



DEPLOYMENT GUIDE

| August 2021 | 3725-69579-001C

Poly Unified Communications for Cisco Webex

Getting Help

For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street
Santa Cruz, California
95060

© 2021 Plantronics, Inc. All rights reserved. Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.

Contents

Before You Begin.....	3
Audience, Purpose, and Required Skills.....	3
Related Poly and Partner Resources.....	3
Privacy Policy.....	4
 Poly Unified Communications for Cisco Webex Requirements.....	 5
Products Tested with this Release.....	5
Supported Deployment Models.....	6
 Registering RealPresence Group Series or Poly Trio with CUCM.....	 8
Configuring CUCM for Poly Endpoints TCP/Unsecure Registration.....	8
Create a Security Profile for TCP/Unsecure Registration.....	8
Add a System User for TCP/Unsecure Registration.....	10
Create a SIP Profile for TCP/Unsecure Registration.....	12
Add a Device Entry for TCP/Unsecure Registration.....	14
Configuring CUCM for Poly Endpoint TLS/Secure Registration.....	17
Create a Security Profile for TLS/Secure Registration.....	17
Add a System User for TLS/Secure Registration.....	18
Create a SIP Profile for TLS/Secure Registration.....	19
Add a Device Entry for TLS/Secure Registration.....	22
Configuring RealPresence Group Series for Secure CUCM Registration.....	24
Configure SIP Settings.....	25
Import CA Certificate to RealPresence Group Series or Immersive Telepresence System.....	26
Enable Encrypted Media Calls.....	28
Configuring a RealPresence Group Series for One Touch Dial Registration.....	29
Configuring a Poly Trio for CUCM Registration.....	29
Log In to the Web Configuration Utility.....	29
Configure Line Settings.....	30
Configure SIP Server Settings.....	30
Configure Date and Time Settings.....	31
Configuring a Poly Trio for Secure CUCM Registration.....	32
Configure SIP Line Settings.....	33
Generate Certificates for CUCM.....	34
Import Root CA and Signed Device Certificates.....	34
Configure Poly Trio Visual Plus Codec Priorities.....	36
Configure Poly Trio Visual Pro Codec Priorities.....	36

Configure a Poly Trio Dial Plan and One Touch Dial Service.....	37
---	----

Before You Begin

Topics:

- [Audience, Purpose, and Required Skills](#)
- [Related Poly and Partner Resources](#)
- [Privacy Policy](#)

This partner deployment guide explains how to integrate Poly products into Cisco Webex environments. It also centers around various Cisco and Poly call control infrastructures.

Poly's integrated suite of hardware devices and software applications allows you to integrate best of breed video and audio communications across Cisco platforms.

Audience, Purpose, and Required Skills

This guide is written for a technical audience. Poly expects the administrator to be a mid-level IT professional experienced in system administration.

The primary audience for this guide is administrators who configure, customize, manage, and troubleshoot video endpoints that are integrated with Poly Unified Communication for Cisco Webex. If configuring Microsoft calendars, the administrator should have Microsoft IT administrative expertise. The administrator should also be familiar with video conferencing concepts.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The [Poly Online Support Center](#) is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The [Poly 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 [Poly Community](#) provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The [Poly Partner Network](#) is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- The [Poly Services](#) help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy Policy

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

Poly Unified Communications for Cisco Webex Requirements

Topics:

- [Products Tested with this Release](#)

The Cisco Webex application enables users to join scheduled meetings by leveraging calendaring integration and use one click to join the meeting. It is available for endpoints that support calendaring. When the meeting time arrives, the user can select the meeting and, join the conference with just one click.

Products Tested with this Release

Polycom/Poly products are tested extensively with a wide range of products. You can view a list of the products that have been tested for compatibility with this release.

Poly strives to support any system that is standards-compliant and investigates reports of Polycom systems that are not interoperable with other vendor systems. Note that the following list is not a complete inventory of compatible equipment, but the products that have been tested with this release.

Note: Poly recommends that you upgrade all of your Polycom/Poly systems with the latest software versions. Any compatibility issues may already have been addressed by software updates. See [Poly Service Policies](#) for the Current Polycom Intraoperability Matrix.

Products Tested with this Release

Product	Tested Versions
Cisco Unified Communications Manager	11.5.1.14900
VCS-C/Expressway	X8.9.1
VCS-E/Expressway	X8.9.1
Polycom RealPresence DMA	9.0.1
Polycom RealPresence Access Director	4.2.5.2
Webex Web Client	N/A
Webex Teams Client	Unsupported
Cisco Webex Meetings Client	33.4.4.5 or higher
Polycom RealPresence Group Series	6.1.5 and higher
Poly Trio	5.7.2 and higher

Product	Tested Versions
Polycom Pano App	1.1 and higher

Endpoint	Registration	Firewall	Protocol	Audio	Video	Content	One Touch Dial
RealPresence Group Series	Cisco Unified Communications Manager	RealPresence DMA/ RealPresence Access Director	SIP	√	√	√	√
Poly Trio Visual+	Cisco Unified Communications Manager	RealPresence DMA/ RealPresence Access Director	SIP	√	√	√	√
Poly Trio Visual Pro	Cisco Unified Communications Manager	RealPresence DMA/ RealPresence Access Director	SIP	√	√	√	√
RealPresence Group Series	Cisco Unified Communications Manager	VCS-E	SIP	√	√	√	√
Poly Trio Visual+	Cisco Unified Communications Manager	VCS-E	SIP	√	√	√	√
Poly Trio Visual Pro	Cisco Unified Communications Manager	VCS-E	SIP	√	√	√	√
RealPresence Group Series	VCS-C	VCS-E	SIP and H.323	√	√	√	√
RealPresence Group Series	RealPresence DMA	RealPresence Access Director	SIP and H.323	√	√	√	√
Poly Trio Visual+	RealPresence DMA	RealPresence Access Director	SIP	√	√	√	√
Poly Trio Visual Pro	RealPresence DMA	RealPresence Access Director	SIP	√	√	√	√

Supported Deployment Models

You can deploy Poly products with Cisco Webex using different deployment models.

Poly supports the following deployment models when integrating Poly products with Cisco Webex environments:

- Direct Registration of Polycom RealPresence Systems with CUCM
- Direct Secure Registration of Polycom RealPresence Endpoints with VCS
- Direct Secure Registration of Polycom RealPresence Endpoints to RealPresence DMA

Registering RealPresence Group Series or Poly Trio with CUCM

Topics:

- [Configuring CUCM for Poly Endpoints TCP/Unsecure Registration](#)
- [Configuring CUCM for Poly Endpoint TLS/Secure Registration](#)
- [Configuring RealPresence Group Series for Secure CUCM Registration](#)
- [Configuring a RealPresence Group Series for One Touch Dial Registration](#)
- [Configuring a Poly Trio for CUCM Registration](#)
- [Configuring a Poly Trio for Secure CUCM Registration](#)
- [Configure Poly Trio Visual Plus Codec Priorities](#)
- [Configure Poly Trio Visual Pro Codec Priorities](#)
- [Configure a Poly Trio Dial Plan and One Touch Dial Service](#)

To register a RealPresence Group Series system with CUCM, you need to perform steps in both the CUCM and the RealPresence Group Series system.

For more information about the Cisco Unified Communications Manager, see the [Cisco Unified Communications Manager Documentation Guide](#). For more information on Polycom RealPresence Group Series, see the [Administrator's Guide](#).

Configuring CUCM for Poly Endpoints TCP/Unsecure Registration

Configure CUCM for Poly endpoint TCP/unsecure registration using the CUCM web administrator interface.

Before you configure CUCM, review the [Cisco Unified Communications Manager Considerations](#).

Create a Security Profile for TCP/Unsecure Registration

Enable the Phone Security Profile with digest authentication to secure the Poly endpoint's connection to CUCM.

Procedure

1. Log in to the CUCM console.
2. Select **System > Security Profile > Phone Security Profile**.
3. Select **Add New**.
4. In the **Phone Security Profile Type** drop-down menu, select **Third-party SIP Device (Advanced)** and click **Next**.

Phone Security Profile Configuration

Next

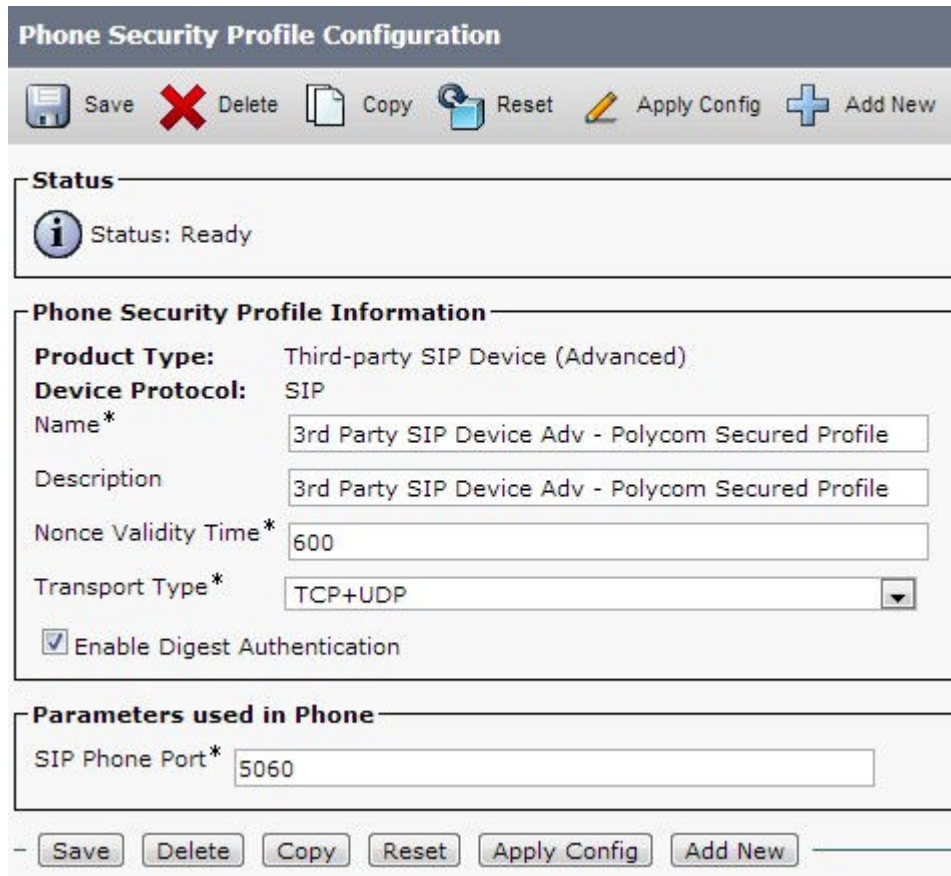
Status
 Status: Ready

Select the type of device profile you would like to create
 Phone Security Profile Type* Third-party SIP Device (Advanced) ▼

Next

*- indicates required item.

5. On the **Phone Security Profile Information** page, complete the following fields:
 - a. In the **Name** text box, enter a profile name for the system.
 - b. In the **Description** field, enter a description for the security profile.
 - c. If you want to use digest authentication (recommended), select the **Enable Digest Authentication** check box. Digest authentication requires valid login passwords to register devices.
 - d. Select the default values for all other fields. This example uses digest authentication.



Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Phone Security Profile Information

Product Type: Third-party SIP Device (Advanced)
Device Protocol: SIP
Name* 3rd Party SIP Device Adv - Polycom Secured Profile
Description 3rd Party SIP Device Adv - Polycom Secured Profile
Nonce Validity Time* 600
Transport Type* TCP+UDP
☒ Enable Digest Authentication

Parameters used in Phone

SIP Phone Port* 5060

Save Delete Copy Reset Apply Config Add New

6. Click **Save**.

In the status bar near the top of the page, **Update Successful** displays.

Add a System User for TCP/Unsecure Registration

Create a CUCM system user for each Poly endpoint.

Note: If you can't add a user, your system may be LDAP integrated. In that case, use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for each CUCM device.

Procedure

1. Select **User Management > End User**.
2. Click **Add New**.

The following screen displays. This example creates two users, one for the RealPresence Group Series integration and one for Poly Trio.

- User Information -	
User Status	Enabled Local User
User ID*	GS2
Password	
Confirm Password	
Self-Service User ID	
PIN	
Confirm PIN	
Last name*	GroupSeries2
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	English, United States ▼
Associated PC	
Digest Credentials	
Confirm Digest Credentials	
User Profile	Use System Default("Standard (Factory Default) U" ▼
User Rank*	1-Default User Rank ▼
User Status	Enabled Local User
User ID*	tptrio2
Password	
Confirm Password	
Self-Service User ID	
PIN	
Confirm PIN	
Last name*	Lastname

3. Complete the required fields (**User ID** and **Last Name**, at a minimum).
 - a. To use digest authentication, enter the **Digest Credentials** (password) for the Poly system. You configure this information in the Poly system in a later step.
 - b. In the **Confirm Digest Credentials** text box, enter the same value that you entered in step (a).

Note: The end user **Password** and **PIN** fields are arbitrary and aren't used for registration.

4. Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays.

Create a SIP Profile for TCP/Unsecure Registration

CUCM associates specific SIP parameters with an endpoint or trunk via a SIP Profile.

This configuration creates a SIP profile that is associated with all Poly devices.

Procedure

1. Select **Device > Device Settings > SIP Profile**.
2. Click **Find** to see the list of existing SIP Profiles, and select the **Standard SIP Profile** (a default in CUCM).
3. Once open, select **Copy**.
4. Change the Name to something meaningful for your deployment, and then ensure the following configuration:
 - a. Use **Fully Qualified Domain Name in SIP Requests** should be checked.
 - b. Allow **Presentation Sharing using BFCP** should be checked.
 - c. **Early Offer support for voice and video calls** should not be checked. This section shows the data as an example.

SIP Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name *	Polycom Standard SIP Profile
Description	Default SIP Profile + BFCP
Default MTP Telephony Event Payload Type *	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls *	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites *	TIAS and AS
User-Agent and Server header information *	Send Unified CM Version Information as User-

☐ Redirect by Application
☐ Disable Early Media on 180
☐ Outgoing T.38 INVITE include audio mline
☐ Enable ANAT
☐ Require SDP Inactive Exchange for Mid-Call Media Change
☒ Use Fully Qualified Domain Name in SIP Requests

Parameters used in Phone	
Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	5
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial
☒ Conference Join Enabled	
☐ RFC 2543 Hold	
☒ Semi Attended Transfer	
☐ Enable VAD	
☐ Stutter Message Waiting	

Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Never ▼
Resource Priority Namespace List	< None > ▼
SIP Rel1XX Options*	Disabled ▼
Video Call Traffic Class*	Mixed ▼
Calling Line Identification Presentation*	Default ▼
Session Refresh Method*	Invite ▼
Early Offer support for voice and video calls*	Disabled (Default value) ▼
☐ Enable ANAT ☐ Deliver Conference Bridge Identifier ☐ Allow Passthrough of Configured Line Device Caller Information ☐ Reject Anonymous Incoming Calls ☐ Reject Anonymous Outgoing Calls ☐ Send ILS Learned Destination Route String ☐ Connect Inbound Call before Playing Queuing Announcement	
SIP OPTIONS Ping	
☐ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	
Ping Interval for In-service and Partially In-service Trunks (seconds)*	60
Ping Interval for Out-of-service Trunks (seconds)*	120
Ping Retry Timer (milliseconds)*	500
Ping Retry Count*	6
SDP Information	
☐ Send send-receive SDP in mid-call INVITE ☒ Allow Presentation Sharing using BFCP ☐ Allow iX Application Media ☒ Allow multiple codecs in answer SDP	
Save Delete Copy Reset Apply Config Add New	

5. Click **Save**. In the status bar near the top of the page, an **Update Successful** message displays.

Add a Device Entry for TCP/Unsecure Registration

Create a CUCM device entry for each endpoint to allow the device to register properly with CUCM.

Procedure

1. Select **Device > Phone**.
2. Click **Add New**.
3. Select **Third-party SIP Device (Advanced)** and click **Next**.

Add a New Phone

 Next

Status

 Status: Ready

Create a phone using the phone type or a phone template

☒ Phone Type* Third-party SIP Device (Advanced) ▼

or

☐ BAT Phone Template* -- Not Selected -- ▼

 Next

4. Configure the following settings in the **Device Information** section.

- Device Information

☒ Device is Active

 Device is not trusted

MAC Address* 00E0DB43111C

Description PADGS2

Device Pool* Default ▼

Common Device Configuration < None > ▼

Phone Button Template* Third-party SIP Device (Advanced) ▼

Common Phone Profile* Standard Common Phone Profile ▼

Calling Search Space < None > ▼

AAR Calling Search Space < None > ▼

Media Resource Group List < None > ▼

Location* Hub_None ▼

AAR Group < None > ▼

Device Mobility Mode* Default ▼

Owner ☒ User ☐ Anonymous (Public/Shared Space)

Owner User ID* GS2 ▼

Mobility User ID < None > ▼

Use Trusted Relay Point* Default ▼

Always Use Prime Line* Default ▼

Always Use Prime Line for Voice Message* Default ▼

Geolocation < None > ▼

☒ Retry Video Call as Audio

☐ Ignore Presentation Indicators (internal calls only)

☒ Logged Into Hunt Group

☐ Remote Device

- a. In the **MAC Address** text box, enter a unique MAC Address for the RealPresence Group Series system. This can be any valid, unique MAC address. CUCM actually uses the RealPresence Group Series system user name to identify the RealPresence Group Series system.

Note: This field is arbitrary for third-party SIP Devices in CUCM, however Poly recommends configuring the actual MAC address of the RealPresence Group Series system to avoid conflicts.

- b. In the **Description** text box, enter a description (Optional).
 - c. From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.
 - d. From the **Phone Button Template** list, select **Third-party SIP Device (Advanced)**.
 - e. If your CUCM implementation uses partitions and Call Search Spaces, from the **Calling Search Space** list, select an appropriate calling search space for the RealPresence Group Series system (Optional).
 - f. If your CUCM implementation uses the CUCM Locations form of Call Admission Control (CAC), from the **Location** list, select an appropriate location for the RealPresence Group Series system. This location should contain video bandwidth. Before making this selection, see [Telepresence Deployment Design Considerations](#) and [Cisco Unified Communications Manager Considerations](#).
5. Configure the following settings in the **Protocol Specific Information** section.

Protocol Specific Information	
BLF Presence Group*	Standard Presence group ▼
MTP Preferred Originating Codec*	711ulaw ▼
Device Security Profile*	Third-party SIP Device Advanced - Standard SIP Ni ▼
Rerouting Calling Search Space	< None > ▼
SUBSCRIBE Calling Search Space	< None > ▼
SIP Profile*	Polycom Standard SIP Profile ▼
Digest User	GS2 ▼
☐ Media Termination Point Required ☐ Unattended Port ☐ Require DTMF Reception ☒ Allow Presentation Sharing using BFCP ☐ Allow iX Applicable Media	

- a. From the **Device Security Profile** list, select the profile created in “Create a Security Profile for TCP/Unsecure Registration.”
 - b. In the **Digest User** field, select a user created in “Add a System User for TCP/Unsecure Registration.”
 - c. From the **SIP Profile** list, select the profile created in “Add a SIP Profile for TCP/Unsecure Registration.”
 - d. Select **Allow Presentation Sharing using BFCP**.
6. Click **Save**.
- In the status near the top of the page, an **Update Successful** message displays.
7. In the **Association Information** section, click **Line [1] - Add a new DN** and complete the following required fields:

- a. In the **Directory Number** field, enter the phone's extension number.
- b. In the **Route Partition** field, choose the appropriate value for your CUCM deployment.

8. Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays.

9. Reset the Poly system in CUCM.
10. Follow the same steps to create a second third-party SIP Device (Advanced) for the Poly Trio. For example, TPTrio2.

Configuring CUCM for Poly Endpoint TLS/Secure Registration

Configure CUCM for Poly endpoint TLS/secure registration using the CUCM web administrator interface.

Before you configure CUCM, review the Cisco Unified Communications Manager Considerations.

Create a Security Profile for TLS/Secure Registration

You must create a security profile to use with your Poly endpoints. Each endpoint uses the same security profile, so you only need to create one.

If you want to create a secure profile, you can choose to enable digest authentication to secure the Poly endpoint's connection to CUCM.

Note: Poly recommends using digest authentication for Poly endpoint registration.

Procedure

1. Log in to the CUCM console.
2. Select **System > Security Profile > Phone Security Profile**.
3. Select **Add New**.
4. In the **Phone Security Profile Type** drop-down menu, select **Third-party AS-SIP Endpoint** and click **Next**.
5. On the **Phone Security Profile Information** page, complete the following fields:
 - a. In the **Name** text box, enter a profile name for the system.
 - b. In the **Description** field, enter a description for the security profile.

- c. Set the **Device Security Mode** to **Encrypted**.
- d. Set the **Transport Type** to **TLS**.
- e. Enable **Digest Authentication**.
- f. Set the **SIP Phone Port** to 5061.

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Phone Security Profile Information

Product Type: Third-party AS-SIP Endpoint
 Device Protocol: SIP
 Name*: thirdpartyAsSIP
 Description: thirdpartyAsSIP
 Nonce Validity Time*: 600
 Device Security Mode: Encrypted
 Transport Type*: TLS
☒ Enable Digest Authentication

Parameters used in Phone
 SIP Phone Port*: 5061

Save Delete Copy Reset Apply Config Add New

6. Click **Save** then **Apply Config**.

In the status bar near the top of the page, **Update Successful** displays.

Add a System User for TLS/Secure Registration

Create a CUCM system user for each Poly endpoint.

For each Generic Single/Multiple Screen Room System device added in CUCM, only a single system user is necessary when adding secure ITP systems.

Note: If you can't add a user, your system may be LDAP integrated. In that case, use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for each CUCM device.

Procedure

1. Select **User Management > End User**.
2. Click **Add New**.

The following screen displays.

User Information

User Status	Enabled Local User
User ID*	GS3
Password	
Confirm Password	
Self-Service User ID	
PIN	
Confirm PIN	
Last name*	GS3
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC	
Digest Credentials	
Confirm Digest Credentials	
User Profile	Use System Default("Standard (Factory Default) U" View Details
User Rank*	1-Default User Rank

3. Complete the required fields (**User ID** and **Last Name**, at a minimum).
 - a. To use digest authentication, enter the **Digest Credentials** (password) for the Poly system. You configure this information in the Poly system in a later step.
 - b. In the **Confirm Digest Credentials** text box, enter the same value that you entered in step (a).

Note: The end user **Password** and **PIN** fields are arbitrary and aren't used for registration.

4. Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays.

Create a SIP Profile for TLS/Secure Registration

CUCM associates specific SIP parameters with an endpoint or trunk via a SIP Profile.

This configuration creates an association with a SIP profile in CUCM and Poly devices.

Procedure

1. Select **Device > Device Settings > SIP Profile**.

2. Click **Find** to see the list of existing SIP Profiles, and select the **Standard SIP Profile** (a default in CUCM).
3. When the profile opens, select **Copy**.

Note: Leave the SIP settings at the default. However, consult a CUCM administrator for any SIP settings that may be specific to your deployment.

4. Change the **Name** to something meaningful for your deployment, then ensure the following configuration settings:
 - a. Ensure that the **Use Fully Qualified Domain Name in SIP Requests** check box is selected..
 - b. Ensure that the **Allow Presentation Sharing using BFCP** check box is selected.
 - c. Ensure that the **Early Offer support for voice and video calls** check box is NOT selected.

This following graphics show the data as an example.

SIP Profile Configuration

 Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Status

 Status: Ready

 All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name *	Polycom Standard SIP Profile
Description	Default SIP Profile + BFCP
Default MTP Telephony Event Payload Type *	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls *	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites *	TIAS and AS
User-Agent and Server header information *	Send Unified CM Version Information as User-

☐ Redirect by Application
☐ Disable Early Media on 180
☐ Outgoing T.38 INVITE include audio mline
☐ Enable ANAT
☐ Require SDP Inactive Exchange for Mid-Call Media Change
☒ Use Fully Qualified Domain Name in SIP Requests

Parameters used in Phone	
Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	5
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial
☒ Conference Join Enabled	
☐ RFC 2543 Hold	
☒ Semi Attended Transfer	
☐ Enable VAD	
☐ Stutter Message Waiting	

Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Never
RSVP Over SIP*	Local RSVP
Resource Priority Namespace List	< None >
☒ Fall back to local RSVP	
SIP Rel1XX Options*	Disabled
Video Call Traffic Class*	Mixed
Calling Line Identification Presentation*	Default
☐ Deliver Conference Bridge Identifier	
☐ Early Offer support for voice and video calls (insert MTP if needed)	
☐ Send send-receive SDP in mid-call INVITE	
☒ Allow Presentation Sharing using BFCP	
☐ Allow iX Application Media	
☐ Allow Passthrough of Configured Line Device Caller Information	
☐ Reject Anonymous Incoming Calls	
☐ Reject Anonymous Outgoing Calls	

- Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays.

Add a Device Entry for TLS/Secure Registration

Create a CUCM device entry for each endpoint. This configuration adds a device to CUCM, which in turn enables the device to securely register with CUCM.

To securely register a RealPresence Group Series or ITP system with CUCM, add a **Third-party AS-SIP Endpoint** device for single-screen systems and a **Generic Multiple Screen Room System (GMSRS)** for multi-screen systems.

Procedure

- Select **Device > Phone**.
- Click **Add New**.
- Select **Third party AS-SIP Endpoint** and click **Next**.

Add a New Phone

Next

Status

Status: Ready

Create a phone using the phone type or a phone template

☒ Phone Type*

Third-party AS-SIP Endpoint

or

☐ BAT Phone Template*

-- Not Selected --

Next

- Configure the following settings in the **Device Information** section.

- Device Information

☒ Device is Active	
Device Trust Mode*	Trusted
MAC Address*	00E0DB0E1B1A
Description	PADGS3
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Third-party AS-SIP Endpoint
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
Media Resource Group List	< None >
Location*	Hub_None
Device Mobility Mode*	Default
Owner	☒ User ☐ Anonymous (Public/Shared Space)
Owner User ID*	GS3
Mobility User ID	< None >
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Geolocation	< None >
☒ Retry Video Call as Audio	
☐ Ignore Presentation Indicators (internal calls only)	
☒ Logged Into Hunt Group	
☐ Remote Device	

- a. In the **MAC Address** text box, enter the unique MAC Address for the RealPresence Group Series system.
For secure registration, this must be the actual MAC Address of the RealPresence Group Series or ITP system.
 - b. In the **Description** text box, enter a description (Optional).
 - c. From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.
 - d. From the **Phone Button Template** list, select **Generic Single Screen Room System** or **Generic Multiple Screen Room System**.
 - e. If your CUCM implementation uses partitions and Call Search Spaces, from the Calling Search Space list, select an appropriate **calling search space** for the Poly system (Optional).
 - f. If your CUCM implementation uses the CUCM Locations form of Call Admission Control (CAC), from the **Location** list, select an appropriate location for the RealPresence Group Series system. This location should contain video bandwidth. Before making this selection, see Telepresence Deployment Design Considerations and Cisco Unified Communications Manager Considerations.
5. Configure the following settings in the **Protocol Specific Information** section.

Protocol Specific Information	
Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	thirdpartyAsSIP
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
Digest User	GS3
☐ Media Termination Point Required ☐ Unattended Port ☐ Require DTMF Reception ☐ Early Offer support for voice and video calls (insert MTP if needed) ☒ Allow Presentation Sharing using BFCP	

- a. From the **Device Security Profile** list, select the profile created in “Create a Security Profile for TLS/Secure Registration.”
 - b. In the **Digest User** field, select the user created in “Add a System User for TLS/Secure Registration.”
 - c. From the SIP Profile list, select the profile created in “Add a SIP Profile for TLS/Secure Registration.”
 - d. Select **Allow Presentation Sharing using BFCP**.
 6. Click **Save**.
- In the status bar near the top of the page, an **Update Successful** message displays.
7. In the **Association Information** section, click **Line [1] - Add a new DN** and complete the following required fields:
 - a. In the **Directory Number** field, enter the phone’s extension number.
 - b. In the **Route Partition** field, choose the appropriate value for your CUCM deployment.

Directory Number Information	
Directory Number*	4565765
Route Partition	< None >
Description	
Alerting Name	padgs2
ASCII Alerting Name	padgs2

8. Click **Save** and **Apply Config**.

In the status bar near the top of the page, an **Update Successful** message displays.

Configuring RealPresence Group Series for Secure CUCM Registration

When you securely register a Poly endpoint with CUCM, the endpoint can make calls to Cisco endpoints. These CUCM registered endpoints can then make encrypted media calls.

Use the RealPresence Group Series web administrator interface to perform the following tasks:

- Configure SIP Settings
- Import Certificates to RealPresence Group Series or Immersive Telepresence Systems
- Enable Encrypted Media Calls

Configure SIP Settings

Configure the SIP settings to securely register a RealPresence Group Series or Immersive Telepresence system with CUCM.

For ITP systems, configure the center codec for secure registrations.

Procedure

1. Enter the Polycom RealPresence Group Series system IP address or host name in a web browser.
2. Go to **Admin Settings > Network > IP Network** and select **SIP**.
3. Configure the settings in the **SIP Settings** section of the **IP Network** screen.

SIP

Enable SIP: ☒

Enable AS-SIP: ☐

Registration Status: Registered

SIP Server Configuration: Specify

Transport Protocol: TLS

Force Connection Reuse: ☐

BFCP transport preference: Prefer UDP

Sign-in Address: 2255

User Name: GS3

Password:

Registrar Server: 10.46.81.101

Proxy Server: 10.46.81.101

Registrar Server Type: Unknown

Save

Setting	Description
Enable SIP	Select this check box to enable the Polycom system to receive and make SIP calls.
Registrar Server	Specify the IP address of the Cisco Unified Communications Manager. Use the Proxy Server if this field is blank.

Setting	Description
Proxy Server	Specify the IP address of the SIP proxy server. Use the Registrar Server if this field is blank. No use of Proxy Server if both fields left blank.
Transport Protocol	The SIP network determines the protocol in which your Polycom system operates. Select TLS for secure registration.
Sign-in Address	Specify the directory number allotted to this device in CUCM.
Domain User Name	This should match the user name created in Task2 of "Configuring CUCM for a Secure Polycom Immersive, Room, or Desktop System."
Password	When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP registrar server. If using Digest Authentication , select the check box for the password and set it to the Digest Credentials password used for the Cisco Unified Communications user created for this system.
Registrar Server Type	Specifies whether the SIP registrar server is a Lync Server. For Cisco environments, leave this check box unselected.

Import CA Certificate to RealPresence Group Series or Immersive Telepresence System

You must import a valid certificate for CUCM to securely register a RealPresence Group Series or Immersive Telepresence system.

To support the sRTP/TLS feature, Polycom endpoints support Cisco Unified Communications Manager X509v3 certificates in Privacy Enhanced Mail (PEM) format.

Procedure

1. Open a browser window and enter the RealPresence Group Series system IP address.
2. Go to **Admin Settings > General Settings > Security > Certificates > Certificate Options**.
3. Click **Create** for a **Signing Request Client**.

4. Fill out the following fields:
 - Type = Client
 - Hash Algorithm = sha-256
 - Common Name (CN) = This must be of the format "Polycom-SEP < MAC_Address >" where the MAC Address is the actual MAC of the RealPresence Group Series system or ITP endpoint (center codec for ITP systems).

5. Fill in the other fields as appropriate for your deployment and click **Create**.

Create Signing Request Client

Hash Algorithm: sha-256

Common Name (CN): SEP00E0DB0E1B1A

Organizational Unit (OU): MCP

Organization (O): PAD

City or Locality (L): Austin

State or Province (ST): TX

Country (C): United States

SAN: FQDN: LOONGROUP.pad.zone

SAN: Additional Name:

SAN: IPv4 Address: 10.46.25.180

SAN: IPv4 Address (DNS): 10.46.25.180

SAN: IPv6 Global Address:

SAN: IPv6 Site Local Address:

SAN: IPv6 Link Local Address:

Cancel Create

6. Generate the CSR, download this client CSR `client_csr.pem` file, and then reboot the RealPresence Group Series system or ITP center codec.

Certificate Options

Maximum Peer Certificate Chain Depth: 2

Always Validate Peer Certificates from Browser: ☐

Always Validate Peer Certificates From Server: ☐

Installed Certificates: No certificates are installed. [View and Add](#)

The certificate signing request was created successfully.

Signing Request Server: No Server Request Created [Create](#)

Signing Request Client: [Download Signing Request](#) [Create](#)

The CSR must have a valid Certification Authority (CA) trusted by CUCM to generate a certificate. This is outside the scope of this documentation.

7. Repeat [3](#) on page 26 to [6](#) on page 27 for **Signing Request Server**.
8. Once you sign the CSR and generate the actual Certificate, go to **Installed Certificates** and select **View and Add**.
9. Select **Browse** and choose the `certificate.pem` file.

▼ Certificate Options

Maximum Peer Certificate Chain Depth:

Always Validate Peer Certificates from Browser: ☐

Always Validate Peer Certificates From Server: ☐

Installed Certificates: 2 [View and Add](#)

Signing Request Server: [Download Signing Request](#) [Create](#)

Signing Request Client: [Download Signing Request](#) [Create](#)

[Save](#)

Once successfully added, it should show on the page. The following is an example:

▼ Certificate Options

Maximum Peer Certificate Chain Depth:

Always Validate Peer Certificates from Browser: ☐

Always Validate Peer Certificates From Server: ☐

ADD_CERTIFICATE [Browse](#)

Issued To:	Issued By:	Expiration Date:	Type:	Remove
SEP00E0DB0E1B1A	mcp-AD-DC01-CA	Apr 5 16:07:06 201...	server,client	Remove

[Close](#)

Signing Request Server: [Download Signing Request](#) [Create](#)

Signing Request Client: [Download Signing Request](#) [Create](#)

[Save](#)

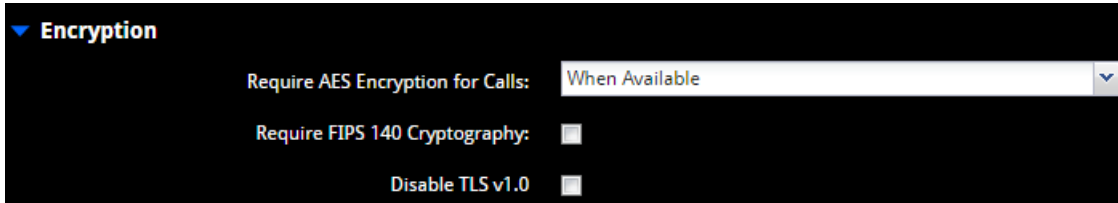
Enable Encrypted Media Calls

You can enable encrypted media calls on your RealPresence Group Series system.

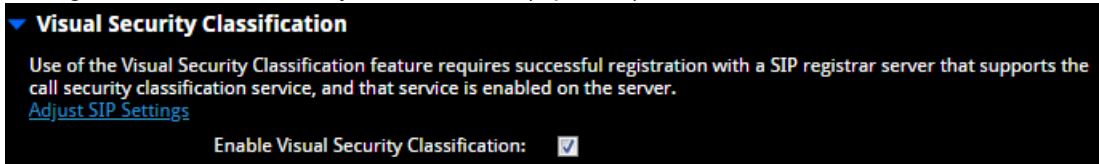
Procedure

1. Enter the Polycom RealPresence Group Series system IP address or host name in a browser window.
2. Go to **Admin Settings > Security Settings > Global Security > Encryption**.
3. **Note:** Set AES Encryption to **When Available** for successful secure registration.

Configure **AES Encryption** to either **When Available** or **Required for All Calls** as appropriate for your deployment.



4. Configure the Virtual Security Classification (Optional).



Configuring a RealPresence Group Series for One Touch Dial Registration

RealPresence Group Series requires registration to the Polycom One Touch Dial cloud. For more information, refer to [Poly One Touch Dial Service Help](#).

Configuring a Poly Trio for CUCM Registration

Use the Poly Web Configuration Utility to configure Poly Trio 8800 and register the system to the Cisco Unified Communications Manager (CUCM).

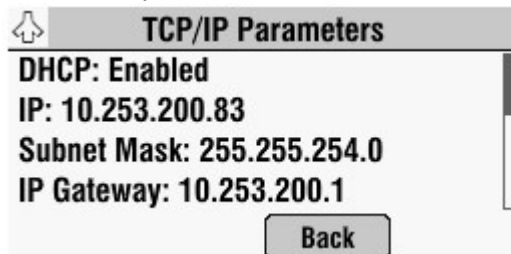
The Web Configuration Utility is a web interface application that is helpful when you're working remotely. You can use the Web Configuration Utility to provision one phone at a time.

Log In to the Web Configuration Utility

You must log in as an administrator to use the Web Configuration Utility.

Procedure

1. Go to **Menu > Status > Network > TCP/IP Parameters > IP** to obtain the IP address of your conference phone.



2. Enter the IP address in a web browser on a computer connected to the same network as the conference phone.
3. Log in to the Web Configuration Utility as an Administrator using the following credentials:
 - User ID: xyz@abc.com

- Password: 456

4. Click **Submit**.

Configure Line Settings

Configure the line settings for your phone using the Web Configuration Utility.

Procedure

1. Go to **Settings > Lines**.
2. Select the line you want to configure and expand the **Identification** menu.
Line 1 is selected by default.
3. Complete the following fields:

Line 1

Identification	
Display Name	2223
Address	2223
Label	CUCM
Type	☒ Private ☐ Shared
Third Party Name	CUCM
Number of Line Keys	1
Calls Per Line	24
Enable SRTP	☒ Yes ☐ No
Offer SRTP	☒ Yes ☐ No
Require SRTP	☐ Yes ☒ No
Server Auto Discovery	☐ Enable ☒ Disable
TCP Fast Failover	☒ Enable ☐ Disable
Authentication	
Use Login Credentials	☐ Enable ☒ Disable
Domain	
User ID	tptrio2
Password	

- Enter the **Display Name**. This example shows 2223.
- Enter the **Address**. This example shows 2223 to match the **Display Name**. **Address** represents the extension created for the device in CUCM.
- Enter the **Authentication User ID**. This example uses tptrio2.
- Enter the **Authentication Password**. This is the same value you entered in the **Digest Credentials** field when configuring digital credentials for the phone in CUCM.
- Enter the **Label** that displays on the phone. This example uses CUCM, but you could change the label to the line number, for example.

Configure SIP Server Settings

Configure the SIP server settings using the Web Configuration Utility.

Procedure

1. In the **Outbound Proxy** section, configure the following settings:
 - In the **Address** field, enter the IP address or hostname of the Cisco Unified Communications Manager. In this example, the CUCM has an IP address of 10.46.81.10.
 - Set **Port** to 5060.
 - In the **Transport** drop-down menu, select **TCP**.
2. In the **SIP Server 1** section, configure the following settings:
 - In the **Address** field, enter the IP address or hostname of the Cisco Unified Communications Manager. In this example, the CUCM has an IP address of 10.46.81.10.
 - Set **Port** to the correct port number for your environment.
 - In the **Transport** drop-down menu, select **TCP**.
3. Click **Save** to apply the settings.

The screenshot shows two configuration sections. The top section, titled 'Outbound Proxy', has a black header with a minus icon. It contains three fields: 'Address' with the value '10.46.81.101', 'Port' with the value '5060', and 'Transport' with a dropdown menu showing 'TCPpreferred'. The bottom section, titled 'Server 1', also has a black header with a minus icon. It contains several fields: 'Special Interop' with a dropdown showing 'Standard', 'Address' with '10.46.81.101', 'Port' with '5060', 'Transport' with 'TCPpreferred', 'Expires (s)' with '3600', 'Subscription Expires (s)' with '3600', 'Register' with radio buttons for 'Yes' (selected) and 'No', 'Retry Timeout (ms)' with '500', 'Retry Maximum Count' with '20', 'Line Seize Timeout (s)' with '30', 'Re-Register on Failover' with radio buttons for 'Yes' (selected) and 'No', 'Fail Back Mode' with a dropdown showing 'duration', and 'Fail Back Timeout (s)' with '3600'.

4. When you successfully register on the SIP server, you see a solid phone icon
 - On a phone, a solid phone icon displays on the phone screen.
 - On the Poly Trio, a green circle with a check mark appears.

Configure Date and Time Settings

Configure the date and time settings using the Web Configuration Utility.

Procedure

1. Go to **Preferences > Date & Time**.

Date & Time

Display Format

Time Format: 12 AM/PM

Date Format: Monday, January 1

Time Synchronization

SNTP Server: north-america.pool.ntp.org

SNTP Resync Period (s): 86400

Time Zone: (GMT -8:00) Pacific Time (US & Canada)

Daylight Savings

Daylight Savings: ☒ Enable ☐ Disable

Fixed Day: ☐ Enable ☒ Disable

Start Date: Second Sunday March 02:00

End Date: First Sunday November 02:00

2. In the **Display Format** section, choose a **Time Format** and **Date Format** that you want the phone to display.
3. In the **Time Synchronization** section, choose an **SNTP server** in your region that the phone receives its time setting from and select a region in **Time Zone**.
4. In the **Daylight Savings** section, enable or disable **Daylight Savings** time changes.

When enabled, the phone's time settings automatically adjust to daylight savings time according to the settings you configure in **Fixed Day**, **Start Date**, and **End Date**.

Configuring a Poly Trio for Secure CUCM Registration

When you securely register a Polycom endpoint with CUCM, the endpoint can make calls to Cisco endpoints. These CUCM registered endpoints can then make encrypted media calls.

Note: If you register Microsoft Skype for Business on Line 1, TLS registration to CUCM gets support from Office365 and not an on-premises instance.

Use the Poly Trio web administrator interface to perform the following tasks:

- Configure SIP Line Settings
- Generate and Import Certificates to Poly Trio

Configure SIP Line Settings

Configure SIP settings to securely register a RealPresence Group Series or Immersive Telepresence system with CUCM.

For ITP systems, configure the center codec for secure registrations.

Procedure

1. Enter the Poly Trio IP address or host name into a browser window.
2. Go to **Settings > Lines** and select the appropriate line.
3. Configure the Poly Trio line settings in each of the following areas:

Identification

Settings	Description
Display Name	Arbitrary name value.
Address	This field must match the Line ID assigned to this device in CUCM.
Label	Arbitrary name value.
Enable SRTP	Select the check box.
Offer SRTP	Select the check box.
Require SRTP	Leave the check box unselected.
Server Auto Discover	Select the check box.
TCP Fast Failover	Leave the check box unselected.

Authentication

Settings	Description
Use Login Credentials	Set to Disabled .
Domain	No Value; leave blank.
User ID	Specify the User ID created in CUCM for this device.
Password	Specify the Digest Authentication password created in CUCM for this device.

Outbound Proxy

Settings	Description
Address	Specify the IP address of hostname of CUCM
Port	Set to 5061
Transport	Set to TLS

Server 1

Settings	Description
Special Interop	Select Standard .
Special Interop	Specify the IP address of hostname of CUCM .
Port	Set to 5061 .
Transport	Set to TLS .
Register	Select Yes .

Generate Certificates for CUCM

You must generate certificates for CUCM for secure registration with Poly Trio.

To support the SRTP/TLS feature, Poly endpoints support Cisco Unified Communications Manager X509v3 certificates.

Procedure

1. Open a browser window and enter the Poly Trio system IP address.
2. Go to **Settings > Advanced > Administrative Settings > Generate CSR**.
3. Click **Create** for a **Client Signing Request Client**.
4. Fill out the following fields:
 - **Common Name**
 - **Organization**
 - **Country Code**
 - **State**
5. Fill in the other fields as appropriate for your deployment and click **Generate**.

Once you create the CSR, the private key file and CSR are uploaded to the FTP server configured on the Poly Trio.

The CSR must have a valid Certification Authority (CA) trusted by CUCM to generate a certificate. This is outside the scope of this documentation.

Import Root CA and Signed Device Certificates

Once you sign the CSR and generate a certificate, you must upload the root CA and signed client certificates to a web server for download.

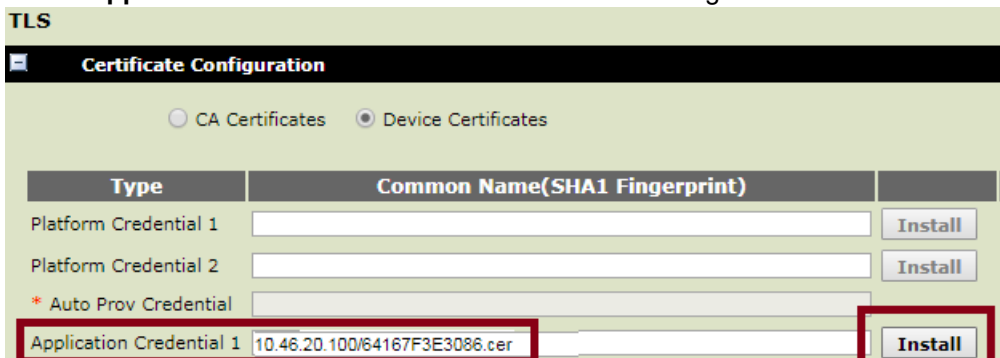
Procedure

1. Open a browser window and enter the Poly Trio system IP address.
2. Go to **Settings > Network > TLS** and select **CA Certificates option**.
3. Select **Application CA 1 > Install** and point to the **Root CA certificate URI**.
4. Select **Install**.

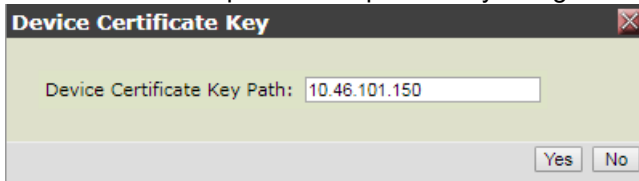
You receive a message box after the cert installation.



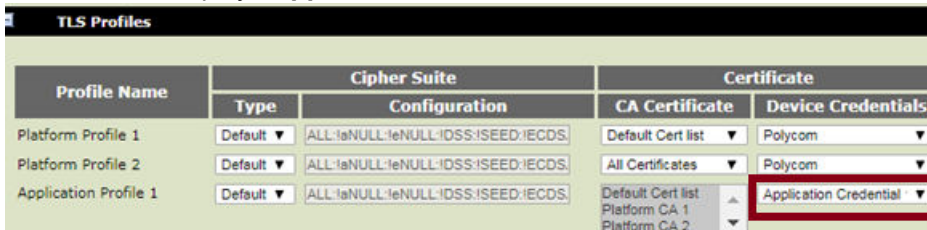
5. Select **Device Certificate** option at the top of the screen.
6. Select **Application Credential 1** and **Install**. Point to the signed client certificate.



7. Generate the next point to the private key along with the CSR on the FTP server.



8. Select **TLS Profiles > Application Profile 1**. Under **Certificate** column, ensure that the drop down list box displays **Application Credential**.



9. Select **TLS Applications > SIP**. Ensure that the **Profile Name** is **TLS Application Profile 1** and **Minimum TLS Version** is **TLS 1.2**.
10. Ensure that the MTLS SIP options are enabled.

Application	Profile Name	Minimum TLS Version
802.1x	TLS Platform Profile 1	TLS 1.0
Syslog	TLS Platform Profile 1	TLS 1.0
Provisioning	TLS Platform Profile 1	TLS 1.0
SIP	TLS Application Profile 1	TLS 1.2
Web Services	TLS Platform Profile 1	TLS 1.0
Presence	TLS Platform Profile 1	TLS 1.0
LDAP	TLS Platform Profile 1	TLS 1.0
SOPI	TLS Platform Profile 1	TLS 1.0
Web Server	Web Server Profile	TLS 1.0
Exchange Services	Exchange Service Profile	TLS 1.0

* Common Name Validation ☒ Provisioning ☐ SIP ☒ LDAP

MTLS SIP ☒ Enable ☐ Disable

* FIPS ☒ Enable ☐ Disable

Configure Poly Trio Visual Plus Codec Priorities

Configure the Poly Trio Visual Plus Codec Properties using the settings for Video Codec Priority.

Procedure

1. Go to **Settings > Codec Priorities > Video Codec Priority**.
2. Set the codec priority to the following order:

Unused:

In use:

- X-H264UC
- H.264 PacketizationMode0
- H.264 HP
- H.264 HP PacketizationMode0
- H.264
- H.263 1998
- H.263
- H.264

- X-H264UC
- H.264 PacketizationMode0
- H.264 HP
- H.264 HP PacketizationMode0
- H.264

Configure Poly Trio Visual Pro Codec Priorities

Configure the Poly Trio Visual Pro Codec Properties using the settings for Video Codec Priority.

Procedure

1. Go to **Settings > Codec Priorities > Video Codec Priority**.
2. Set the codec priority to the following order:
 - X-UlpFecUC
 - X-H264 UC
 - H-264
 - H-264 HP
 - H-264 PackatizationMode 0
 - H-264 HP PackatizationMode 0

Configure a Poly Trio Dial Plan and One Touch Dial Service

If CUCM on line 1 has Poly Trio registration, use or append this information to the Poly Trio configuration.

The parameters allow Poly Trio to provide a Join button for calendar invites and route calls to Webex through a correct line. There's also a mandatory config to disable Far End Camera Control. For more information, refer to the [Knowledge Base Article 35545](#).

The `dialplan.1.digitmap.mode` parameter is new to Poly Trio 5.7.2 and allows the use of regex for the dialplan.

Copy this info into a text file and save as a .cfg file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<UPLOAD>
<ALL
feature.fecc.enabled="0"
dialplan.applyToDirectoryDial="1"
dialplan.digitmap.lineSwitching.enable="1"
dialplan.1.digitmap.mode="regex"
dialplan.1.digitmap=".+@.+\.webex\.com"
exchange.meeting.parseAllowedSipUriDomains="webex.com"
exchange.meeting.parseEmailsAsSipUris="1"
exchange.meeting.parseOption="All"/>
</UPLOAD>
```

If CUCM on line 2 has Poly Trio registration, use or append this information to the Poly Trio configuration.

The parameters allow Poly Trio to provide a Join button for calendar invites and route calls to Webex through a correct line. The `dialplan.1.digitmap.mode` parameter is new to Poly Trio 5.7.2 and allows the use of regex for the dialplan.

Copy this info into a text file and save as a .cfg file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<UPLOAD>
<ALL
feature.fecc.enabled="0"
dialplan.applyToDirectoryDial="1"
dialplan.digitmap.lineSwitching.enable="1"
dialplan.2.applyToDirectoryDial="1"
dialplan.2.digitmap.mode="regex"
dialplan.2.digitmap=".+@.+\.webex\.com"
```

```
exchange.meeting.parseAllowedSipUriDomains="webex.com"  
exchange.meeting.parseEmailsAsSipUris="1"  
exchange.meeting.parseOption="All"/>  
</UPLOAD>
```