password`

Authenticates the password from the Exchange server.

String (maximum of 255 characters)

Audio Features

Topics:

- [Polycom NoiseBlock](#)
- [Supported Audio Codecs](#)
- [Music on Hold](#)

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 details the supported audio codecs and priorities for Polycom phone models.

Note the following limitations when using the Opus codec:

- VVX 301, 311, 401, 411, 500, 501, 600, and 601 business media phones support a single Opus stream. Users can establish only one call at a time when using the Opus codec on these phones.
- VVX 250, 350, and 450 business IP phones support a single Opus stream. Users can establish only one call at a time when using the Opus codec on these phones.
- VVX 500 and 600 do not support video when using Opus.
- VVX 500 and 600 do not support local conferences when using Opus.
- Opus is not compatible with G.729 and iLBC. If you set Opus to the highest priority, G.729 and iLBC are not published; if you set G.729 and iLBC to the highest priority, Opus is not published.

Note: When you enable video on VVX 500/501 and 600/601 phones, the G.722.1C codec is disabled. Due to performance constraints, Polycom also recommends disabling the SILK and G.720 AB/ Opus codec when video is enabled on VVX 501 and 601 phones.

Audio Codec Priority

Phone	Supported Audio Codecs	Priority
VVX 201	G.711µ-law	6
	G.711a-law	7
	G.722	4
	G.729AB	8
	iLBC (13.33kbps, 15.2kbps)	0, 0
VVX 300/301, 310/311, 400/401, 410/411 VVX 250, 350, 450 * Note: VVX 301, 311, 401, 411 support a single Opus stream. VVX 300, 310, 400, 410 do not support Opus.	G.711µ-law	6
	G.711a-law	7
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.729AB	8
	iLBC (13.33kbps, 15.2kbps)	0, 0
	Opus*	0
	Siren 7	0
VVX 500/501, 600/601 • VVX 500 and 600 support a single Opus stream. • VVX 500 and 600 do not support both Opus and video.	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
	Siren 7	0

Phone	Supported Audio Codecs	Priority
VVX 1500	G.711 µ -law	6
	G.711a-law	7
	G.719 (64kbps)	0
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.722.1C (48kbps)	2
	G.729AB	8
	Siren14 (48kbps)	3
	iLBC (13.33kbps, 15.2kbps)	0, 0
SoundStructure VoIP Interface • SoundStructure VoIP Interface supports a single Opus stream. • SoundStructure VoIP Interface does not support both Opus and video.	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
	iLBC (13.33kbps, 15.2kbps)	0, 0
	Siren 7	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

Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
G.719	RFC 5404	32 Kbps	48 Kbps	48 Ksps	20 ms	20 KHz
		48 Kbps	64 Kbps			
		64 Kbps	80 Kbps			
G.711	RFC 1890	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
G.722[1]	RFC 3551	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
G.722.1	RFC 3047	24 Kbps	40 Kbps	16 Ksps	20 ms	7 KHz
		32 Kbps	48 Kbps			
G.722.1C	G7221C	24 Kbps	40 Kbps	32 Ksps	20 ms	14 KHz
		32 Kbps	48 Kbps			
		48 Kbps	64 Kbps			
G.729AB	RFC 1890	8 Kbps	24 Kbps	8 Ksps	20 ms	3.5 KHz
Opus	RFC 6716	8 - 24 Kbps	24 - 40 Kbps	8 Ksps	20 ms	3.5 KHz
				16 Ksps		7 KHz
Lin16	RFC 1890	128 Kbps	132 Kbps	8 Ksps	10 ms	3.5 KHz
		256 Kbps	260 Kbps	16 Ksps		7 KHz
		512 Kbps	516 Kbps	32 Ksps		14 KHz
		705.6 Kbps	709.6 Kbps	44.1 Ksps		20 KHz
		768 Kbps	772 Kbps	48 Ksps		22 KHz
Siren 7	SIREN7	16 Kbps	32 Kbps	16 Ksps	20 ms	7 KHz
		24 Kbps	40 Kbps			
		32 Kbps	48 Kbps			
Siren14	SIREN14	24 Kbps	40 Kbps	32 Ksps	20 ms	14 KHz
		32 Kbps	48 Kbps			
		48 Kbps	64 Kbps			
Siren22	SIREN22	32 Kbps	48 Kbps	48 Ksps	20 ms	22 KHz
		48 Kbps	64 Kbps			
		64 Kbps	80 Kbps			
iLBC	RFC 3951	13.33 Kbps	31.2 Kbps	8 Ksps	30 ms	3.5 KHz
		15.2 Kbps	24 Kbps		20 ms	

Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
SILK	SILK	Skype SILK	6 - 20 Kbps	36 Kbps	8 Ksps	3.5 KHz
			7 - 25 Kbps	41 Kbps	12 Ksps	5.2 KHz
			8 - 30 Kbps	46 Kbps	16 Ksps	7 KHz
			12 - 40 Kbps	56 Kbps	24 Ksps	11 KHz

[1] Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.

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

Audio Codec Parameters

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

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

- Permitted values to set audio codec priority are 1 - 27
- A value of 1 is the highest priority, 27 the lowest.
- If 0 or Null, the codec is disabled.
- A change to the default value does not cause a phone to restart or reboot

If a phone does not support a codec, the phone treats the value as 0, does not offer or accept calls using that codec, and continues to the codec next in priority. For example, using the default values, the VVX 310 doesn't support G.722.1C or G.719 and uses G.722.1 as the next highest-priority codec.

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

    5 (default)

voice.codecPref.G7221.32kbps

    0 (default)

voice.codecPref.G7221_C.48kbps

    2 (default)

voice.codecPref.G729_AB

    8 (default)

voice.codecPref.iLBC.13_33kbps

    0 (default)

voice.codecPref.iLBC.15_2kbps

    0 (default)

voice.codecPref.Lin16.8ksps

    0 (default)

voice.codecPref.Lin16.16ksps

    0 (default)

voice.codecPref.Lin16.32ksps

    0 (default)

voice.codecPref.Lin16.44_1ksps

0 (default)

`voice.codecPref.Lin16.48ksps`

0 (default)

`voice.codecPref.Siren7.16kbps`

0 (default)

`voice.codecPref.Siren7.24kbps`

0 (default)

`voice.codecPref.Siren7.32kbps`

0 (default)

`voice.codecPref.Siren14.24kbps`

0 (default)

`voice.codecPref.Siren14.32kbps`

0 (default)

`voice.codecPref.Siren14.48kbps`

0 (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

Polycom VVX 501 and 601 business media phones support the SILK audio codec.

However, Polycom recommends disabling the SILK codec due to performance constraints when video is enabled on VVX 501 and 601 business media phones.

SILK Audio Codec Parameters

Polycom VVX 501 and 601 business media phones support the SILK audio codec. Poly recommends disabling the SILK codec due to performance constraints when video is enabled.

Use the following parameters to configure the SILK audio codec.

`voice.codecPref.SILK.8ksps`

    Set the SILK audio codec preference for the supported codec sample rates.

    0 (default)

`voice.codecPref.SILK.12ksps`

    Set the SILK audio codec preference for the supported codec sample rates.

`voice.codecPref.SILK.16ksps`

    Set the SILK audio codec preference for the supported codec sample rates.

    0 (default)

`voice.codecPref.SILK.24ksps`

    Set the SILK audio codec preference for the supported codec sample rates.

    0 (default)

`voice.audioProfile.SILK.8ksps.encMaxAvgBitrateKbps`

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

    20 kbps (default)

    6 – 20 kbps

`voice.audioProfile.SILK.12ksps.encMaxAvgBitrateKbps`

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

25 kbps (default)

7 – 25 kbps

voice.audioProfile.SILK.16ksps.encMaxAvgBitrateKbps

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

40 kbps (default)

12 – 40 kbps

voice.audioProfile.SILK.encComplexity

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

2 (default)

0-2

voice.audioProfile.SILK.encDTXEnable

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

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

voice.audioProfile.SILK.encExpectedPktLossPercent

Set the SILK encoder expected network packet loss percentage.

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

0 (default)

0-100

voice.audioProfile.SILK.encInbandFECEnable

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

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

voice.audioProfile.SILK.MaxPTime

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

20 ms

voice.audioProfile.SILK.MinPTime

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

20 ms

voice.audioProfile.SILK.pTime

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

20 ms

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 Web Configuration Utility. 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 Web Configuration Utility.

Procedure
1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password (the default is `456`), and click **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 phoneperformance, 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`.

Message	Cause
Unsupported file format	The file you are uploading is not a supported file format.
Network is down	A network failure occurred during download.

Skype for Business Video Features

Topics:

After you set up phones on your network with the default configuration, you can make custom configurations to optimize video calling for your phones, if supported.

The following Polycom phones support transmission and reception of high quality video images in Skype for Business environments:

- Polycom EagleEye Mini with VVX 501 and VVX 601 business media phones

  VVX 501 and VVX 601 phones with a connected EagleEye Mini camera transmit video streams up to 1080p with a maximum bit rate of 4 Mbps for H.264 AVC calls. For SVC video calls, VVX 501 phones support Common Intermediate Format (CIF) 352 × 288 resolution and VVX 601 phones support 480 × 270 resolution.

When BToE is enabled and the video-enabled phone is paired to the Skype for Business client on your computer, the preference for transmitting and receiving video streams is given to Skype for Business client. The preference is given to the phones only when the phone unpairs with the Skype for Business client. You can place all Skype for Business related-calls from the phones as audio-only irrespective of the call mode selected on the phone. However, users can choose to enable video from the paired Skype for Business client.

Video and Camera Options

By default, at the start of a video call, the connected USB camera transmits an RTP encapsulated video stream with images captured from the local camera.

Users can stop and start video transmission by pressing the Video key, and then selecting the **Stop** or **Start** soft key.

You can use the parameters in the following sections to configure video transmission, the video and local camera view, and video camera options.

Video Quality Parameters

Use the following parameters to configure quality settings for video calls.

`video.quality`

   The optimal quality for video that is sent in a call or a conference.

motion (default) — For outgoing video that has motion or movement.

sharpness — For outgoing video that has little or no movement.

motion (default) — for VVX 500 and 600 series business media phones.

sharpness (default) — for VVX 1500 business media phone.

Note: If you don't select **motion**, moderate to heavy motion can cause the phone to drop some frames.

video.quality.content

motion (default) - For outgoing video that has motion or movement.

sharpness — For outgoing video that has little or no movement.

video.autoFullScreen

0 (default) — Video calls only use the full screen layout if it is explicitly selected by the user.

1 — Video calls use the full screen layout by default, such as when a video call is first created or when an audio call transitions to a video call

video.callRate

The default call rate (in Kbps) to use when initially negotiating bandwidth for a video call.

512 (default) - The overlay does not time out.

2048 (default for VVX 501/601)

128 – 2048

128 – 4096 for VVX 501/601

For VVX 501 and VVX 601 phones with a connected Polycom EagleEye Mini USB camera, the recommended call rate value is 4096 Kbps. Comparatively, 384 Kbps is the minimum value the phone accepts for audio and video calls when EagleEye Mini is connected.

video.forceRtcpVideoCodecControl

0 (default) — RTCP feedback messages depend on a successful SDP negotiation of a=rtcp-fb and are not used if that negotiation is missing.

1 — The phone is forced to send RTCP feedback messages to request fast I-frame updates along with SIP INFO messages for all video calls irrespective of a successful SDP negotiation of a=rtcp-fb.

For an account of all parameter dependencies when setting I-frame requests, refer to the section I-Frames.

video.maxCallRate

Sets the maximum call rate that the users can select. The value set on the phone cannot exceed this value. If **video.callRate** exceeds this value, this parameter overrides **video.callRate** and this value is used as the maximum.

768 (default)

2048 (default for VVX 501/601)

128 – 2048

128 – 4096 for VVX 501/601

Video and Camera Parameters

Use the following configuration parameters to configure the video and camera options for supported cameras.

video.camera.brightness

Sets the brightness level of the video stream. The value range is from 0 (dimmest) to 1000 (brightest).

NULL (default)

0 - 1000

video.camera.contrast

Sets the contrast level of the video stream for all supported USB cameras. The value range is from 0 (no contrast increase) to 3 (most contrast increase), and 4 (noise reduction contrast).

NULL (default)

0 - 1000

video.camera.flickerAvoidance

Sets the flicker avoidance for all supported USB cameras.

NULL (default)

0 - Flicker avoidance is automatic.

1 - 50hz AC power frequency flicker avoidance (Europe/Asia).

2 - 60hz AC power frequency flicker avoidance (North America).

video.camera.frameRate

Sets the target frame rate (frames per second) for all supported USB cameras. Values indicate a fixed frame rate from 5 (least smooth) to 30 (most smooth).

25 (default)

5 - 30

If `video.camera.frameRate` is set to a decimal number, the value 25 is used instead.

video.camera.saturation

Sets the saturation level of video captured by any supported USB camera.

NULL (default)

0 - 1000

video.camera.sharpness

Sets the sharpness level of video captured.

NULL (default)

0 - 1000

video.screenMode

Specify the view of the video window in normal viewing mode.

normal (default)

full

crop

video.screenModeFS

Specify the view of the video window in full screen viewing mode.

normal (default)

video.localCameraView.idleState

1 (default) – Enables camera idle self-view.

0 – Disables camera idle self-view.

Supported Video Codecs

See the following table for a summary of video codecs supported on VVX business media phones.

Video Codec Specifications

Algorithm	MIME Type	Frame Size	Bit Rate (kbps)	Frame Rate (fps)
H.261	H261/90000	Tx Frame size: CIF, QCIF, SQCIF RX Frame size: CIF, QCIF	64 to 768	5 to 30
H.263	H263/90000,H263-1998/90000	Tx Frame size:CIF, QCIF Rx Frame size:CIF, QCIF, SQCIF, QVGA, SVGA, SIF	64 to 768	5 to 30

Algorithm	MIME Type	Frame Size	Bit Rate (kbps)	Frame Rate (fps)
H.264	H264/90000	Tx Frame size:CIF, QCIF	64 to 768	5 to 30
		VVX 5xx and 6xx with a USB camera support sending 720p resolution for Tx Frame size		
		Rx Frame size:CIF, QCIF, SQCIF, QVGA, SVGA, SIF		

Toggling Between Audio-only or Audio-Video Calls

You can enable users to toggle between audio-only and audio-video calls.

When this feature is enabled on the video-enabled business media phones, a soft key displays to enable users to toggle calls between audio-only or audio-video. This feature also applies to audio and video conference calls in Skype for Business environments.

When the phone is registered, you can:

- Use **video.callMode.default** to begin calls as audio-video or audio only. By default, calls begin as audio-video. After a video call has ended, the phone returns to audio-only.

  If you set this parameter to audio, users can choose to add Video to the call.

- Use `feature.audioVideoToggle.enabled` to enable users to start video during an audio call.

  If the call is established as audio-only, then users can use the **Start Video** soft key to add video to the call. After the video call ends, the phone returns to audio-only.

- Use `audioVideoToggle.callMode.persistent` to maintain or reset the call mode set by users.

Audio-only or Audio-Video Call Parameters

The following parameters configure whether the phone starts a call with audio and video.

video.autoStartVideoTx

   1 (default) - Automatically begin video to the far side when you start a call.

   0 - Video to the far side does not begin.

   Note that when the phone Base Profile is set to Skype or Lync, the default is 1.

audioVideoToggle.callMode.persistent

   0 - Resets the call mode set by a user to the default.

   1 - Maintains the call mode set by a user.

feature.audioVideoToggle.enabled

   Applies to the video-enabled business media phones.

0 (default) - the audio/video toggle feature is disabled.

1 - the feature is enabled.

`video.callMode.default`

Allow the user to begin calls as audio-only or with video.

audio (default) - Calls begin with audio only and the Start Video soft key displays.

video - Calls begin with video.

Forward Error Correction

The phones support Forward Error Correction (FEC) DV0 and DV1 with Skype for Business Server 2015, Skype for Business 2015 client, and Lync 2013 environments for H.264 SVC. The scheme introduces recovery packets on the transmitter which recover lost video packets on the receiver.

FEC performance and quality improvements with this release may vary depending on network conditions.

Forward Error Correction Parameter

Use the following parameter to set values for forward error correction.

`video.codecPref.XulpFecUC`

Set the forward error correction (FEC) codec priority.

6 (default)

0 - 6

Simulcast Video

Phones registered to Skype for Business can simultaneously send a low resolution video stream (up to 180p) and a second higher-resolution video stream (up to 720p) to conference participants in a Skype for Business AVMCU meeting. Simulcast is enabled by default.

The following lists the supported video resolutions for Transmit (Tx) and Receive (Rx) in an AVMCU-based call:

- Transmit (Tx)
    - 1920X1080p
    - 1600X896p
    - 1280X720p
    - 1024X576p
    - 960X540p
    - 848X480p
    - 800X448p
    - 640X360p

- ◦ 480X270p
- ◦ 424X240p
- ◦ 320X180p
- Receive (Rx)
  - ◦ 424X240p

Skype for Business AVMCU-based video meetings are driven by endpoint requests to receive video, which is called a video source request (VSR). The VSR specifies the resolution (among other constraints) and the participant(s) whose video the endpoint would like to display. The requested resolution in Skype for Business client video calls is based on the size of the video window and new VSRs are sent when the size of the window changes.

Video Parameters

Use the following parameters to configure video features on video-capable phones.

video.allowWithSource

Restricts sending video codec negotiation in Session Description Protocol (SDP).

0 (default)

0 or 1

This parameter applies only to VVX 500/501 and VVX 600/601 business media phones.

video.enable

1 (default) - Enables video calling capabilities for outgoing and incoming calls.

0 - Disables video calling capabilities.

video.autoFullScreen

0 (default) - Video calls use the full screen layout, only if explicitly selected by the user.

1 - Video calls use the full screen layout by default.

video.conf.profile

Sets the video resolution to large window in all layouts.

540p (default)

1080p

720p

360p

240p

180p

video.dynamicControlMethod

0 (default)

1 - The first I-Frame request uses the method defined by
video.forceRtcpVideoCodecControl and subsequent requests alternate
between RTCP-FB and SIP INFO.

To set other methods for I-frame requests, refer the parameter
video.forceRtcpVideoCodecControl.

video.iFrame.delay

0 (default)

1 -10 seconds - Transmits an extra I-frame after the video starts.

You can configure the amount of delay from the start of video until the I-frame is sent up to 10
seconds.

Change causes system to restart or reboot.

video.iFrame.minPeriod

Time taken before sending a second I-frame in response to requests from the far end.

2 (default)

1 - 60

video.iFrame.onPacketLoss

0 (default)

1 - Transmits an I-frame to the far end when video RTP packet loss occurs.

video.iFrame.period.onBoard

Set the I-Frame interval used for the VC4 encoder.

180 (default)

300 maximum

Video Codec Preference Parameters

Use the following video codec parameters to specify video codec preferences.

You can specify video codec preferences for the VVX 500/501, 600/601, and 1500 phones. To disable
codecs, set the value to 0. A value of 1 indicates the codec is the most preferred and has highest priority.
The VVX 500/501 and 600/601 support H.263 and H.264 and do not support H.261 or H.263 1998.

video.codecPref.H261

Sets the H.261 payload type.

6 (default)

0 - 8

video.codecPref.H264

Sets the H.264 payload type.

4 (default)

0 - 8

video.codecPref.H263 1998

Sets the H.263 payload type.

5 (default)

0 - 8

video.codecPref.H263

5 (default)

0 - 8

video.codecPref.H264

4 (default)

0 - 8

video.codecPref.XH264UC

Sets the Microsoft H.264 UC video codec preference priority.

Generic - 0 (default)

Skype for Business - 1 (default)

video.codecPref.XUlpFecUC

Sets the forward error correction (FEC) codec priority.

Generic - 0 (default)

Skype for Business - 6 (default)

Video Profile Parameters

These settings include a group of low-level video codec parameters.

For most use cases, the default values are appropriate. does not recommend changing the default values unless specifically advised to do so.

video.profile.H261.annexD

1 (default) - Enables Annex D when negotiating video calls.

0 - Disables Annex D when negotiating video calls.

Change causes system to restart or reboot.

video.profile.H264.packetizationMode

Set to control H.264 encoding and decoding capabilities on supported VVX business media phones.

0 (default) - Supports Single NAL unit mode.

For Incoming calls:

- If the remote endpoint supports only Non-interleaved mode, the VVX business media phone rejects the video with m line 0.
- If the remote endpoint supports Single NAL Unit mode, then the VVX business media phone answers the incoming call with Single NAL mode.

For Outgoing calls:

- In all outgoing calls, the VVX business media phone sends packetization-mode=0 in the offer.

1 - Supports both Single NAL Unit mode and Non-Interleaved mode.

For Incoming calls:

- The VVX business media phone answers both the Single NAL Unit mode and Non-Interleaved mode.

For Outgoing calls:

- The VVX business media phones send packetization-mode=0 and packetization-mode=1 in the offer.

video.profile.H264.payloadType

Specifies the RTP payload format type for H264/90000 MIME type.

109 (default)

96 to 127

Change causes system to restart or reboot.

video.profile.H264.profileLevel

Specifies the highest profile level within the baseline profile supported in video calls.

1.3 (default)

1, 1b, 1.1, 1.2, 1.3, and 2

VVX 500/501 and VVX 600/601 phones support H.264 with a profile level of 2, and VVX 1500 phones support H.264 with a profile level of 1.3.

Change causes system to restart or reboot.

video.profile.H264.packetizationMode0.payloadType

Specifies the RTP payload format type for H264/90000 packetization Mode 0 MIME type.

109 (default)

96 to 127

Change causes system to restart or reboot.

Phone Display Features

Topics:

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
- Local and remote participants for Boss-Admin 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.

All VVX phones support this Skype for Business feature except the following:

- VVX 101 business media phones
- VVX 150 business IP phones

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

The following two parameters configure a time zone location description for their associated GMT offset:

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

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

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

Permitted Value	Time Zone Description
21	(GMT -4:00) Atlantic Time (Canada)
22	(GMT -4:00) San Juan
23	(GMT -4:00) Manaus,La Paz
24	(GMT -4:00) Asuncion,Cuiaba
25	(GMT -4:00) Georgetown
26	(GMT -3:30) Newfoundland
27	(GMT -3:00) Brasilia
28	(GMT -3:00) Buenos Aires
29	(GMT -3:00) Greenland
30	(GMT -3:00) Cayenne,Fortaleza
31	(GMT -3:00) Montevideo
32	(GMT -3:00) Salvador
33	(GMT -3:00) Santiago
34	(GMT -2:00) Mid-Atlantic
35	(GMT -1:00) Azores
36	(GMT -1:00) Cape Verde Islands
37	(GMT 0:00) Western Europe Time
38	(GMT 0:00) London,Lisbon
39	(GMT 0:00) Casablanca
40	(GMT 0:00) Dublin
41	(GMT 0:00) Edinburgh
42	(GMT 0:00) Monrovia
43	(GMT 0:00) Reykjavik
44	(GMT +1:00) Belgrade
45	(GMT +1:00) Bratislava
46	(GMT +1:00) Budapest
47	(GMT +1:00) Ljubljana
48	(GMT +1:00) Prague
49	(GMT +1:00) Sarajevo,Skopje
50	(GMT +1:00) Warsaw,Zagreb

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

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

Permitted Value	Time Zone Description
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 or expansion module's current screen.

Before you can take a screen capture, provide power and connect the expansion module to your phone and make sure the phone's web server is enabled.

Procedure

1. Add the parameter `up.screenCapture.enabled` to your configuration.
2. Set the value to **1** and save.
3. On the device, go to **Settings** > **Basic** > **Preferences** > **Screen Capture**.

   Note you must repeat step 3 each time the device restarts or reboots.
4. Locate and record the phone's IP address at **Status** > **Platform** > **Phone** > **IP Address**.
5. Set the phone to the screen you want to capture.
6. In a web browser address field, enter `https://<phoneIPaddress>/captureScreen` where `<phoneIPaddress>` is the IP address you obtained in step 5.

   The web browser displays an image showing the phone's current screen. You can save the image as a BMP or JPEG file.

Capture 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.value

> 0 (Default) - The Screen Capture feature is disabled.
>
> 1 - The Screen Capture feature is enabled.

Font Size Customization

Polycom UC Software enables you to customize font size on VVX 250, 350, and 450 business IP phones.

The following font size options are available:

- Normal
- Large

Note: This feature is only applicable for English (default) language.

Change the Font Size

You can customize the font size from the available options.

Procedure

1. Navigate to **Settings** > **Basic** > **Preferences** > **Font Size**.
2. Select a font size.
3. Select **Save**.

   A notification displays to reboot the phone to make the changes effective.
4. Select **Yes**.

Font Size Customization Parameters

Use the following parameters to customize font size on the phone interface.

device.font.size

> Normal (default) – Set font to the normal size.

Large – Set a large font size.

Change causes system to restart or reboot.

Port Usage

Topics:

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)

Configuring Security Options

Topics:

- [Accessing the Web Configuration Utility](#)
- [Securing Audio Using Master Key Identifier (MKI)](#)
- [Administrator and User Passwords](#)
- [Device Lock for Skype for Business](#)
- [Configuring Privacy Settings](#)

Poly UC Software enables you to optimize security settings, such as changing the passwords for the phone, enabling users to lock their phones, and blocking administrator functions from phone users.

Accessing the Web Configuration Utility

When the Base Profile of a phone is set to **Skype**, access to the Web Configuration Utility is disabled by default.

Administrators must enable access to a phone's Web Configuration Utility 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 Web Configuration Utility as an administrator.

On the SoundStructure VoIP Interface, you must enable the Web Configuration Utility using configuration files on a provisioning server before you set the Base Profile to Skype. If you do not enable the Web Configuration Utility before setting the Base Profile to Skype, the Web Configuration Utility will not be available and you will need to reset the SoundStructure VoIP Interface to factory default settings.

Related Links

Enable Access to the Web Configuration Utility From the Phone Menu

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

Procedure

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 Web Configuration Utility

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 Poly UC Software.

Use the following parameters to enable and configure the Web Configuration Utility.

device.sec.coreDumpEncryption.enabled

0 (default)

1

device.sec.coreDumpEncryption.enabled.set

0 (default)

1

httpd.cfg.enabled

Base Profile = Generic

1 (default) - The Web Configuration Utility is enabled.

0 - The Web Configuration Utility is disabled.

Base Profile = Skype, SkypeUSB

0 (default) - The Web Configuration Utility is disabled.

1 - The Web Configuration Utility is enabled.

httpd.cfg.secureTunnelRequired

1 (default) - Access to the Web Configuration Utility is allowed only over a secure tunnel (HTTPS) and non-secure (HTTP) is not allowed.

0 - Access to the Web Configuration Utility is allowed over both a secure tunnel (HTTPS) and non-secure (HTTP).

httpd.enabled

Base Profile = Generic

1 (default) - The web server is enabled.

0 - The web server is disabled.

Base Profile = Skype, SkypeUSB

0 (default) - The web server is disabled.

1 - The web server is enabled.

Securing Audio Using Master Key Identifier (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, the phones displays a message prompting you to change the default administrator password (456). Poly strongly recommends that you change the default password. This password is separate from the Skype for Business user Sign In password. The default administrator password enables administrators to access advanced settings menu on the phone menu and to log in to a phone's Web Configuration Utility as an administrator.

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

- The pop-up prompt when the phone first registers
- Phone menu
- System web interface (Web Configuration Utility)
- Use the parameter **reg.1.auth.password**

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

- Administrator password: 456
- User password: 123

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

Change the Default Administrator Password on the Phone

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

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

Procedure

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

Change the Default Passwords in the Web Configuration Utility

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

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

Procedure

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password (the default is `456`), and click **Submit**.
3. Select **Settings** > **Change Password**.
4. For the **Admin**, enter the **Old Password**, **New Password**, and re-enter to confirm the new password.
5. Select **Save**.
6. For the **User**, enter the **New Password** and re-enter to confirm the new password.
7. Select **Save**.

Administrator and User Password Parameters

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

sec.pwd.length.admin

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

1 (default)

0 -32

Change causes system to restart or reboot.

sec.pwd.length.user

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

2 (default)

0 -32

Change causes system to restart or reboot.

up.echoPasswordDigits

1 (default) The phone briefly displays password characters before being masked by an asterisk.

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

device.auth.localAdminPassword

Specify a local administrator password.

0 - 32 characters

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

device.auth.localAdminPassword.set

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

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

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.

Profile photos on the lock screen are supported on the following VVX phones: VVX 400, 500, and 600 series business media phones, and VVX 250, 350, and 450 business IP phones,

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 by using the following parameter.

Privacy Configuration Parameter

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.

Certificates

Topics:

-
-
-

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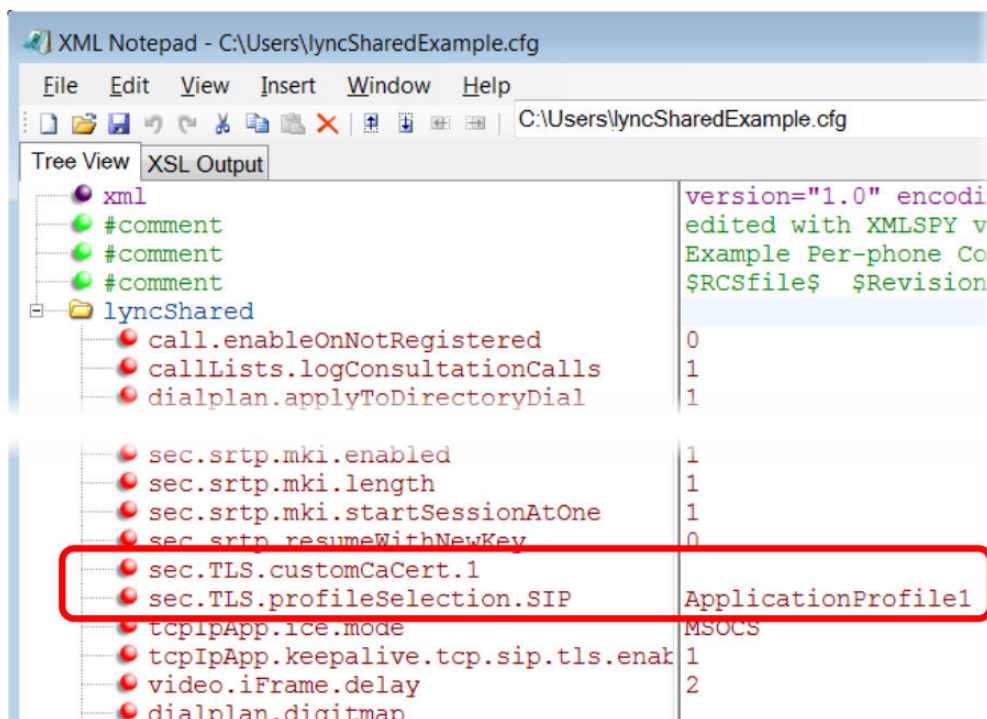
You can also enter the certificate by doing one of the following:

- 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.

Procedure

» Enter the root CA certificate, in Base64 format, in `sec.TLS.customCaCert.1` and set the application profile in `sec.TLS.profileSelection.SIP` .
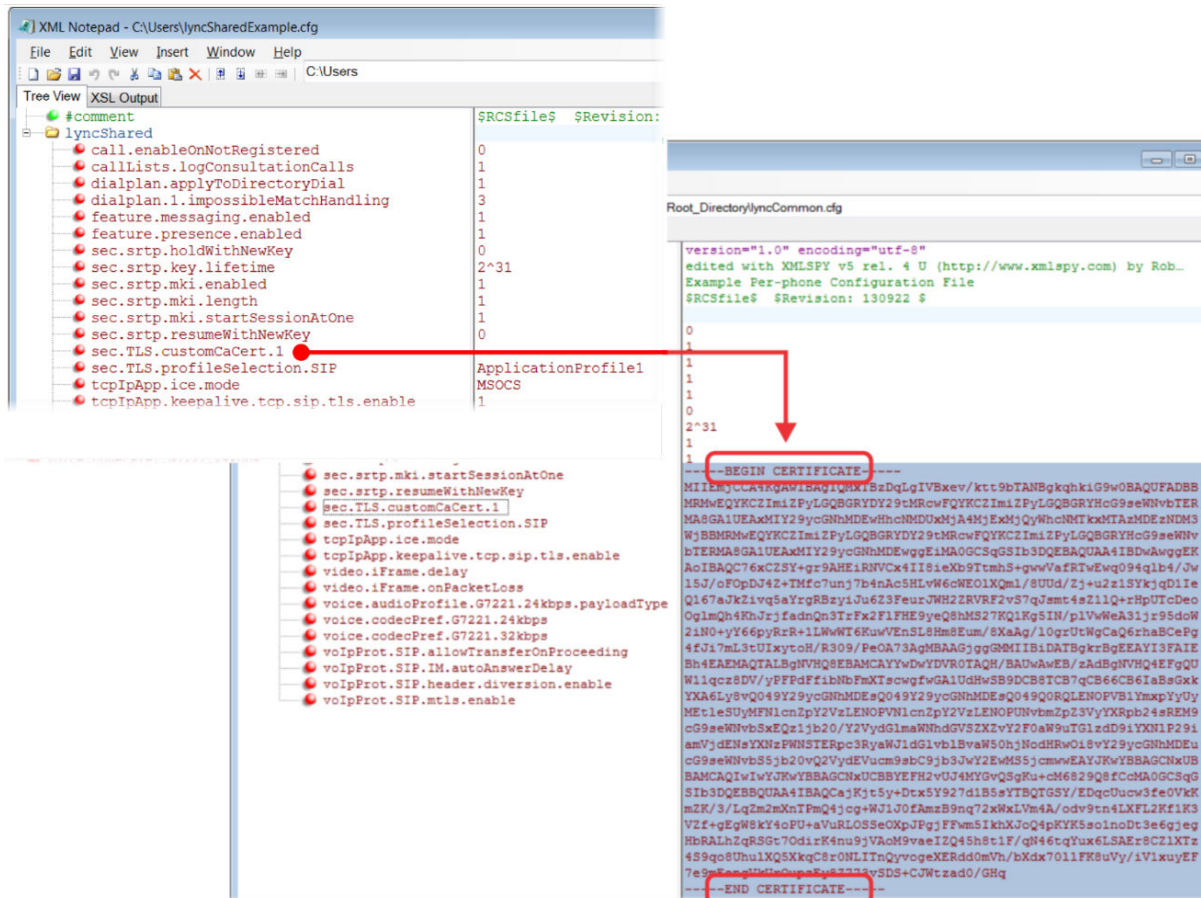
You have successfully installed a security certificate.

Manually Install a Certificate with the Web Configuration Utility

You can use the Web Configuration Utility to install a certificate manually.

Procedure

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password (the default is `456`), and click **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 will retrieve the information whether the certificate is valid or revoked.

Online Certificate Status Protocol Parameter

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

`device.sec.TLS.OCSP.enabled`

0 (default) OCSP is disabled.

1 – OCSP is enabled

Change causes system to restart or reboot.

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

Upload Logs to the Skype for Business Server

Topics:

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.

Procedure

>> Go to **Settings** > **Basic** > **Diagnostic Logs** > **Upload Logs**.

The files are uploaded to the server as plain text.

Send Diagnostic Logs from the Web Configuration Utility

To help troubleshoot issues, you can send diagnostic logs to the Skype for Business server from the Web Configuration Utility.

This option is available when logged in as Administrator or User.

Procedure

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.

Setting Log Levels

You can set log levels from the phone or Web Configuration Utility. By default, the phone sends log levels set on the server.

Set Log Levels from the Phone

You can set log levels from the phone.

Procedure

>> On the phone, go to **Settings** > **Basic** > **Diagnostic Logs** > **Server Log Level**.

Set Log Levels from the Web Configuration Utility

You can set log levels from the Web Configuration Utility.

Procedure

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.

Hardware and Accessories

Topics:

- [Manually Pairing with BToE](#)
- [TLS Feature Support for BToE](#)
- [Plantronics Headset Settings](#)

This section provides information on configuring Better Together over Ethernet (BToE), hardware pairing options, and supported accessories.

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.

Manual BToE Pairing is supported on the following VVX phones:

- VVX 400, 500, and 600 series business media phones
- VVX 250, 350, and 450 business IP phones

When you enable this feature users can select Auto or Manual pairing mode in the Web Configuration Utility 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.

To use the Manual Pairing feature, users must update to UC Software version supported to the corresponding BToE Connector application version.

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
UC Software version 5.8.0	BToE version 3.8.0	Yes	Yes
UC Software version 5.7.0	BToE version 3.7.0	Yes	Yes

Software Version	BToE Application Version	Manual Pairing	Automatic Pairing
UC Software version 5.5.1	BToE version 3.4.0	Yes	Yes
UC Software version 5.5.1	BToE version earlier to 3.4.0	No	Yes
UC Software version earlier to 5.5.1	BToE version 3.4.0	No	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.

Procedure
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 Web Configuration Utility

You can enable or disable the BToE PC Pairing feature from the Web Configuration Utility.

Procedure
1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password (the default is `456`), and click **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) to authenticate:

- 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.

Plantronics Headset Settings

Polycom UC Software enables you to configure Plantronics headset settings on VVX 401, 411, 501, 601 business media phones, VVX 250, 350, and 450 business IP phones. By default, this feature is disabled.

Plantronics Headset Settings Configuration Parameter

Use the following parameter to configure Plantronics headset settings.

`usb.headset.config.enabled`

1 – Enables the Plantronics headset configuration.

0 (default) - Disables the Plantronics headset configuration.

Directories and Contacts

Topics:

- [Unified Contact Store](#)
- [Configuring Contacts](#)
- [Call Lists](#)

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 parameters configure the Contact Directories.

up.queryContactInfo

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

0 (default)

1

Call Lists

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

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

The 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

Lync Base Profile – 0 (default)

Generic Base Profile – 1 (default)

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

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

callLists.logConsultationCalls

Lync Base Profile – 1 (default)

Generic Base Profile – 1 (default)

0 – Consultation calls not joined into a conference call are not listed as separate calls in the calls list.

1 – Each consultation calls is listed individually in the calls list.

feature.callList.enabled

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

0 - Disables all call lists.

feature.callListMissed.enabled

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

1 - The missed call list is enabled.

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

feature.callListPlaced.enabled

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

1 - The placed call list is enabled.

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

feature.callListReceived.enabled

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

1 - The received call list is enabled.

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

feature.exchangeCallLog.enabled

If Base Profile is:

Generic - 0 (default)

Skype for Business - 1 (default)

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

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

0 - The Exchange call list feature is disabled, the user call list history cannot be retrieved from the Exchange server, and the phone generates call lists locally.

Call Controls

Topics:

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.

When Call Forwarding is enabled on the Skype for Business server, you can override Microsoft settings from a provisioning server using the following parameters or from the Web Configuration Utility.

If call forwarding is disabled on the Microsoft server then call forwarding is also disabled 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 phone menu.

    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 soft key.

0 - The Forward soft key does not 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.

EFLK is not supported on VVX 201 business media phones.

Phones display registrations and contacts in the following order:

- Registration
- Enhanced Feature Key (EFK) as line key
- Shared Line Appearance (SLA) or Boss contacts
- 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 cannot use a sub-directory.

- The phone does not load the .csv file when checking the server for updates using check sync.

- The user cannot configure Speed Dials and Enhanced Feature Key (EFK) as line key.

- The previous FLK feature using `lineKey.reassignment.enabled` does not work with UC Software 5.4.1 or later on phones using a Skype for Business Base Profile. The later EFLK feature requires UC Software 5.4.1 or later.

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**.

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.

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.

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.

You can configure the phone allowing users to control the Skype for Business conference view during a video call. Users can set the conference view from **Conference Settings** menu.

Note: VVX 501 and 601 business media phones show the dominant speaker in the conference view.

Centralized Conference Control Protocol (CCCP) Parameters

The following parameters configure CCCP.

`video.CCCPView`

> Specify the conference view in a Skype for Business video enabled call.
>
> Normal (default)
>
> Roster
>
> By default, the view is set to Roster for audio only calls. The Normal view is not supported for audio only calls.

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.1.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.1.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.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.

Note also that 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.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.1.applyServerDigitMapLocally

Skype Base Profile: 1(default)

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.
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)

Hybrid Line Registration

The phones support Hybrid Line Registration that enables you to register a Skype for Business server on one line and an OpenSIP server on other lines.

You must register Skype for Business server on line 1 and other lines with any Open SIP server. You can configure and register a maximum of three different servers. You can also view the status of a hybrid line in the Web Configuration Utility.

Polycom VVX 101 business media phones and VVX 150 business IP phones do not support Hybrid Line Registration.

You cannot use the following features when you enable a phone for Hybrid Line Registration:

- Hot Desking
- Shared Line Appearance
- Busy Lamp field
- Automatic Call Distribution.

Note: When enabling Hybrid Line Registration, you must set the value for `call.stickyAutoLineSeize` and `call.enableOnNotRegistered` to 1.

Note:

When you enable Hybrid Line Registration, Skype for Business features change behavior in the following ways:

- When you enable Hybrid Line Registration on VVX phones, the H.323 protocol is not supported.

- When you enable the `up.oneTouchVoicemail` parameter, you can call voicemail services directly from the phone.

- **Do Not Disturb**

  The Do Not Disturb (DND) feature provides an **All** option. When the user selects **All**, DND is enabled on all registered lines. If only one line is registered, users can set DND directly by navigating to **Settings** > **Features** > **DND**. Server-based DND behaves the same way in hybrid registration mode.

- **Recent Calls**

  Users can view all the registered line's information and call logs for the corresponding registered line under the **Recent Calls** menu. However, when a Skype for Business user signs out of the phone, server-based call logs and the registered line's information for the Skype for Business server are not available.

- **Call Forwarding**

  Users can enable call forwarding per-line to forward an incoming call to a contact, voicemail, or delegates. Server-based call forwarding behaves the same way in hybrid registration mode.

- **Dial Plan**

  You can configure dial plans that enable the phone to select the line automatically for an outgoing call. Every line must have a unique dial plan. When a dial plan is not configured for a line, the value defined in the global parameter for a dial plan takes priority.

  Additionally, you can configure the line switching feature based on the dial plan when the phone is on-hook. The line switching feature enables the dialed number to switch to the corresponding line. For example, when you place a call from the phone and the number corresponds to an Open SIP line, the line switching feature enables the dialed number to switch to the corresponding line. Using the `reg.1.mergeServerDigitMapLocally` parameter, you can merge the dial plans received from the server with the dial plans configured for line 1 on your provisioning server. When a user dials a number directly from the call list or directory list, the value set in the corresponding parameter decides whether the dial plan must be parsed or not.

  You can also configure the dial plan for SIP URL dialing. For SIP URL dialing, the value defined in the per-registration dial plan parameter takes priority over the general dial plan parameter.

- **Conference Calls**

Hybrid Registration enables users to make Skype for Business and OpenSIP conference calls in parallel. Users can switch between OpenSIP and Skype for Business conference calls. However, you can't make conference calls between phones registered to Skype for Business and OpenSIP servers.

- **Securing Phone Calls with SRTP**

  When hybrid line registration is enabled, the Secure Real-Time Transport Protocol (SRTP) parameters for enable, require, and offer supports on per-line basis.

- **Enhanced 911**

  In hybrid registration mode, the Enhanced 911 service is supported only on the line registered with the Skype for Business server.

- **Presence Status**

  When hybrid line registration is enabled, users can set the presence status for the line registered to the Skype for Business server only. Users can view the device presence only on the line registered to the Skype for Business server.

- **Contact Directory**

  Users can access contact directories of all the registered lines. When user selects a contact from any directory and presses **Dial**, the call generates automatically based on the dial plan for the corresponding line without the need for the user to select the line. However, the home menu icon and presence status aren't available for the BroadSoft UC-One directory. You must set the `homeScreen.UCOne.enable` parameter value to 0.

- **Call Park**

  In hybrid registration mode, users can only park and unpark an active call to the corresponding registered line. For example, when an active call exists on a Skype for Business line and a user chooses to park the call, the call park applies only on the Skype for Business line.

- **Music on Hold**

  When a user places a call on hold using the registered line, the user hears only the call hold tone for the corresponding line. For example, when a Skype for Business call is put on hold, the user hears the Skype for Business hold tone.

- **Flexible Line Key**

  When the phone is in hybrid registration mode and the Flexible Line Key (FLK) feature is enabled, you can assign FLK to lines that are not hybrid line registered. However, when hybrid registration is enabled after FLK assignment, the feature replaces lines 2 and 3 configured with FLKs with hybrid registered lines.

Hybrid Line Registration Parameters

The following parameters configure Hybrid Line Registration.

reg.limit

Specify the maximum number of lines to use for registration.

1 (default)

1 to 3

For VVX 201 business media phones, the maximum number of lines to use for registration is limited to 2.

Change causes system to restart or reboot.

reg.1.mergeServerDigitMapLocally

0 (default) - Doesn't allow the dial plans from `dialplan.1.digitmap` to append on top of the dial plans received from the server.

1- Allows the dial plans from `dialplan.1.digitmap` to append on top of the dial plans received from the server.

dialplan.digitmap.lineSwitching.enable

0 (default) - Disables the line switching in dial plan to switch the call to the dial plan matched line.

1 - Enables the line switching in dial plan to switch the call to the dial plan matched line.

reg.1.urlDialing.enabled

0 (default) – Disables URL dialing.

1 – Enables URL dialing.

tcpIpApp.port.rtp.lync.audioPortRangeStart

Specifies the audio port range of start port for Lync/Skype for Business.

5350 (default)

1024 to 65436

tcpIpApp.port.rtp.lync.videoPortRangeStart

Specifies the video port range of start port for Lync/Skype for Business.

5406 (default)

1024 to 65486

tcpIpApp.port.rtp.lync.audioPortRangeEnd

Specifies the audio port range of end port for Lync/Skype for Business.

5402 (default)

1024 to 65485

tcpIpApp.port.rtp.lync.videoPortRangeEnd

Specifies the video port range of end port for Lync/Skype for Business.

5458 (default)

1024 to 65535

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)

1

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 accepts 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 200 contacts on the Skype for Business server.

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, ensure that the USB port is enabled.

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

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

This feature is available on the following devices:

- VVX 401, 411 business media phones
- VVX 5xx and 6xx series business media phones
- VVX 250, 350, and 450 business IP phones
- SoundStructure VoIP Interface

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.

Dial plans apply on-hook when no Skype for Business line is registered or when line switching is enabled and at least one line has a non-empty dial plan.

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

Note: For instructions on how to modify the local digit map, see *Technical Bulletin 11572: Changes to Local Digit Maps on SoundPoint IP, SoundStation IP, and Polycom VVX 1500 Phones* at Polycom Engineering Advisories and Technical Notifications.

Local Digit Maps Parameters

Use the following parameters to configure the local digit map.

dialplan.applyToCallListDial

> Choose whether the dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus.
>
> 1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToDirectoryDial

Lync Base Profile – 1 (default)

Generic Base Profile – 0 (default)

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

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

Change causes system to restart or reboot.

dialplan.applyToForward

Lync Base Profile – 1 (default)

Generic Base Profile – 0 (default)

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

1—The dial plan applies to forwarded calls.

Change causes system to restart or reboot.

dialplan.applyToTelUriDial

Choose whether the dial plan applies to URI dialing.

1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToUserDial

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

1 (default)

0

Change causes system to restart or reboot.

dialplan.applyToUserSend

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

1 (default)

0

Change causes system to restart or reboot.

dialplan.conflictMatchHandling

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

0 (default for Generic Profile)

1 (default for Skype Profile)

dialplan.digitmap.timeOut

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

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

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

Change causes system to restart or reboot.

dialplan.digitmap

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

Lync Base Profile (default) – NULL

```
[2-9]11|0T|+011xxx.T|0[2-9]xxxxxxxxx|+1[2-9]xxxxxxxx|[2-9]xxxxxxxxx|
[2-9]xxxT (default)
```

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

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

    1—Low precedence

    9—High precedence

Change causes system to restart or reboot.

dialplan.filterNonDigitUriUsers

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

0 (default)

1

Change causes system to restart or reboot.

dialplan.impossibleMatchHandling

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

1—The phone gives a reorder tone.

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

3 (default) (Skype for Business) — No digits are sent to the call server until the timeout is configured by `dialplan.impossibleMatchHandling.timeout` parameter.

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

Change causes system to restart or reboot.

dialplan.removeEndOfDial

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

1 (default)

0

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.x.description

Set the label or description for the emergency contact address.

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

string

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

Change causes system to restart or reboot.

dialplan.routing.emergency.x.server.y

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

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

positive integer

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

Change causes system to restart or reboot.

dialplan.routing.emergency.x.value

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

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

SIP URL (single entry)

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

dialplan.routing.server.x.address

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

Null (default)

IP address

hostname

Blind transfer for 911 or other emergency calls may not work if registration and emergency servers are different entities.

Change causes system to restart or reboot.

dialplan.routing.server.x.port

Set the port of a SIP server to use for routing calls.

5060 (default)

1 to 65535

Change causes system to restart or reboot.

`dialplan.routing.server.x.transport`

Set the DNS lookup of the first server to use and dialed if there is a conflict with other servers.

DNSnaptr (default)

TCPpreferred

UDPOnly

TLS

TCPOnly

For example, if `dialplan.routing.server.1.transport`= "UDPOnly" and `dialplan.routing.server.2.transport` = "TLS", then UDPOnly is used.

Change causes system to restart or reboot.

`dialplan.userDial.timeOut`

Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook.

Lync Base Profile (default) – 4

0-99 seconds

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

Open SIP Digit Map

If you are using a list of strings, each string in the list can be specified as a set of digits or timers, or as an expression which the gateway uses to find the shortest possible match.

In addition, the digit map feature allows SIP URI dialing to match the URIs based on dial plan.

The following is a list of digit map string rules for open SIP environments.

- The following letters are case sensitive: x, T, R, S, and H.
- You must use only *, #, +, or 0-9 between the second and third R.
- If a digit map does not comply, it is not included in the digit plan as a valid map. That is, no match is made.
- There is no limit to the number of R triplet sets in a digit map. However, a digit map that contains less than a full number of triplet sets (for example, a total of 2 Rs or 5 Rs) is considered an invalid digit map.
- Digit map extension letter R indicates that certain matched strings are replaced. Using an RRR syntax, you can replace the digits between the first two Rs with the digits between the last two Rs. For example, *R555R604R* would replace 555 with 604. Digit map timer letter T indicates a timer expiry. Digit map protocol letters S and H indicate the protocol to use when placing a call.
- If you use T in the left part of RRR's syntax, the digit map will not work. For example, R0TR322R will not work.

The following examples illustrate the semantics of the syntax:

- R9R604Rxxxxxxx-Replaces 9 with 604
- xxR601R600Rxx-When applied to 1160122 gives 1160022

- R9RRxxxxxxx-Remove 9 at the beginning of the dialed number (replace 9 with nothing)
  - For example, if you dial 914539400, the first 9 is removed when the call is placed.
- RR604Rxxxxxxx-Prepend 604 to all seven-digit numbers (replace nothing with 604)
  - For example, if you dial 4539400, 604 is added to the front of the number, so a call to 6044539400 is placed.
- xR60xR600Rxxxxxxx-Replace any 60x with 600 in the middle of the dialed number that matches.

  For example, if you dial 16092345678, a call is placed to 16002345678.
- 911xxx.T-A period (.) that matches an arbitrary number, including zero, of occurrences of the preceding construct. For example:
- 911123 with waiting time to comply with T is a match
- 9111234 with waiting time to comply with T is a match
- 91112345 with waiting time to comply with T is a match and the number can grow indefinitely given that pressing the next digit takes less than T.
- `sip\:764xxxxxRR@registrar.polycomcsn.comR` - appends `@registrar.polycomcsn.com` to any URI calls matching with "764xxxxx".

  For example, if you make a SIP URI call with 76412345 then `@registrar.polycomcsn.com` is appended to the string such that the SIP URI call INVITE becomes `sip::76412345@vc.polycom.com` . Here, `@domain` string is required only for SIP URI calls from unregistered lines.
- `sip\:xxxx\@registrar\.polycomcsn\.com` - This will match with any four digit URI calls having the domain `@registrar.polycomcsn.com` .

  For example, if you configure three lines and has dial plan based line switching enabled. Now, if the third line's dial plan has `sip\:xxxx\@registrar\.polycomcsn\.com` then call will be initiated from the third line if user dial `1234@registrar.polycomcsn.com` because it matches with the third line's dial plan.
- `0xxxS|33xxH` —All four digit numbers starting with a 0 are placed using the SIP protocol, whereas all four digit numbers starting with 33 are placed using the H.323 protocol.

Note: Only VVX 500/510, 600/611, and 1500 phones support the H. On all other phones, the H is ignored and users need to perform the Send operation to complete dialing. For example, if the digit map is 33xxH, the result is as follows: If a VVX 1500 user dials 3302 on an H.323 or dual protocol line, the call is placed after the user dials the last digit.

Generating Secondary Dial Tone with Digit Maps

You can regenerate a dial tone by adding a comma "," to the digit map.

You can dial seven-digit numbers after dialing "8" as shown next in the example rule `8,[2-9]xxxxxxT` :

`[2-9]11|0T|011xxx.T|[0-1][2-9]xxxxxxxxx|8,[2-9]xxxxxxT|[2-9]xx.T`

By adding the digit "8", the dial tone plays again, and users can complete the remaining seven-digit number. In this example, if users also have a 4-digit extension that begins with "8", then users will hear dial tone after the first "8" was dialed because "8" matches the "8" in the digit map.

If you want to generate dial tone without the need to send the "8", replace one string with another using the special character "R" as shown next in the rule *R8RR*. In the following example, replace "8" with an empty string to dial the seven-digit number:

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

International Dialing Prefix

Enter a plus (+) symbol before you dial an international phone numbers to identify to the switch that the phone number you are dialing is international.

International Dialing Prefix Parameters

The following parameters configure the international dialing prefixes.

call.internationalDialing.enabled

This parameter applies to all numeric dial pads on the phone, including for example, the contact directory.

Changes you make to this parameter cause a restart or reboot.

1 (default) - Disable the key tap timer that converts a double tap of the asterisk "*" symbol to the "+" symbol to indicate an international call. By default, this parameter is enabled so that a quick double tap of "*" converts immediately to "+". To enter a double asterisk "**", tap "*" once and wait for the key tap timer to expire to enter a second "*".

0 - When you disable this parameter, you cannot dial "+" and you must enter the international exit code of the country you are calling from to make international calls.

Change causes system to restart or reboot.

call.internationalPrefix.key

The phone supports international call prefix (+) with both "0" and "*".

0 (default) - Set the international prefix with "*".

1 - Set the international prefix with "0".

Enhanced 911 (E.911)

This E.911 feature allows you to configure one of three sources the phone obtains location information from:

- LLDP-MED
- DHCP via option 99
- LIS compliant with RFC 5985

Configuring the source of location information allows the phone to share its location details in the invite sent when a 911 call is made to ensure the 911 operator dispatches emergency services to the correct address.

Enhanced 911 (E.911) Parameters

Use the following parameters to configure E.911.

lync.E911.notificationUri.expansion.enabled

0 (default) - Disables expansion of distribution lists.

1 - Enables users to expand distribution lists received as part of the notification URI.

lync.E911.notificationUri.maxUrls

Set the limit for the number of URLs in the notification URI.

30 (default)

1 - 100

voIpProt.SIP.releaseOnSipFrag100Trying.enable

0 (default)

1 - DUT sends the BYE on SIPFrag100 trying NOTIFY.

Using the Phones as Shared Devices

Topics:

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`.

Polycom 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.

Procedure

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.

Procedure

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 master 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.

Guest Soft Key Customization

Poly UC Software enables you to rename the **Guest** soft key for idle and lock screens. You can move the position of the **Guest** soft key on the idle screen only.

To customize **Guest** soft key, you must set `feature.enhancedFeatureKeys.enabled` parameter to 1.

Guest Soft Key Customization Parameters

Use the following parameters to customize guest soft key.

softkey.x.label

The text displayed on the soft key label.

Null (default)

String

0 to 15

The maximum number of characters for this parameter value is 15. However, the maximum number of characters that a phone displays varies by phone model and by the width of the characters used.

Parameter values that exceed the phone's maximum display length are truncated by ellipses (…).

If string is labeled as "ospite" in italic, the guest key displays as "*ospite*" on both idle and lock screen.

It's recommended to use the optimal label length of 5 to 7 characters to avoid truncation.

softkey.x.insert

0 (default) - The phone places the soft key in the first available position after the default soft keys.

0 to 10 - The phone places the soft key in the corresponding position and moves the following soft keys by one position to the right.

For example, if you set the soft key to 3, the soft key is displayed in the third position from the left. If the soft key already exists in the third position, it moves to fourth position and the following soft keys move to right by one space.

softkey.x.action

Controls the action or function for the custom soft key x.

Null (default)

$THotDesk$

Macro action string, 2048 characters. This value uses the same macro action string syntax as an Enhanced Feature Key.

softkey.x.enable

0 (default) – Disables the soft key x.

1 – Enables the soft key x.

softkey.x.use.idle

0 (default) - Doesn't display the soft key x in designated position in the idle state.

1 - Displays the soft key x in designated position in the idle state.

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.

Note: Poly recommends that you do not enable Boss-Admin or Shared Line Appearance while CAP is enabled.

Use of CAP requires UC Software 5.7.0 or later. After you enable this feature using `feature.CAP.enable=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`
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`

Soft Key / Menu	CAP Mode Default	Parameters to Enable

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.

Procedure
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

You can sign out of a CAP-enabled phone using a code sent to the phone by the Common Area Provisioning Portal.

Procedure

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.enable`

   0 (default) - Disable Common Area Phone.

   1 - Enable Common Area Phone.

Configuring Shared Line Appearance (SLA) for Skype for Business

Shared Line Appearance (SLA) feature enables user to share a single line with other contacts as a member of a group.

Each shared line can receive only one incoming call at a time, and users cannot make outgoing calls from the shared line, including 911 emergency calls.

An incoming call to the shared line is received by all phones sharing the line. Any SLA group member can place, answer, hold, or resume calls on the line, and all group members can view the status of a call on the shared line on their phones.

This feature is not supported on VVX 201 business media phones.

SLA Limitations

The following features are not supported on SLA lines:

- BToE
- Conference class
- Call Park

SLA Configuration for Skype for Business

Administrators must install the Shared line Application on the Microsoft Front End server and configure SLA groups in Windows PowerShell.

Administrators can configure a ring tone type, and users can set a ring type from the phone's Basic Settings menu.

Shared Line Appearance (SLA) Parameters

Use the following parameters to configure SLA for Skype for Business.

`up.SLA.ringType`

Set the ring type for the share line so that users can distinguish between incoming calls to a private, primary line and the group SLA line. Note that users can set this ring type from the phone, which overrides the value you set here.

0 - 25

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. Both the Boss and Admin can sort shared Boss-Admin lines on the phone.

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.

Admins can be assigned up to an additional three Bosses, for a total of 18, by connecting an Expansion Module to the Admin delegate's 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.

Boss-Admin user instructions are available in the User Guide for your phone model on Polycom Voice Support.

Note: The Enhanced Boss-Admin feature is disabled by default.

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.
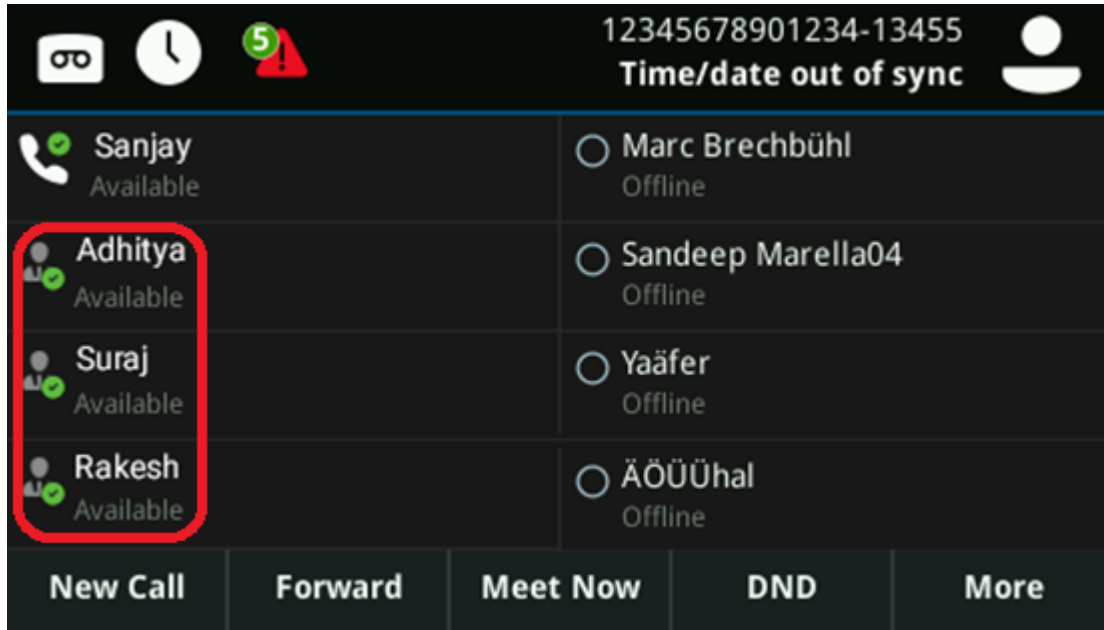
Boss-Admin Parameters

Use the following parameters to configure Boss-Admin.

up.numOfDisplayColumns

Specify the maximum number of columns displayed on VVX 500 and 600 series business media phones.

2 (default)

1 – 4

Note that the maximum number of columns supported on VVX 500 and 600 series business media phones are 3 and 4 respectively.

Change causes system to restart or reboot.

up.enhancedbossadmin

1 (default)- Enable Enhanced Boss-Admin.

0 - Disable Enhanced Boss-Admin.

Change causes system to restart or reboot.

Configure Boss-Admin with Lync Server 2010

If you are using Lync Server 2010, complete the following procedure.

Procedure

1. Add the following SQL write operation command to a row in a static SQL database table:

```
osql -E -S se.fabrikam.com\RTC -Q "use rtc;exec
RtcRegisterCategoryDef N'dialogInfo'"
```

   You need to substitute the path to the RTC presence back end, shown as <se.fabrikam.com> in this example.

   The SQL server operation is sent to the presence back end and must be run in every pool you need to enable.

2. Run the command.
3. Run the following command to verify that the category is registered

```
osql -E -S se.fabrikam.com\RTC -Q "use rtc;select * from CategoryDef"
```

   You must substitute the path to the RTC presence back end, shown as `<se.fabrikam.com>` in this example.

Network Configuration

Topics:

-
-
-
-

Poly UC Software enables you to make custom network configurations.

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 Polycom phones to locate the URL of a Proxy Auto-Configuration (PAC) file you configure.

Polycom VVX business media phones support WPAD beginning UC Software 5.7.0 and later.

WPAD is enabled by default. You can configure WPAD using configuration parameters on your provisioning server, DHCP Option 252, or 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.

The priority for PAC file searching is as follows, from first to last:

- 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://technet.microsoft.com/en-us/library/cc995090.aspx

- DNS-A. For instructions, see *Creating a WPAD entry in DNS* on Microsoft TechNet: https://technet.microsoft.com/en-us/library/cc995062.aspx

> **Note:** If the proxies you configure in the PAC file or configuration file are either invalid or unreachable with a working fallback proxy, the time to register with Skype for Business is delayed and the responsiveness of features that support WPAD degrade.

The phones also support Digest and NTLM Authentication mechanisms to authenticate with a proxy server. When you sign in to Skype for Business, the phone uses the Skype credentials to sign into the Web proxy. To manually configure proxy-specific credentials common to all users, use Basic Authentication which is supported only when you configure the following parameters on a provisioning server:

- `feature.wpad.proxy.username`
- `feature.wpad.proxy.password`

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:

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

Other

- HTTP/HTTPS Provisioning
- Core File Upload

View WPAD Diagnostic Information

You can confirm that the Web proxy server is successfully configured and operational, and access important WPAD diagnostic information to track HTTP and HTTPS traffic flowing via the proxy you configure for WPAD.

You can view the following diagnostic information on a pre-phone basis by logging into a phone's Web Configuration Utility.

- View if the WPAD PAC file fetch is successful
- View the configured method used to fetch the PAC file and source URLs
- View the DNS domain if configured
- View PAC file expiry details
- View the Exchange and Upload proxy
- Download the PAC file

Procedure

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password (the default is `456`), and click **Submit**.
3. Go to **Diagnostics** > **Skype for Business Status** > **WPAD**.

WPAD Configuration Parameters

The following parameters configure the Web Proxy Auto Discovery (WPAD) feature.

`feature.wpad.enabled`

Skype for Business Base Profile (default) - 1

Generic Base Profile (default) - 0

You can configure values for this parameter from your provisioning server or from the phone to enable to disable WPAD.

Change causes system to restart or reboot.

`feature.wpad.curl`

Enter the Proxy Auto-Configuration (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 do not discover DHCP or DNS-A or fetch the PAC file even if you configure a PAC file location using `feature.wpad.curl` .

0-255

You can specify multiple proxies using this parameter by separated each with a semicolon the same way you specify them in the PAC file. For example:

PROXY 0.10.1.1:8080;

PROXY 10.12.2.1:8080

Change causes system to restart or reboot.

feature.wpad.proxy.username

Enter the user name to authenticate with the proxy server.

0-255

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 do not need to configure user name or password credentials.

0-255

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 following phones support Data Center Resiliency:

- VVX 201, 300/310, 301/311, 400/410, 401/411, 500/501, and 600/601 business media phones
- VVX 250, 350, and 450 business IP phones
- SoundStructure VoIP Interface using Polycom UC Software 5.1.1 or later

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

This section lists parameters that configure the following Microsoft network features:

- Traversal Using Relays Around NAT (TURN)
- 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.MaxCandidateGatheringInParallel

The number of ICE candidates gathering threads run in parallel in the maximum time span of 2 seconds for simultaneous incoming calls only.

3 (default for VVX 201 business media phone)

5 (default for all other VVX platforms)

2 – 24

tcpIpApp.ice.MaxConnectivityChecksInParallel

The number of ICE connectivity checks threads that run in parallel in the maximum time span of 30 seconds (connectivity checks will be complete in 1 sec after answering call in general) for simultaneous incoming calls only.

The following lists the default value set when using a particular VVX phone model.

1 - 24

1 - VVX 150, 201, 300, 310, 400

5 - VVX 250, 350, 450

2 - VVX 410

7 - VVX 501, 601

3 - VVX 600

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.policy

Default<*VVXxxx*>, where <*xxx*> is the VVX phone model number.

For example, If you are using VVX 201 phone model, the value is set to DefaultVVX 201 by default.

Legacy - support the legacy behavior of ICE stack.

Custom - tune the following ICE parameters according to network conditions:

- tcpIpApp.ice.NetworkMode
- tcpIpApp.ice.MaxCandidateGatheringInParallel
- tcpIpApp.ice.MaxConnectivityChecksInParallel
- tcpIpApp.ice.ConnCheckInetvalPairs
- tcpIpApp.ice.ConnCheckInetvalRetries
- tcpIpApp.ice.ReflexiveChecksRequired
- tcpIpApp.ice.MaxRetries

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)

Skype for Business Device and Software Support

Topics:

- [Microsoft Quality of Experience Monitoring Server Protocol (MS-QoE)](#)
- [Quality of Service for Audio and Video Calls](#)
- [Updating Poly UC Software](#)

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.

MS-QoE is compatible with Skype for Business and Lync Server 2010 and 2013.

All parameters for enabling or disabling QoE are included in the in-band provisioning parameters sent from the Skype for Business server.

Note: Polycom 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](#).

Note that VVX phones use only the Audio port and range.

Set QoE Parameters on the Skype for Business Server

Set the following QoE parameters on the Skype for Business Server.

Procedure

» 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.

Figure 1: QoE Parameters on Server Media Configuration


```
PS C:\Users\administrator.COHOWINERY> Get-CsMediaConfiguration | fl


Identity                 : Global
EnableQoS                : True
EncryptionLevel          : RequireEncryption
EnableSiren              : False
MaxVideoRateAllowed      : UGA600K
EnableInCallQoS          : True
InCallQoSIntervalSeconds : 35
EnableRtpRtcpMultiplexing : True
```

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 Web Configuration Utility

Users and administrators can query the in-band QoE status, interval, and URI from a phone's Web Configuration Utility.

Procedure

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**.

Add Traceroute Data to QoE Reporting

You can include traceroute information in the quality of experience (QoE) data for metrics reporting that Poly phones using Skype for Business send at the end of a call.

To enable traceroute reporting, you must assign the policy to the user.

Procedure

1. Add the following commands to your management tool:

   - `$x = New-CsClientPolicyEntry -Name "EnableTraceRouteReporting" -Value "TRUE"`
   - `$y = Get-CsClientPolicy -Identity policyname`
   - `$y.PolicyEntry.Add($x)`
   - `Set-CsClientPolicy -Instance $y`

2. In the Skype for Business control panel, go to **Users** > **Search User**.
3. Select the user, double-click, and assign the **Client Policy** as **policyname**.
4. Select **Commit**.

   This feature is automatically implemented for the assigned user after registering for Skype for Business.

   Note: There is a possibility that the traceroute data isn't captured in the QoE report when the call duration is less than 60 seconds.

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
VQSessionReport	SessionId
	Endpoint
	DialogInfo
	MediaLine

Parent Element	Child Elements/Attributes
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

Parent Element	Child Elements/Attributes
LocalAddr, RemoteAddr, RelayAddr	IPAddr
	Port
	SubnetMask
	v2:MACAddr
Connectivity	Ice
	IceWarningFlags (Five flags supported)
	RelayAddress
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

Parent Element	Child Elements/Attributes
Payload.Audio	PayloadType
	PayloadDescription
	SampleRate
	v4:JitterBufferSizeAvg
	v4:JitterBufferSizeMax
	v4:JitterBufferSizeMin
	v4:NetworkJitterAvg
	v4:NetworkJitterMax
	v4:NetworkJitterMin
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

Quality of Service for Audio and Video Calls

When the Quality of Service (QoS) setting is enabled on the Skype for Business server, phones receive the Differentiated Services Code Point (DSCP) value from the server for Quality of Service (QoS) of audio calls placed or received from phones registered to the Skype for Business server.

The Skype for Business server does not provide in-band provisioning for DSCP for QoS of video calls for outbound video streams. When video is enabled on VVX 501 and VVX 601 phones, provision the phones to receive DSCP for QoS of audio calls using the parameter `qos.ip.rtp.dscp` and for video calls using `qos.ip.rtp.video.dscp`.

Note: If the parameter `lync.provisionDeviceParams.enabled` is set to 0 and DSCP is not set in the Web Configuration Utility, the phone marks IP packets with the DSCP value Expedited Forwarding (EF).

Related Links

QoS Parameters for Audio and Video Calls

Use the following parameters to configure DSCP for Quality of Service for audio and video calls.

`qos.ip.rtp.dscp`

Specify the DSCP of packets. If the value is set to the default NULL the phone uses `quality.ip.rtp.*` parameters.

If the value is not NULL, this parameter overrides `quality.ip.rtp.*` parameters.

- Null (default)
- 0 to 63
- EF
- Any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43

`qos.ip.rtp.video.dscp`

Allows you to specify the DSCP of packets.

If the value is set to the default NULL the phone uses `qos.ip.rtp.video.*` parameters.

If the value is not NULL, this parameter overrides `qos.ip.rtp.video.*` parameters.

- NULL (default)
- 0 to 63
- EF
- Any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43

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.

Procedure

1. Download and unzip UC Software to a directory on your provisioning server.
2. On the phone, go to **Settings** > **Advanced**, enter the 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 Web Configuration Utility.

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

Troubleshooting

Topics:

- [The phone fails to register](#)
- [I cannot sign in; I'm getting a sign in failure message](#)

Use the following section as a guide to resolving issues, problems, or common difficulties you may encounter while using Microsoft-enabled Polycom UC Software.

The phone fails to register

The most common issue with a failure to register is basic connectivity to the phone.

You can check basic connectivity in a number of ways:

- Obtain the host IP by looking at the phone registration status, configuration file, DNS, and Lync Computer Client Configuration Information Screen.
- Make sure the phone can communicate with the server by performing a diagnostic ping.
- From a computer connected on the same network as the phone, perform a telnet to the Lync server SIP TCP port 5061 or 443.
- Check for a DNS issue.
- Check if Lync Services is temporarily out of service, for example, a firewall or routing problem with the network.

Check that the phone is reading the configuration files. On the phone, go to Status > Platform > Configuration. The phone displays the current configuration and files. If the phone is not reading the correct configuration files, redo the provisioning procedures. If the phone is reading the configuration files, go to the next troubleshooting tip.

If the phone still cannot register, check autodiscover:

- Ensure the SRV Record exist and points to a valid A record.
- Ensure that the A record points to a valid host IP.
- Use the shell command `dnsCacheShow` to display a cached DNS entry. If an entry has a negative cache, the phone is trying to perform a lookup and is failing to resolve.

If you get a TLS error, you may have an untrusted, corrupted, or expired certificate. Check if a root CA is installed on the phone by going to Settings > Advanced > Administration Settings > TLS Security > Custom CA Certificate. If you need to troubleshoot TLS, use `log.level.change.tls=0` and l `og.level.change.sip=0` to log for TLS problems.

Check for invalid user credentials. Use `log.level.change.tls=0` , `log.level.change.sip=0` , and l `og.level.change.dns=0` to troubleshoot authentication failures.

Log into a computer Lync client with a user's credentials and ensure that the user account logs in. Use a simple password for testing purposes.

I cannot sign in; I'm getting a sign in failure message

PIN authentication can fail for several reasons, most commonly an invalid extension or invalid PIN.

When PIN authentication fails, a warning message displays:

Press Ok to open the PIN Authentication screen to sign in again. Any one of the following messages might display:

- Lync Sign In has failed System Administrator. This message indicates that something is wrong with the network. When you receive this message, speak to your administrator.

- Lync Sign In has failed Invalid login credentials. This message indicates that the user credentials you entered are incorrect. Try entering your credentials again and if sign in still fails, speak to your administrator.

- Lync Sign In has failed Please update Sign In Information. This message is rarely expected, and indicates a problem with the generation of certificate signing request (CSR) publishing the certificate.