ADMINISTRATOR GUIDE

6.1.0 | February 2017 | 3725-61084-005B

Polycom® RealPresence Centro™ Administrator Guide

6001 America Center Drive
San Jose, CA 95002
USA

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at mailto:OpenSourceVideo@polycom.com (for video products) or mailto:OpenSourceVoice@polycom.com (for voice products).

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to mailto:DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin

Topics:

- Get Help

The *Polycom RealPresence Centro Administrator Guide* is for administrators who need to install system software, options, and accessories, and to configure, customize, manage, and troubleshoot Polycom® RealPresence Centro™ systems.

This guide provides concepts and general guidance to the system administrator. Polycom expects the administrator to be a mid-grade IT professional who is experienced in system administration.

Please read the Polycom system documentation before you install or operate the system. The following related documents for systems are available at Polycom Support:

- *Polycom RealPresence Centro Setup Sheet*: Describes the contents of your package, how to assemble the system and accessories, and how to connect the system to the network. The setup document is included in the system package.
- *Polycom RealPresence Centro Quick Tips*: Quick reference on how to use basic features
- *Polycom RealPresence Centro User Guide*: Describes how to perform video conferencing tasks in the system local interface
- *Polycom RealPresence Centro Regulatory Notices*: Describes safety and legal considerations for using Polycom RealPresence Centro systems
- *Polycom RealPresence Centro Room Preparation Guide*: Provides information on preparing a room before installing a RealPresence Centro system.
- *Polycom RealPresence Centro Release Notes*

Polycom recommends that you record the serial number and option key of your system here for future reference. The serial number for the system is printed on the unit.

System Serial Number: ____

Option Key: ____

Get Help

For more information about installing, configuring, and administering Polycom products, refer to **Documents and Downloads** at Polycom Support.

For support or service, please contact your Polycom distributor or go to Polycom Support at Polycom Support.

Polycom and Partner Resources

To find all Polycom partner solutions, see Strategic Global Partner Solutions.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

Getting Started

Topics:

High Definition Video Conferencing

The RealPresence Centro systems offer the following high-definition (HD) capabilities:

RealPresence Centro systems offer the following high-definition (HD) capabilities:

- Send people or content video to the far site in HD
- Receive and display video from the far site in HD
- Display near-site video in HD
- Full-motion HD

RealPresence Centro systems can support up to 1080p 60 fps video resolution, depending upon bandwidth and system setup. The system's camera supports up to 1080p 30 fps video resolution.

When the far site sends HD video, RealPresence Centro systems with HD capability and an HD monitor can display the video in wide-screen, HD format. RealPresence Centro systems with 1080 capability can receive 1080p progressive format and can display 1080p progressive or 1080i interlaced format.

Near-site video is displayed in HD format when you use an HD video source and an HD monitor. However, near-site video is displayed in SD if the system is in an SD or lower-resolution call.

To use HD for a multipoint call, keep the following requirements in mind:

- The call must be hosted by a system or a conferencing platform that supports HD such as Polycom RealPresence Collaboration Server 1500 or 2000.
- The system host must have the appropriate option keys installed.
- All systems in the call must support HD (720p at 30 fps) and H.264.
- The call rate must be high enough to support HD resolution.
- The call cannot be cascaded.

User Interface Customization

You can use the RealPresence Centro system web interface to configure how information is displayed for end users on the Home screen of the system local interface.

Home Screen Icons appear in the lower center of the system local interface, three at a time. By default, users see the icons shown in the following table in this location.

Icon	Name
🎥	Camera This icon takes you to the Camera Control screen.
📞	Place a Call This icon takes you to the Place a Call screen, where you can manually dial a call, or can select a contact name from a list.
◔☰	Content This icon appears only when a content source is detected.

Security Setting Management

To configure your RealPresence Centro system security settings using the system web interface, use a supported browser with cookies enabled. For a list of supported browsers and version numbers, refer to the *Polycom RealPresence Centro Release Notes.*

To access the system web interface, open a web browser and enter the IP address of the system using the https protocol; for example, use the format https://10.11.12.13.

Caution: The HTTPS protocol ensures that the configuration of all login information (such as user names and passwords) is transmitted using an encrypted channel, including those user names and passwords used to communicate with third-party systems on your network. Using HTTPS severely limits the ability of anyone on the network to discover these credentials. For this reason, all attempts to use the system web interface via HTTP are redirected to the HTTPS interface.

You can find security settings and passwords in the system web interface at **Admin Settings** > **Security**. Settings are under different sections of the security interfaces. In accordance with local laws and regulations, not all security settings are available in all countries.

Call Setting Configuration

The RealPresence Centro system call settings screen allows you to determine which settings are available to users when they place and answer calls in the system local interface.

Powering the System On and Off

After you have connected all of the equipment that you will use with the RealPresence Centro system, you can power on the system.

Power On the RealPresence Centro System

You can either use a remote control or press the power button on the system base.

Procedure

» Do one of the following:

- Press the green Select button on your remote control until the system responds.
- Press the power button. To expose the power button, you must first remove the corner from the base unit. For details on this procedure, refer to the *Polycom RealPresence Centro Setup Sheet* at Polycom Support. Press the power button and replace the corner.
- Note: Make sure that the system is powered off before you connect devices to it or before you unplug the power cable. Do not unplug the power cable when the system is powered on.

Automatic Wake With Motion Sensors

If the administrator has enabled a setting in the system web interface, when a person enters the room or comes near the RealPresence Centro system, it automatically wakes from power saving mode using motion sensors.

Procedure

1. In the system web interface, navigate to **Admin Settings > Audio/Video > Sleep**.
2. Select the **Enable Motion Sensor to Wake System** checkbox.

Navigating the System

You can navigate the RealPresence Centro system using the system web interface.

Log On

You can use the system web interface to perform most of the calling and configuration tasks you can perform on the local system. To log on to your system's web interface, you must open a web browser and enter the system's IP address.

Login credentials are user IDs and passwords that identify the user and define the user's ability to access the system. You can configure both local and remote access for users.

The system web interface supports the most commonly used web browsers. For a list of supported browsers, refer to the *Polycom RealPresence Centro Release Notes* at Polycom Support.

To configure your browser to use the system web interface, you must do the following:

- Use a supported web browser.
- Configure your browser to allow cookies.

Procedure

1. In your web browser address line, enter the system's IP address, for example, "http://10.11.12.13".
2. Enter the Admin ID as the user name (default is `admin`).
3. Enter the Admin Remote Access Password, if one is set.

Changing a Password

Polycom recommends that you change the default Admin ID and the default password for your RealPresence Centro system. Keep the following naming conventions in mind:

- The string “root” cannot be used as an ID.
- ID and password strings are not case sensitive.

Note: Make sure you can recall the admin password if you set one. If you forget the password, you must use the restore button to run the setup wizard again to access the **Admin Settings** in the system web interface and reset the password.

Search the Web Interface

In a text box just under the IP Address bar on the RealPresence Centro system web interface **Place a Call** screen, you can enter a search term to receive a list of system web screens. For instance, if you type `Call`, the system generates a list of screens that match your search term, such as **Call Settings**, **Recent Calls**, and **Time in Call**.

Procedure

1. In the **Search** box, type a text string.
2. Select any of the search results to go directly to that screen in the system web interface.

Setting Up System Hardware

Topics:

- Positioning the RealPresence Centro System
- Position the Polycom EagleEye Director II Camera System
- Setting Up Polycom EagleEye Acoustic Camera

The following topics provide information on how to set up and configure Polycom video systems and cameras.

Positioning the RealPresence Centro System

This manual provides information to supplement the setup sheets provided with your RealPresence Centro system and its elective peripherals. A printed copy of the setup sheet is provided with each system. PDF versions of the setup sheets are available at Polycom Support.

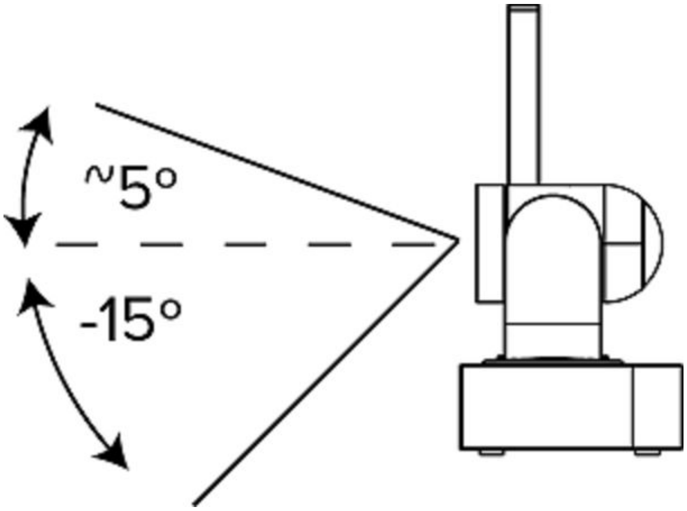
The RealPresence Centro system is designed to be placed in a dedicated room. If moving the system between rooms, consider removing the monitors to accommodate small doorways. Refer to the *Polycom RealPresence Centro Setup Sheet* before attempting to remove any monitors.

For information on how to set up your RealPresence Centro system, refer to the *Polycom RealPresence Centro Room Preparation Guide* at Polycom Support.

Position the Polycom EagleEye Director II Camera System

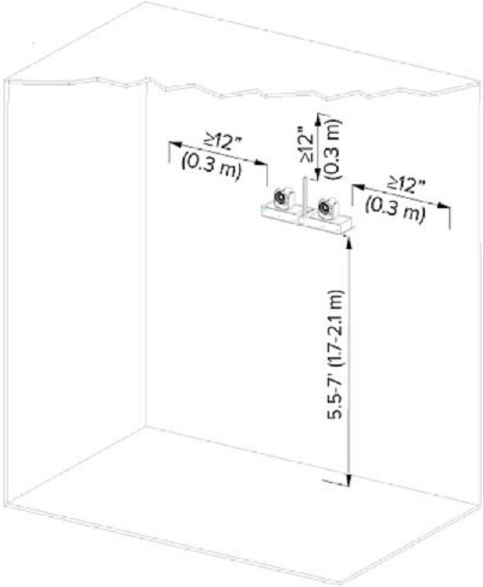
Follow these guidelines when you use the EagleEye Director II camera system with your RealPresence Centro system.

- Make sure the EagleEye Director II camera system is on a level surface or mounting bracket.
- The camera’s viewing angle is approximately 9 degrees above and 30 degrees below its direct line of sight as shown below.

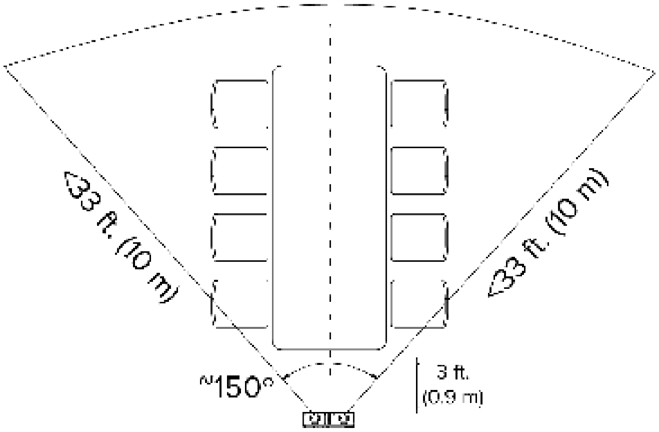


- To ensure the optimal performance of the EagleEye Director II camera system facial recognition feature, follow these suggestions:
  - Provide ample lighting on faces of participants. This allows the EagleEye Director II camera system to correctly frame faces, using the eyes, noses, and mouths as guidelines.
  - Allow only minimal backlighting.
- To ensure the best view from the EagleEye Director II camera system voice-tracking feature, follow these suggestions:
  - Make sure ambient room noise is quiet enough to allow the EagleEye Director II camera system to locate the participant who is speaking.
  - Be sure to set up the audio connection from theRealPresence Centro system to the EagleEye Director II camera system, whether you connect it directly to the audio output of the RealPresence Centro system or to an audio processor managing the room audio.
  - Set the EagleEye Director II camera system on top of a monitor. Ideally, place the camera between 5.5 and 7 feet from the ground.

The following figure shows placement of EagleEye Director II camera system:



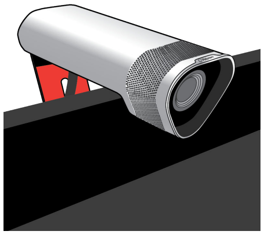
Ensure that people are sitting within the viewing range of between 3 and 33 feet from the device. The following figure shows the viewing range of EagleEye Director II camera system.



Note: Before powering on the EagleEye Director II camera system, connect the camera system to the RealPresence Centro system using a HDCI cable. This will prevent the camera system from automatically entering sleep mode after three minutes.

Setting Up Polycom EagleEye Acoustic Camera

The Polycom EagleEye Acoustic camera is designed to be placed on top of your monitor, as shown next.



Running the Setup Wizard

Topics:

- Run the Setup Wizard from a Remote Location
- Run the Setup Wizard Locally

When you power on your RealPresence Centro system or enter the IP address for the first time, the setup wizard detects the system's IP connections and leads you through the minimum configuration steps. The setup wizard is also called the out-of-box (OOB) wizard. The setup wizard is available during initial setup, after a software update or system reset with system settings deleted, or after using the restore button.

You can install the system software in either of two ways:

- In the room with the system — Use the remote control to navigate the screens and enter information. You can use the number pad on the remote control to enter text. Point the remote control at the camera to control the system.
- From a remote location — If you know the IP address of the system, you can access and configure the system by using the system's web interface.

Run the Setup Wizard from a Remote Location

You can launch and run the setup wizard from a remote location to begin configuring your RealPresence Centro system on the system web interface. If you know the IP address of the system, you can access and configure it using the system web interface.

Procedure

1. Enter the IP address of your system in the system web interface.
2. Navigate the screens and perform the required steps to configure the system.

   After the system starts up from the setup wizard (OOB) wizard, you might be unable to gain access to system web interface for up to a minute. This can occur after the IP address displays on the local interface.

Run the Setup Wizard Locally

You must launch and run the setup wizard to begin configuring your RealPresence Centro system.

Procedure

» After you power on the system for the first time and the setup wizard launches, navigate the screens and perform the required steps to configure the system.

The setup wizard allows you to set an Admin ID and password, where you can limit access to the **Admin Settings**. The default Admin ID is `admin` and the default admin password is the 14-digit system serial number on the **Settings** > **System Information** > **Information** > **System Detail** screen in the local interface or on the back of the system.

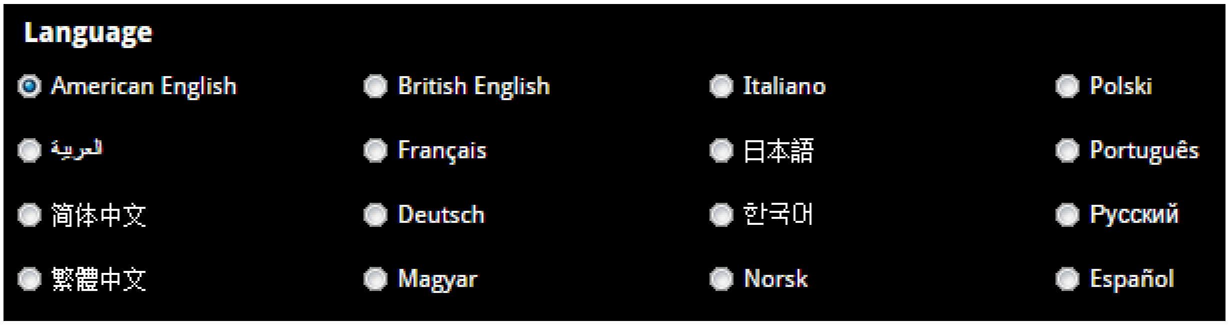
Configuring General System Settings

Topics:

- Name the System
- Enter Contact Information
- Set the Location
- Set the Language
- Set the Date and Time

Name the System

The RealPresence Centro system name appears on the screen of the far-end site when you make a call. The system interface supports the 16 language fonts listed in the following figure. Other languages might not display correctly. The first character of a System Name must be a letter or a number instead of a dollar sign ($) or underscore (_) character. Polycom supports double-byte characters for the system name.



Language

● American English ○ British English ○ Italiano ○ Polski

○ العربية ○ Français ○ 日本語 ○ Português

○ 简体中文 ○ Deutsch ○ 한국어 ○ Русский

○ 繁體中文 ○ Magyar ○ Norsk ○ Español

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **System Name**.
2. In the **System Name** field, enter a name and click **Save**.

Enter Contact Information

You can enter contact information for your RealPresence Centro system so that users know whom to call when they need assistance.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **My Information** > **Contact Information**.
2. Configure the following settings.

Setting	Description
Contact Person	Specifies the name of the system administrator.
Contact Number	Specifies the phone number for the system administrator.
Contact Email	Specifies the email address for the system administrator.
Contact Fax	Specifies the fax number for the system administrator.
Tech Support	Specifies the name of the person who provides technical support.
City	Specifies the city where the system administrator is located.
State/Province	Specifies the state or province where the system administrator is located.
Country	Specifies the country where the system administrator is located.
Help Desk Number	Specifies the phone number of the help desk. This number is used in the help desk setting so that your users can place an audio-only call to the help desk.

Set the Location

On the system web interface, you can set the location to specify the country and the country code where the RealPresence Centro system is located.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **My Information** > **Location**.
2. Configure these settings.

Setting	Description
Country	Specifies the country where the system is located. Changing the country automatically adjusts the country code associated with your system.
Country Code	Displays the country code associated with the country where the system is located.

Set the Language

You can select from 16 different languages to display in the RealPresence Centro local and system web interfaces.

Procedure

» In the system web interface, go to **Admin Settings** > **General Settings** > **Language** and select the language to use in the interface.

Set the Date and Time

On either the system web interface, you can set the date and time settings for your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Date and Time** > **System Time**.
2. Configure these settings:

Setting	Description
Date Format	Specifies how the date is displayed in the interface. **Note:** This a web-only setting.
Time Format	Specifies how the time is displayed in the interface.
Auto Adjust for Daylight Saving Time	Specifies the daylight saving time setting. When you enable this setting, the system clock automatically changes for daylight saving time. **Note:** This a web-only setting.
Time Zone	Specifies the time difference between GMT (Greenwich Mean Time) and your location.
Time Server	Specifies whether the connection to a time server is automatic or manual for system time settings. You can also select **Off** to enter the date and time yourself.
Primary Time Server Address	Specifies the address of the primary time server to use when **Time Server** is set to **Manual**.
Secondary Time Server Address	Specifies the address of the time server to use when the **Primary Time Server Address** does not respond. This is an elective field.

Setting	Description
Current Date and Current Time	• If the **Time Server** is set to **Manual** or **Auto**, these settings are not displayed. • If the **Time Server** is set to **Off**, these settings are configurable.

3. In the system web interface, go to **Admin Settings** > **General Settings** > **Date and Time** > **Time in Call**.
4. Configure these settings:

Setting	Description
Show Time in Call	Specifies the time display in a call: • **Elapsed Time**—Displays the amount of time in the call. • **System Time**—Displays the system time on the screen during a call. • **Off**—Time is not displayed.
When to Show	Specifies when the time should be shown: • **Start of the call only**—Displays only when the call begins. • **Entire call**—Displays continuously throughout the call. • **Once per hour**—Displays at the beginning of the hour for one minute. • **Twice per hour**—Displays at the beginning of the hour and midway through the hour for one minute.
Show Countdown Before Next Meeting	This setting is displayed only when the calendaring service has been enabled. When enabled, it displays a timer that counts down to the next scheduled meeting 10 minutes before that meeting. If a timer is already showing, the countdown timer replaces it 10 minutes before the next scheduled meeting.

Using a Provisioning Service

Topics:

If your organization uses a RealPresence Resource Manager system or a BroadSoft BroadWorks® Device Management System (DMS) system, you can manage systems in dynamic management mode. In dynamic management mode, the following might be true:

- Polycom systems are registered to a standards-based presence service, so presence states are shared with Contacts.
- Polycom systems have access to a corporate directory that supports LDAP access.
  - The Domain, User Name, Password, and Server Address fields are populated on the Provisioning Service screen.
  - Configuration settings that are provisioned, or that are dependent on provisioned values, are read-only on the system.
  - The system checks for new software from the provisioning service every time it restarts and at an interval set by the service. It automatically accesses and runs any software updates made available by the service.
  - A provisioning service system administrator can upload a provisioned bundle from an already configured system. When systems request provisioning, the provisioned bundle and any automatic settings are downloaded. A system user with administrative rights can change the settings on the system after the provisioned bundle is applied. If you later download a new provisioned bundle from the provisioning service, the new bundle overwrites the manual settings.
- If the system has previously registered successfully with a provisioning service but fails to detect the service when it restarts or checks for updates, an alert appears on the System Status screen. If the system loses registration with the provisioning service, it continues operating with the most recent configuration that it received from the provisioning service.

If you use BroadSoft DMS provisioning, note the following points:

- Bundled provisioning is not supported.
- Provisioning uses the same XML-based profile used for dynamic provisioning.
- Provisioned fields are read only.

Enable a Provisioning Service

You can register your RealPresence Centro system with the RealPresence Resource Manager system in a few ways:

- If the system detects a provisioning service on the network while running the setup wizard, it prompts you to enter information for registration with the service.

  The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the restore button. For information about configuring the RealPresence Resource Manager system so that Polycom systems detect and register with it, refer to the *Polycom RealPresence Resource Manager System Operations Guide*.
- You can enter the registration information and attempt to register by going to the **Admin Settings** in the Polycom system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Provisioning Service**.
2. Select the **Enable Provisioning** setting.

Configure a Provisioning Service

After you enable the provisioning service, the RealPresence Centro system should complete the following fields automatically. If the system does not complete the fields automatically, get the information from your network administrator. Multiple Polycom systems can be registered to a single user.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Provisioning Service**.
2. At **Enable Provisioning**, select the checkbox.
3. Configure these settings for automatic provisioning.

Setting	Description
Server Type	Specifies the type of provisioning server. Select RPRM, DMS, or CLOUD. • RPRM is the RealPresence Resource Manager. • DMS is the Broadsoft BroadWorks Device Management System. • CLOUD is the RP Cloud server.
Domain Name	Specifies the domain for registering to the provisioning service.
User Name	Specifies the endpoint's user name for registering to the provisioning service.
Password	Specifies the password that registers the system to the provisioning service.
Server Address	Specifies the address of the system running the provisioning service.

4. Select **Save** or **Update**.

   The system tries to register with the RealPresence Resource Manager or with a DMS system using NTLM authentication.

5. Verify that **Registration Status** changes from **Pending** to **Registered**.

   You might need to wait for a minute or two before the status changes.

Disable a Provisioning Service

You can disable a provisioning service on the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Provisioning Service**.
2. Disable the **Enable Provisioning** setting.

ZTP Web Service Solution

The ZTP solution is a cloud-based Web service designed to simplify the deployment of Polycom devices. The Polycom ZTP console is a web interface that you can use to create and manage profiles and device associations. The ZTP solution is intended as a one-time step at initial deployment. Usually, end customers require a supplier or skilled installer to deploy devices out of the box. The ZTP web console enables you to create provisioning profiles that you can associate with one or more devices. These profiles enable end customers to install the devices themselves. The profiles also provide a central provisioning server address that automatically redirects multiple customer devices to your provisioning server. In addition to setting the provisioning server address, you might also use the solution to do the following:

- Perform software updates (VOIP phones only)
- Set additional configuration parameters that simplify deployment, for example, a custom CA certificate for HTTPS provisioning (VOIP phones only)

For more information, refer to the *Polycom Zero Touch Provisioning User Guide* at Polycom Support.

Certificates and Security Profiles within a Provisioned System

When your RealPresence Centro system is provisioned through the RealPresence Resource Manager system and you use PKI certificates, consider the following information. Be sure to enable provisioning after you follow the procedures applicable to each Security Profile type.

- To use the Maximum Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using Maximum Security Mode.
  - You must manually assign the Maximum Security Profile to the system during installation using the setup wizard, or afterwards using the system web interface.
  - You must use full PKI and observe the following procedures before you enable provisioning on the system:
    1. You must install a signed client certificate on the system to enable the provisioning connection to be authenticated by the RealPresence Resource Manager system.
    2. Decide whether to automatically validate web clients by enabling the **Always Validate Peer Certificates from Browsers** setting. If you do enable the setting, you'll need to

install a signed server certificate and all of the CA certificates needed to validate browser certificates for all web clients. Then configure the certificate revocation method.

3. Decide whether to validate servers by enabling the **Always Validate Peer Certificates from Servers** setting. If you do enable the setting, you must install of the CA certificates needed to validate server certificates from all remote servers. Then adjust the certificate revocation method accordingly. For example, you might need to load additional CRLs if you use the CRL revocation method).

- To use the Medium or High Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using commercial mode.
  - You must manually assign the Medium or High Security Profile to the system during installation using the setup wizard, or afterwards using the system web interface.
  - Configure PKI according to your company's guidelines.
- To use the Low Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using commercial mode.
  - You can enable provisioning in the setup wizard. All provisionable settings are taken from the RealPresence Resource Manager system.

Set Up Multitiered Directory Navigation

You can use the RealPresence Resource Manager to navigate the RealPresence Centro system directories or contacts. Contacts are displayed in a hierarchical format, where you can select the top directory and search for contacts within each level of the directory hierarchy.

This feature is supported using a RealPresence Resource Manager server (LDAP) and does not include standalone LDAP servers or other global directory servers.

The following limitations apply to this feature:

- You can use RealPresence Resource Manager 7.1 and higher only.
- You can search and navigate up to three directory levels.
- This feature is supported on dynamically-managed video conferencing systems only.

Procedure

1. Go to **Admin Settings** > **Servers** > **Directory Servers** and make selections for each setting.
2. Go to **Admin Settings** > **Servers** > **Provisioning Service** and enable provisioning.

Activating System Options

Topics:

- System Software Options

The following topics provide information on how to update software, and to add system software options for your Polycom system.

System Software Options

In the system local interface, activated system options have checkmarks next to them. The following system option is available for your RealPresence Centro system.

For information about integrating with Skype for Business Server 2015, refer to the *Polycom Unified Communications Deployment Guide for Microsoft Environments* at Polycom Support.

View System Software Options

You can view options supported on your RealPresence Centro system in the system web interface.

Procedure

» In the system web interface, go to **Admin Settings** > **General Settings** > **Options**.

The options available on your system are displayed.

Obtain Software or System Option Keys

To perform a major or minor software update or activate options, obtain a key before you run the software update. A *key* is the number that activates software or options on a specific RealPresence Centro system. A key is valid only on the system for which it is generated. You can obtain software or option keys for a single system or for multiple systems. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.

The following types of keys are available:

- **Software keys** are valid for the software updates you are installing as well as for any point, maintenance, or patch releases that may later become available.
- **Option keys** activate software options and are valid across all software releases.

Procedure

1. Open a browser and navigate to Polycom Support.
2. Under Licensing & Product Registration, click **Activation/Upgrade**.
3. Log in to your account.
4. Do one of the following:
    - To update one system, click **Site & Single Activation/Upgrade**. Follow the onscreen instructions to enter your system license number and serial number.

- To update multiple systems that are covered by a software service agreement, click **Batch Upgrade** and then select your product. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers, or serial numbers only.
- To update multiple systems not covered by a software service agreement, click **Batch Activation**. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers, or serial numbers only. Polycom sends a text file containing the requested keys for each system.

Create a Single Key File to Update Multiple Systems

After you receive your key files from Polycom, you can create a single key file to upgrade multiple RealPresence Centro systems.

Procedure

1. Open the key files with a text editor, such as Notepad.
2. Copy the contents of one file to the end of the other file.

   Repeat, as necessary.
3. Save the combined file with the name `sw_keys.txt`.

You now have a single text file that contains all of your keys for software updates. Use the keys in the file to upgrade the applicable systems.

Key File Formats

Most key files use this format:

```
License Number <TAB>Serial Number<TAB>Key
For example, a text file with update license numbers, serial numbers, and
keys might look like this:
U1059-3131-6042-3609<TAB>8213190FFAE7D5<TAB>UBA5-1D6E-EB00-0000-0192
```

The following example shows a software update key file:

```
U1000-0000-0000-0000-0003<TAB>82041003E070B0<TAB>U8FB-0D4E-6E30-0000-0009
U1000-0000-0000-0000-0004<TAB>820327024193AK<TAB>U982-4507-5D80-0000-0009
```

The following example shows an option key file:

```
 K1000-0000-0000-0000-0001<TAB>82041003F082B1<TAB>K15B-DC2D-E120-0000-0009
K1000-0000-0000-0000-0002<TAB>82041503E093B0<TAB>K27E-30F9-2D20-0000-0009
```

RealPresence Centro systems covered by a software service agreement use a slightly different key file format. The following is an example of a software update key file for such a system:

```
U<TAB>82041003F082B1<TAB>U7B6-698E-1640-0000-02C1
U<TAB>82041503E093B0<TAB>UCC1-C9A6-FE60-0000-02C1
U<TAB>82041003E070B0<TAB>UEC6-FDA0-8F00-0000-02C1
U<TAB>820327024193AK<TAB>U7B7-D6BD-3610-0000-02C1
```

Activate System Options

To activate certain features on your RealPresence Centro system, you must use the system's web interface. Some of the features of a system are optional. If you want to activate your system options without upgrading your software, you do not need to download software or run the software update. The only thing you need is your system option key.

Procedure

1. Open a supported browser and go to the system's web interface.
2. Navigate to **Admin Settings** > **General Settings** > **Options**.
3. Enter the option key and click **Save**.

Enter a Multipoint Option Key

You can use your RealPresence Centro system to participate in multipoint conferences. Multipoint conferences include multiple video sites and can also include H.323 audio-only or SIP audio-only sites. All H.323 audio-only and SIP audio-only connections count toward the number of sites in a call. Multipoint calls require a multipoint conferencing unit (MCU) or a hosting system. Depending on the system's configuration, systems can host multipoint calls. You cannot configure multipoint calls without purchasing and installing a Multipoint Video Conferencing option key code.

Depending on your system model, you might need to enter a multipoint option key to enable multipoint calling. For information about purchasing a multipoint call option, please contact your Polycom distributor.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Options**.
2. In the **Key** field, enter the Multipoint Video Conferencing option key.
3. Click **Save**.

Calendaring Service

Topics:

- Enable the Calendaring Service
- Join Scheduled Meetings

RealPresence Centro systems can connect to Microsoft Exchange Server 2013 to retrieve calendar information for a specific Microsoft Outlook or a Microsoft Office 365 individual or system account. The system connects to Microsoft Exchange Server using the credentials you provide, or by automatically discovering the connection information based on an email address or SIP server address.

Connection to a calendaring service allows the system to:

- Display the day's scheduled meetings, along with details about each
- Display a Join button on all scheduled meetings for the current day
- Let users join the meeting without knowing the connection details
- Hide or show details about meetings marked Private, depending on the configuration of the system
- Display a meeting reminder before each scheduled meeting, along with a reminder tone

Professional Services for Microsoft integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details, please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Enable the Calendaring Service

Before users can view their scheduled meetings on the RealPresence Centro system local interface, you must enable the Calendaring Service in the system web interface. Microsoft Exchange Server 2013 and Skype for Business 2015 are supported.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Calendaring Service**.
2. Configure these settings, as appropriate:

Setting	Description
Enable Calendaring Service	Enables the room video system to connect to a calendaring service and retrieve meeting information.
Email	Specifies the mailbox account this system should monitor for calendar information. This should match the Primary SMTP Address for the account on Microsoft Exchange Server 2013/Skype for Business 2015, which displays as the value of the mail attribute in the account properties.

Setting	Description
Domain	Specifies the domain for registering to the Microsoft Exchange Server 2013/Skype for Business 2015, in either NETBIOS or DNS notation, for example, either `company.local` or `COMPANY`. If you are using the **Auto Discover Using** setting, do not provide a value in this field.
User Name	Specifies the user name for registering to Microsoft Exchange Server 2013/Skype for Business 2015, with no domain information included. This can be the system name or an individual's name. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the user name for that account in this field.
Password	Specifies the system password for registering with Microsoft Exchange Server 2013/Skype for Business 2015. This can be the system password or an individual's password. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the password for that account in this field.
Auto Discover Using	Specifies how the system obtains the Microsoft Exchange Server/Skype for Business 2015 address. If you select Email Address, the system uses the value provided in the Email field. If you select SIP Server, the system uses the registered SIP server domain name configured for the system. When using this feature, you must provide values in the Email, User Name, and Password fields that correspond to the Microsoft Outlook or Microsoft Office 365 individual or system account you want the system to use for the Calendaring Service. The system may prompt you to confirm the password. If after configuring the Calendaring Service a message displays that the system was unable to discover the service, ensure the information you provided is correct. For example, make sure the email address is in a valid <username@domain> format.

Setting	Description
Microsoft Exchange Server	Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access Server/ Skype for Business 2015. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server's Virtual IP Address. If required, an IP address can be used instead of an FQDN, but Polycom recommends using the same FQDN that is used for Outlook clients. Provide a value in this field only if you want to manually provide connection information to Microsoft Exchange Server/Skype for Business 2015. Otherwise, use the **Auto Discover Using** setting that allows the system to automatically determine the connection information for Microsoft Exchange Server/Skype for Business 2015 and populate this field.
Secure Connection Protocol	Specifies the connection protocol to use to connect to the server. Select **Automatic** or **TLS 1.0**.
Meeting Reminder Time in Minutes	Specifies the number of minutes before the meeting that a reminder will display on the system.
Play Reminder Tone When Not in a Call	Specifies whether to play a sound along with the text reminder when the system is not in a call.
Show Information for Meetings Set to Private	Specifies whether to display details about meetings marked private.

For more information about using the calendar, refer to the *Polycom RealPresence Centro User Guide.*

Join Scheduled Meetings

If your RealPresence Centro RealPresence Centro system is configured to connect to the Microsoft Exchange Server/Skype for Business 2015, you can join a scheduled meeting from the Calendar screen. If the home screen does not display calendar information, the system is not registered with the Microsoft Exchange Server. If no meetings are scheduled, a “No Meetings Today” message is displayed.

Procedure

1. With your remote control, select a meeting on the home screen.
2. Select **Join** to call into the meeting.

For more information about joining scheduled meetings, refer to the *Polycom RealPresence Centro User Guide*. For more information about setting up Microsoft Exchange Server 2013 accounts to use the calendaring service, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at Polycom Support.

Configuring Network Settings

Topics:

Before you begin configuring network settings, make sure your network is ready for video conferencing. Polycom offers contract high-definition readiness services. For more information, contact your Polycom distributor.

The following topics cover network types used worldwide, but note that not all network types are available in all countries.

Connecting to a LAN

You must connect the RealPresence Centro system to a LAN to do any of the following with your system:

- Make H.323 or SIP calls
- Use a Global Directory Server
- Register with a management system
- Access the system web interface
- Use People+Content IP
- Connect to a RealPresence Touch device

Configure LAN Properties

You can configure LAN properties for your RealPresence Centro system in the local or system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. Configure the following LAN Options settings in the system web interface at **Admin Settings** > **Network** > **LAN Properties** > **LAN Options**.

Setting	Description
Host Name (system web interface only)	Indicates the system's name. If the system discovers a valid System Name during the software installation process, a Host Name is automatically created. However, if an invalid system name is found, such as a System Name with a space, the system creates a Host Name with the following format: SystemType-XXXXXX, where XXXXXX is a set of random alphanumeric characters. **IPv4 networks**: The system sends the host name to the DHCP server to enable it to register the host name with the local DNS server, or it looks up the domain where the endpoint is registered (if supported). **IPv6 networks**: This function is not supported, so you can leave this field blank. However, configuring the field to contain the registered host name is recommended.
Domain Name (system web interface only)	Displays the domain name currently assigned to the system. If the system does not automatically obtain a domain name, enter one here.
Autonegotiation (under **General Settings** in local interface)	Specifies whether the system should automatically negotiate the LAN speed and duplex mode per IEEE 802.3 autonegotiation procedures. If this setting is enabled, the **LAN Speed** and **Duplex Mode** settings become read only. Polycom recommends that you use autonegotiation to avoid network issues.
LAN Speed (under **General Settings** in local interface)	Specifies whether to use **10 Mbps**, **100 Mbps**, or **1000 Mbps** for the LAN speed. Note that the speed you choose must be supported by the switch.
Duplex Mode (under **General Settings** in local interface)	Specifies the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch.
Ignore Redirect Messages (system web interface only)	Enables the system to ignore ICMP redirect messages. You should enable this setting under most circumstances.

Setting	Description
ICMP Transmission Rate Limit (millisec) (system web interface only)	Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 signifies that the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled. This setting applies only to “error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies.
Generate Destination Unreachable Messages (system web interface only)	Generates an ICMP `Destination Unreachable` message if a packet cannot be delivered to its destination for reasons other than network congestion.
Respond to Broadcast and Multicast Echo Requests (system web interface only)	Sends an ICMP `Echo Reply` message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the system.
IPv6 DAD Transmit Count (system web interface only)	Specifies the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The system sends DAD messages to determine whether the address it is requesting is already in use. Select whether to transmit 0, 1, 2, or 3 DAD requests for an IPv6 address.
Enable PC LAN Port	Specifies whether the PC LAN port is enabled on the back of the system. Disable this setting for increased security.
Enable LLDP (under **General Settings** in the system local interface)	Specifies whether Link Layer Discovery Protocol (LLDP) is enabled.
Enable EAP/802.1X (under EAP 802.1X in the system local interface)	Specifies whether EAP/802.1X network access is enabled. The following authentication protocols are supported: • EAP-MD5 • EAP-PEAPv0 (MSCHAPv2) • EAP-TTLS • EAP-TLS
EAP/802.1X Identity (under **EAP 802.1X** in local interface)	Specifies the system's identity used for 802.1X authentication. This setting is available only when EAP/802.1X is enabled. The field cannot be blank.

Setting	Description
EAP/802.1X Password (under **EAP 802.1X** in local interface)	Specifies the system's password used for 802.1X authentication. This setting is required when EAP-MD5, EAP-PEAPv0 or EAP-TTLS is used.
Enable 802.1p/Q (under **802.1p/Q** in local interface)	Specifies whether VLAN and link layer priorities are enabled.
VLAN ID	Specifies the identification of the Virtual LAN.This setting is available only when 802.1p/Q is enabled. The value can be any number from 1 to 4094.
Video Priority	Sets the link layer priority of video traffic on the LAN. Video traffic is any RTP traffic consisting of video data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
Audio Priority	Sets the priority of audio traffic on the LAN. Audio traffic is any RTP traffic consisting of audio data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
Control Priority	Sets the priority of control traffic on the LAN. Control traffic is any traffic consisting of control information associated with a call: • 323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for room systems, is the **Allow Other Participants in a Call to Control Your Camera** setting under **Admin Settings** > **Audio/Video** > **Video Inputs** > **General Camera Settings**) • SIP—SIP Signaling, FECC, Binary Floor Control Protocol (BFCP) This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.

For more information about configuring LAN settings for Microsoft environments, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide at* Polycom Support.

Configure IP Address (IPv4) Settings

You can configure IP address (IPv4) settings for RealPresence Centro systems.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **LAN Properties**.

2. Configure the following IPv4 settings on the LAN Properties screen.

Setting	Description
IP Address	Specifies how the system obtains an IP address. • **Obtain IP address automatically**—Select if the system gets an IP address from a DHCP server on the LAN. • **Enter IP address manually**—Select if the IP address will not be assigned automatically.
Your IP Address is	If the system obtains its IP address automatically, this area displays the IP address currently assigned to the system. If you selected **Enter IP address manually**, enter the IP address here.
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here.
Default Gateway	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here.

Configure IP Address (IPv6) Settings

You can configure IP address (IPv6) settings for RealPresence Centro systems.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. Configure the following IPv6 settings on the LAN Properties screen.

Setting	Description
Enable IPv6	Enables the IPv6 network stack and makes the IPv6 settings available.
IP Address	Specifies how the system obtains an IP address. • **Obtain IP address automatically**—Select if the system gets an IP address from a SLAAC or a DHCP server on the LAN. • **Enter IP address manually**—Select if the IP address will not be assigned automatically.

Setting	Description
Enable SLAAC	Specifies whether to use stateless address autoconfiguration (SLAAC) instead of DHCP to automatically obtain an IP address. Using DHCP to get the IP address requires a DHCP server to get the address from the network, but with SLAAC, existing routers help the system get the IP address from the network.
Link-Local	Displays the IPv6 address used for local communication within a subnet. This setting is configurable only when **Enter IP Address Manually** is selected.
Site-Local	Displays the IPv6 address used for communication within the site or organization. This setting is configurable only when **Enter IP Address Manually** is selected.
Global Address	Displays the IPv6 internet address. This setting is configurable only when **Enter IP Address Manually** is selected.
Default Gateway	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. This setting is configurable only when **Enter IP Address Manually** is selected.

Configure DNS Server Settings

You can configure DNS Server settings in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. Configure the following DNS Servers settings on the LAN Properties screen.

Setting	Description
DNS Servers (in the local interface **DNS** and is not editable)	Displays the DNS servers currently assigned to the system. When the IPv4 or IPv6 address is obtained automatically, the DNS Server addresses are also obtained automatically. You can specify IPv4 DNS server addresses only when the IPv4 or IPv6 address is entered manually.

Setting	Description
Server 1 AddressServer 2 Address Server 3 Address Server 4 Address (read-only in the local interface)	If the system does not automatically obtain a DNS server address, you can enter one here. Up to four DNS server addresses are allowed. If all four address fields show addresses, you cannot add another.

LLDP and LLDP-MED Support

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) are supported on RealPresence Centro systems. LLDP is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices to advertise their identity and capabilities on an IEEE 802 local area network (LAN). This protocol runs over the data-link layer only, allowing connected systems running different network layer protocols to discover information about each other. LLDP-MED is an extension of LLDP.

Examples of applications that use information discovered by LLDP include:

- Network topology - A network management system (NMS) can accurately represent a map of the network topology.
- Inventory - A management system can query a switch to learn about all the devices connected to that switch. The LLDP protocol is formally specified in standards document IEEE 802.1AB.

LLMP-MED Information Discovery

LLDP-MED enables the following information discovery for RealPresence Centro systems:

- Auto discovery of LAN policies enabling plug and play networking
- Inventory management, which allows network administrators to track their network devices.

Behavior When LLDP is Enabled

When LLDP is enabled on a RealPresence Centro system, it discovers VLANs advertised by the network switch and automatically configures the system for one of the VLANs. If the room system discovers any of the following VLAN types in LLDP data from the network switch, the system automatically configures itself for one of them. The chosen VLAN type is based on the order of precedence, as follows:

- Video Conferencing VLAN
- Voice VLAN
- Voice Signaling VLAN

If none of the above VLAN types are found, the room system configures itself for the default or native LAN of the switch port to which it is connected.

LLDP packets are transmitted regularly so that the network switch (and the neighboring endpoints) are aware of the system presence on the network.

Enable LLDP Using a USB Storage Device

When you install a new RealPresence Centro system on a network (or reset the system), you can enable LLDP just before the setup wizard process using a USB storage device.

Procedure

1. Create a usbprovisioning.properties file with the following text string:

   ```
   lldpenable=true
   ```

2. Copy the usbprovisioning.properties file to a USB storage device into the root folder.
3. Ensure that the system is powered off.
4. Insert the USB storage device into the system USB drive.
5. Power on the system.

   ```
   After the room system detects the file, you cannot interact with the
   system while it detects and places it into the VLAN network. Once the
   LLDP detection process is complete, you can continue the setup wizard
   process.
   ```

Enable LLDP in the Web Interface

If you have already used the setup wizard and do not want to reset your RealPresence Centro system to run the setup wizard again, you can configure LLDP in the system web interface.

Procedure

» In the system web interface, go to **Admin Settings** > **Network** > **LAN Properties**.

Select the check box at **Enable LLDP** and click **Save**.

IP Network Settings

You can configure the following IP network protocols in the RealPresence Centro system web interface.

- H.323
- SIP

Configure H.323 Settings

If your network uses a gatekeeper, the RealPresence Centro system can automatically register its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

Procedure

» In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **H.323 Settings** to configure the following settings:

Setting	Description
Enable IP H.323	Allows the H.323 settings to be displayed and configured.

Setting	Description
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The **H.323 Name** is the same as the **System Name**, unless you change it. Your organization's dial plan might define the names you can use.
H.323 Extension (E.164)	Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system. Your organization's dial plan might define the extensions you can use.

Configure the System to Use a Gatekeeper

A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows RealPresence Centro system users to make calls using static aliases instead of IP addresses that can change.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **H.323 Settings**.
2. Configure the following settings.

Setting	Description
Use Gatekeeper	Select this setting to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **Off**—Calls do not use a gatekeeper. • **Auto**—System attempts to automatically find an available gatekeeper. • **Specify**—Calls use the specified gatekeeper. This setting must be selected to enable H.235 Annex D Authentication. When you select a setting other than **Off**, the **Registration Status** is displayed below the **Enable IP H.323** setting.

Setting	Description
Require Authentication	Enables support for H.235 Annex D Authentication. When H.235 Annex D Authentication is enabled, the H.323 gatekeeper ensures that only trusted H. 323 endpoints are allowed to access the gatekeeper. This setting is available when **Use Gatekeeper** is set to **Specify**.
User Name	When authentication is required, specifies the user name for authentication with H.235 Annex D.
Enter Password	When authentication is required, specifies the password for authentication with H.235 Annex D.
Current Gatekeeper IP Address	If you chose **Off** for the **Use Gatekeeper** field, the **Current Gatekeeper IP Address** field is not displayed. Displays the IP address that the gatekeeper is currently using.
Primary Gatekeeper IP Address	• If you chose **Off** for the **Use Gatekeeper** field, the **Primary Gatekeeper IP Address** field is not displayed. • If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper's IP address. • If you chose to specify a gatekeeper, enter the gatekeeper's IP address or name (for example, `10.11.12.13` or `gatekeeper.companyname.usa.com`). The primary gatekeeper IP address contains the IPv4 address the system registers with. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the system unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper.

SIP Settings

If your network supports the Session Initiation Protocol (SIP), you can use SIP to connect IP calls on your RealPresence Centro system.

The SIP protocol has been widely adapted for voice over IP communications and basic video conferencing; however, many of the video conferencing capabilities are not yet standardized. Many capabilities also depend on the SIP server.

The following are examples of features that are not supported using SIP:

- Cascaded multipoint in SIP calls.
- Meeting passwords. If you set a meeting password, SIP endpoints will be unable to dial in to a multipoint call.

For more information about SIP compatibility issues, refer to the *Polycom RealPresence Centro Release Notes*.

Configure SIP Settings

You can configure SIP settings in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **SIP.**
2. Configure the following settings.

Setting	Description
Enable SIP	Allows the SIP settings to be displayed and configured.
Enable AS-SIP	Allows the SIP settings to be displayed and configured.
SIP Server Configuration	Specifies whether to automatically or manually set the SIP server's IP address. If you select **Auto**, the Transport Protocol, Registrar Server, and Proxy Server settings cannot be edited. If you select **Specify**, those settings are editable.

Setting	Description
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required for the room system. **Auto**—Enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. **TCP**—Provides reliable transport via TCP for SIP signaling. **UDP**—Provides best-effort transport via UDP for SIP signaling. **TLS**—Provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. Select TLS if you want to encrypt SVC calls.
Force Connection Reuse	This setting is disabled by default (recommended). When disabled, it causes the system to use an ephemeral source port for all outgoing SIP messages. When enabled, it causes the system to use the active SIP listening port as the source port (5060 or 5061, depending on the negotiated SIP transport protocol in use). This can be useful to establish correct operation with remote SIP peer devices, which require that the source port match the contact port in SIP messages.

Setting	Description
BFCP Transport Preference	Controls the negotiation behavior for content sharing using the Binary Floor Control Protocol (BFCP). Establishes the relationship between the floor control server and its clients, while the available settings determine how network traffic flows between the server and clients. TCP is typically known as the older, slightly slower, and more reliable method, but is not supported under some circumstances, such as with session border controllers (SBCs). **Prefer UDP**—Starts resource sharing using UDP, but fall back to TCP if needed. This is the default value when SIP is enabled. **Prefer TCP**—Starts resource sharing using TCP, but fall back to UDP if needed. **UDP Only**—Shares resources only through UDP. If UDP is unavailable, content sharing in a separate video stream is not available. **TCP Only**—Shares resources only through TCP. If TCP is unavailable, content sharing in a separate video stream is not available.
Sign-in Address	Specifies the SIP address or SIP name of the system, for example, mary.smith@department.company.com. If you leave this field blank, the system's IP address is used for authentication.
User Name	Specifies the user name to use for authentication when registering with a SIP Registrar Server, for example, marySmith. If the SIP proxy requires authentication, this field and the password cannot be blank.
Password	Specifies the password associated with the User Name used to authenticate the system to the Registrar Server. The password can be up to 47 characters in length.

Setting	Description
Registrar Server	Specifies the IP address or DNS name of the SIP Registrar Server. The address can be specified as either an IP address or a DNS fully qualified domain name (FQDN). If registering a remote system with an Edge Server, use the FQDN of the edge server. By default for TCP, the SIP signaling is sent to port 5060 on the registrar server. By default for TLS, the SIP signaling is sent to port 5061 on the registrar server. Enter the address and port using the following format: • <IP_Address>:<Port> • <IP_Address> can be an IPv4 or IPv6 address, or a DNS FQDN such as `servername.company.com:6050`. Syntax Examples: • To use the default port for the protocol you have selected: 10.11.12.13 • To specify a different TCP or UDP port: 10.11.12.13:5071
Proxy Server	Specifies the DNS FQDN or IP address of the SIP Proxy Server. If you leave this field blank, the address of the Registrar Server is used. If you leave both the SIP Registrar Server and Proxy Server fields blank, no Proxy Server is used. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server. The syntax used for this field is the same as for the Registrar Server field.
Registrar Server Type	Specifies the registrar server type. Select **Microsoft** or **Unknown**.

If you have entered specific server addresses into the address fields Registrar server and Proxy server at **Admin Settings** > **Network** > **IP Network** > **SIP**, before you change the SIP Server Configuration setting from **Specify** to **Auto**, you must clear the address fields and then click **Save**. If the server fields are not cleared, SIP registration might fail.

For more information about this and other Microsoft interoperability considerations, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide at* Polycom Support.

RTV and Skype-Hosted Conference Support

Real-time video (RTV) provides higher resolutions during video calls when integrated with Skype for Business Server 2015. To use RTV in a Skype-hosted conference, you must have the Skype for Business Interoperability License key enabled on your RealPresence Centro system.

For more information about configuring your Skype for Business Server 2015 video settings for RTV, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at Polycom Support.

Multilevel Precedence and Preemption (MLPP)

Multilevel Precedence and Preemption (MLPP) provides call prioritization over network resources and far-end system access. Authorized users place precedence calls to elevate the priority of the call through the AS-SIP network. RealPresence Centro systems already in a call can be preempted by an incoming call with a higher priority. In addition, precedence call signaling and media packets are marked with DSCP values associated with the precedence level to ensure network QoS commensurate with the call precedence level.

Systems provide support for placing precedence calls through the use of precedence prefix codes in the dial string. Calls can be placed at any of the precedence levels defined within the network domain configured as the default domain for outbound calls. The default network domains `uc` and `dsn` define five precedence levels: **Routine**, **Priority**, **Immediate**, **Flash**, or **Flash Override**. The system signals the precedence level according to the standards in *UCR 2008, Change 3*, and provides appropriate feedback to the user placing the call.

Incoming calls are announced with the appropriate precedence level, and the authorized user can select one of the following ways to handle the call:

- Answer directly
- Join into conference
- Hang up current call and answer

Define MLPP Network Domains

You can define MLPP network domain names for your RealPresence Centro system.

Procedure

1. To edit a domain, click ✎.
2. If needed, edit the **Network Domain Name** or change the **Allow Incoming Calls** setting.

   Disabling the **Allow Incoming Calls** setting causes the system to reject any calls from this network domain.
3. Select a **Precedence Level**.

   You can define a total of 10 precedence levels.
4. Configure these settings.

Setting	Description
Precedence Level	The name associated with the precedence level. You can click **Add Precedence Level** to create a level and you can click ☒ to remove a level.
Dial Digit	A single numeric field (0-9) that represents the dialing digit used to indicate the requested call precedence. The precedence dial string is indicated by a leading '9' followed by the Dial Digit, followed by the 7- or 10-digit number.
Resource Priority Header	Represents the value in the SIP Resource Priority Header used to signal the precedence level. This field accepts a single UTF-8 character.
Audio DSCP	Indicates the DSCP value used for audio RTP/ SRTP packets sent in calls using this precedence level. The field accepts an integer value range from 0-63.
Video DSCP	Indicates the DSCP value used for video RTP/ SRTP packets sent in calls using this precedence level. The field accepts an integer value range from 0-63.

5. Click **Save**.

Add an MLPP Network Domain

You can add an MLPP network domain for your RealPresence Centro system.

Procedure

1. To add a network domain, click ⊞ and then configure the same settings for the new network domain in the define MLPP network domains task above.
2. Click **Save** when you are finished configuring the settings to save your changes.

Alternative Network Address Type (ANAT)

ANAT signaling is used for IPv4 and IPv6 support in AS-SIP and is only useful in AS-SIP environments. When AS-SIP is enabled, and dual stack (IPV4 and IPV6) is enabled, ANAT signaling is enabled.

RealPresence Centro

- Be sure to register the system only to AS-SIP-aware proxy/registrar servers, because AS-SIP signaling can be incompatible with other types of proxy/registrar servers.
- If the Cisco Telepresence Interoperability Protocol (TIP) software option is installed, turn off TIP signaling on the RealPresence Centro

When you enable AS-SIP on a RealPresence Centro system, register the system only to AS-SIP-aware proxy/registrar servers, because AS-SIP signaling can be incompatible with other types of proxy/registrar servers.

Configure Network Quality Settings

You can specify how your RealPresence Centro system responds to network quality issues by configuring the Network Quality settings; these settings control how your network handles IP packets during video calls.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **Network Quality**.
2. Configure the following settings.

Setting	Description
Automatically Adjust People/Content Bandwidth	Specifies whether the system should automatically adjust the bandwidth necessary for the People stream or Content stream depending on the relative complexity of the people video, content video, or both. If this setting is enabled, the **Quality Preference** setting is not available.
Quality Preference	Specifies which stream has precedence when attempting to compensate for network loss: • **Both** People and Content streams • **People** streams • **Content** streams The stream defined to have precedence experiences less quality degradation during network loss compensation than the stream not having precedence. Choosing **Both** People and Content streams means that both streams experience roughly equal degradation. This setting is not available when the **Automatically Adjust People/Content Bandwidth** setting is enabled.

Setting	Description
Type of Service	Specifies your service type and lets you choose how to set the priority of IP packets sent to the system for video, audio, FECC, and OA&M: • **IP Precedence**—Represents the priority of IP packets sent to the system. The value can be between 0 and 7. • **DiffServ**—Represents a priority level between 0 and 63. **Note:** If AS-SIP is enabled and you select **DiffServ**, the DSCP values for audio and video defined for the negotiated call precedence level in the default network domain that was configured for outbound calls override the **Video** and **Audio** settings defined on this screen of the system web interface. If you have not enabled AS-SIP, the **Video** and **Audio** values defined here are used.
Video	Specifies the IP Precedence or Diffserv value for video RTP traffic and associated RTCP traffic.
Audio	Specifies the IP Precedence or Diffserv value for audio RTP traffic and associated RTCP traffic.
Control	Specifies the IP Precedence or Diffserv value for control traffic on any of the following channels: • **323**—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for room systems, is the **Allow Other Participants in a Call to Control Your Camera** setting under **Admin Settings** > **Audio/Video** > **Video Inputs** > **General Camera Settings**) • **SIP**—SIP Signaling, FECC, Binary Floor Control Protocol (BFCP)
OA&M	Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC.
Maximum Transmission Unit Size	Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or select a maximize size.
Maximum Transmission Unit Size Bytes	Specifies the MTU size, in bytes, used in IP calls. If the video becomes blocky or network errors occur, packets might be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets might be too small; increase the MTU.

Setting	Description
Enable Lost Packet Recovery	Allows the system to use LPR (Lost Packet Recovery) if packet loss occurs. For more details.
Enable RSVP	Allows the system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.
Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum call rate for a call.
MRC Bandwidth Allocation	Adjusts media bit stream bandwidth, reducing packet loss. Specifically designed for SVC-based calls.
Maximum Transmit Bandwidth	Specifies the maximum transmit call rate between 64 kbps and the system's maximum line rate. This setting can be useful when the system is connected to the network using an access technology that provides different transmit and receive bandwidth (such as cable or DSL access).
Maximum Receive Bandwidth	Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate. This setting can be useful when the system is connected to the network using an access technology that provides different transmit and receive bandwidth (such as cable or DSL access).

Lost Packet Recovery and Dynamic Bandwidth Settings

You can handle video quality issues on your RealPresence Centro system by enabling the **Enable Lost Packet Recovery** (LPR) setting, the **Dynamic Bandwidth** setting, or both settings.

If both settings are enabled, Dynamic Bandwidth adjusts the video rate to reduce packet loss to 3% or less. When packet loss drops to 3% or less, LPR cleans up the video image on your monitor. The additional processing power required might cause the video rate to drop while the system is using LPR. If this happens, the Call Statistics screen shows the Video Rate Used as lower than the Video Rate. If Packet Loss is 0 for at least 10 minutes, LPR stops operating and the Video Rate Used increases to match the Video Rate.

If only LPR is enabled and the system detects packet loss, LPR attempts to clean the image but the video rate is not adjusted. If only Dynamic Bandwidth is enabled and the system detects packet loss of 3% or more, the video rate is adjusted but LPR does not clean the image.

You can view percent Packet Loss, Video Rate, and Video Rate Used on the Call Statistics screen.

Securing the System

Topics:

For detailed information about configuring security settings, see the following topics.

Configure Security Profiles

System security profiles provide varying levels of secure access to your RealPresence Centro system. The security profile your system uses provides the basis for secure access within the system and determines how users can operate the system.

The security profile is selected during system setup with the setup wizard, but this setting is configurable through **Admin Settings** in the system web interface. The default values and ability to change some settings are affected by which security profile your system uses.

Consider each security profile as a set of default values for all configuration settings that affect product security and that achieves some level of base product security. You can choose from four profiles—Maximum, High, Medium and Low. Each profile provides a basic security posture, ranging from the most secure to the least secure, which allows you to select a level of security that is appropriate for the deployment of the system in your environment.

Because you can change most of the individual configuration settings regardless of the security profile you chose, Polycom recommends that you select the profile that is closest to the level of security you want in your environment and then customize the settings from there, as needed. In the higher profiles, however, some settings are either not changeable at all or have restricted ranges of values.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security**.
2. Determine which of the following **Security Profile** settings your system uses.

Setting	Description
Maximum	Configures the system to be compliant with U.S. DoD security requirements. Some configuration settings are made read-only in this profile; other settings have restricted ranges of values. This profile represents the highest level of security.
High	Configures the system with most security controls enabled, but does not mandate the use of some controls that are mandated in Maximum profile. Some configuration settings are not changeable in this profile; other settings have restricted ranges of values. This profile is most appropriate for enterprise deployments that demand high security.
Medium	Configures the system with some of the basic security controls enabled, but not all. Most settings are changeable in this profile.
Low	Configures the system with no mandated security controls, although all controls can be enabled as needed. This is the default profile.

3. To change the profile setting, select the **Security Profile** you want to use.

   You can increase or decrease the level of security.
4. Follow the prompts in the Security Profile Change wizard.

Maximum Security Profile Requires Default Value Changes

When you configure the RealPresence Centro system to use the Maximum Security Profile, the system forces you to change the following settings from their default values:

- Admin account User Id
- User account User Id
- Admin room password
- Admin remote access password
- User room password
- User remote access password

Managing System Access

An administrator can configure RealPresence Centro systems to grant access using network accounts that are authenticated through an Active Directory (AD) server such as the Microsoft Active Directory server. In this case, the account information is stored on the AD server and not on the room system. The AD administrator assigns accounts to AD groups, one for the room system admin access and one for user access. For this reason, external authentication is also referred to as Active Directory authentication.

The room system administrator configures the external authentication settings on the system to specify the address of an AD Server for authenticating user logins, AD group for user access, and AD group for admin access on the room system. The system can map only one Active Directory group to a given role.

Users can enter their network account credentials to access the system on the following interfaces:

- Web interface (admin access only)
- Local interface (`user` and `admin` role accounts when **Require Login for System Access** is enabled; `admin` accounts when admin-only areas of the local interface are accessed)

When External Authentication is enabled in PKI environments where Always Validate Peer Certificates from Server is enabled on the system, configure the Active Directory Server Address on the system using the address information that is in the Active Directory Server identity certificate. This allows the system to validate the identity certificate. As an example, if the Active Directory Server identity certificate contains its DNS name only, and no specific IP address, configuring the Active Directory Server Address on the system using the server's IP address results in certificate validation failure, and consequently authentication failure. The system configuration would have to specify the server by DNS name, in this case, to successfully match the server certificate data.

The system local user account is disabled when **Enable Active Directory External Authentication** is enabled. The admin account is active and usable, however.

Enable External Authentication

You can enable external authentication for your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Authentication**.
2. Configure these settings on the Authentication screen, then click **Save**.

Setting	Description
Enable Active Directory External Authentication	Specifies whether to authenticate users through the Active Directory server. When Active Directory authentication is enabled, users are allowed to log in with their network account credentials, using this format: `domain\user` With this format, users can have accounts on multiple domains.
Active Directory Server Address	Specifies the DNS fully qualified domain name (FQDN) or IP address of the Active Directory server (ADS). If you are using subdomains, append port number 3268 as follows: `ad.domain.com:3268` **Note:** Systems can use the RealPresence Resource Manager system as an ADS. If one is deployed in your environment, enter its address here. Otherwise, enter the address of an ADS.
Active Directory Admin Group	Specifies the Active Directory group whose members should have admin access to the system. This name must exactly match the name in the ADS for authentication to succeed.

Setting	Description
Active Directory User Group	Specifies the Active Directory group whose members should have user access to the system. This name must exactly match the name in the ADS for authentication to succeed.

3. If external authentication is not active after completing these steps, go to **Admin Settings** > **Network** > **LAN Properties** > **LAN Options** and ensure that the **Domain Name** setting contains the name of your Active Directory domain.

Use the local system admin credentials to pair the system with a touch device, such as the RealPresence Touch.

Configure Local Access

You can configure local access so that users can reach a RealPresence Centro system through the local interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Local Accounts** > **Login Credentials**.
2. Configure the following settings.

   The order in which the settings are displayed differs between the interfaces.

Setting	Description
Admin ID	Specifies the ID for the administrator account. The default Admin ID is `admin`. Admin IDs are not case sensitive.
Admin Room Password	Specifies the password for the local administrator account used when logging in to the system locally. When this password is set, you must enter it to configure the system **Admin Settings** using the remote control. The password cannot contain spaces or be more than 40 characters. Passwords are case sensitive. The default Admin Room Password is the 14-digit system serial number from the **System Information** screen or the back of the system.
Use Room Password for Remote Access	Specifies whether the room password used for local login is also used for the remote login. When this setting is disabled, the remote access password settings are displayed.

Setting	Description
Admin Remote Access Password	Specifies the password for the local administrator account used when logging in to the system remotely using the system web interface or a telnet session. When this password is set, you must enter it to update the software or manage the system from a computer. The password cannot contain spaces or more than 40 characters.
Require User Login for System Access	Specifies whether the system automatically prompts users to log in when the system comes out of sleep mode or completes the startup process. Enabling this setting requires a login to use the local interface. **Note**: This setting is supported for systems only and is not supported for the Polycom touch devices.
User ID	Specifies the ID for the user account. The default User ID is `user`. User IDs are not case sensitive.
User Room Password	Specifies the password for the local user account used when logging in to the system locally. The password cannot contain spaces or more than 40 characters. Passwords are case sensitive.
User Remote Access Password	Specifies the password for the local user account used when logging in to the system remotely. The password cannot contain spaces or more than 40 characters. Passwords are case sensitive.

Configure Remote Access

You can configure, manage, and monitor Polycom systems from a computer using the RealPresence Centro system web interface. You can also use RealPresence Resource Manager, SNMP, or the API commands.

- The system web interface requires only a web browser.
- RealPresence Resource Manager requires the management application to be installed on your network.
- SNMP requires network management software on your network management station.

Remote access means reaching a system in some way other than through the local interface, such as by using the web, a serial port, or telnet. A session is an instance of a user connected to the system through one of these interfaces. Sessions include an indication of how you are logged on to the system, such as the local interface, web interface, telnet, or serial API.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access**.

2. Configure the following settings.

Not all settings are available on both interfaces. The visibility of some settings is affected by the type of security profile your system uses.

Setting	Description
Enable Network Intrusion Detection System (NIDS) (system web interface only)	Activates the ability to log entries to the security log when the system detects a possible network intrusion. This setting is enabled or disabled by default based on the security profile, but can be changed.
Enable Web Access	Specifies whether to allow remote access to the system by using the system web interface.
Allow Access to User Settings	Specifies whether the User Settings screen is accessible to users through the local interface.
Restrict to HTTPS	Specifies that the web server is accessible only over a secure HTTPS port. Enabling this setting closes the HTTP port and so disables redirects of sessions from HTTP to HTTPS (all access must be initiated as HTTPS).
Web Access Port (HTTP)	Specifies the port to use when accessing the system using the system web interface using HTTP. If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the system web interface to access the system. This makes unauthorized access more difficult. If Restrict to HTTPS is enabled, the Web Access Port setting is unavailable.
Enable Telnet Access	Specifies whether to allow remote access to the system by telnet.
Enable SSH Access	Specifies whether to allow SSH access.
API Port	Specifies the port for API access. Select port 23 or 24. If you set the API port to port 23, the diagnostics port changes to port 24.
Enable Diagnostics Port Idle Session Timeout	Specifies whether to allow the diagnostics port to time out at the configured time interval or not. The timeout setting is set under Idle **Session Timeout in Minutes**.

Setting	Description
Enable API Port Idle Session Timeout	Specifies whether to allow the API port to time out at the configured time interval or not. The timeout setting is set under Idle **Session Timeout in Minutes**.
Enable SNMP Access	Specifies whether to allow remote access to the system by SNMP.
Allow Video Display on Web **(local interface only)**	Specifies whether you can use the system web interface to view the room where the system is located, or video of calls in which the system participates. **Note**: This feature activates both near site and far site video displays in Web Director.
Lock Port after Failed Logins	Temporarily locks the login port after a configurable number of unsuccessful login attempts have been made.
Enable Whitelist	Specifies whether to enable a whitelist.
Idle Session Timeout in Minutes (system web interface only)	Specifies the number of minutes your system web interface session can be idle before the session times out.
Maximum Number of Active Sessions (system web interface only)	Specifies the maximum number of users who can be logged in to and using your system through telnet or the system web interface at the same time.

Local Accounts

Managing access to the RealPresence Centro system is essential for security. Two roles are supported for accessing the system, an admin role and a user role. Admins can perform administrator activities such as changing configuration, as well as user activities such as placing and answering calls. Users can perform only user-type activities.

Two local accounts are provided, one for the user role (by default named `user`) and one for the admin role (by default named `admin`). The IDs and passwords for these local accounts are stored on the system itself.

Configure Password Policy Settings

You can configure password policies for Admin, User, Meeting, Remote Access, and SNMP passwords. These password settings can ensure that strong passwords are used. Polycom strongly recommends that you create an Admin password for your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Local Accounts** > **Password Requirements**.

2. Configure the following settings for **Admin Room, User Room, Meeting**, **Remote Access**, or **SNMP** passwords.

   Click **Save.**

Setting	Description
Minimum Length	Specifies the minimum number of characters required for a valid password.
Require Lowercase Letters	Specifies whether a valid password must contain one or more lowercase letters.
Require Uppercase Letters	Specifies whether a valid password must contain one or more uppercase letters.
Require Numbers	Specifies whether a valid password must contain one or more numbers.
Require Special Characters	Specifies whether a valid password must contain one or more special characters. Supported characters include:@ - _ ! ; $, \ / & . # *
Reject Previous Passwords	Specifies the number of most recent passwords that cannot be reused. If set to **Off**, all previous passwords can be reused.
Minimum Password Age in Days	Specifies the minimum number of days that must pass before the password can be changed.
Maximum Password Age in Days	Specifies the maximum number of days that can pass before the password must be changed. **Note:** This setting is unavailable for Meeting and SNMP passwords.
Minimum Changed Characters	Specifies the number of characters that must be different or change position in a new password. If this is set to **3**, `123abc` can change to `345cde` but not to `234bcd`. **Note:** This setting is unavailable for Meeting and SNMP passwords.
Maximum Consecutive Repeated Characters	Specifies the maximum number of consecutive repeated characters in a valid password. If this is set to **3**, `aaa123` is a valid password but `aaaa123` is not.
Password Expiration Warning	Specifies how many days in advance the system displays a warning that the password will soon expire, if a maximum password age is set. **Note:** This setting is unavailable for Meeting and SNMP passwords.

Setting	Description
Can Contain ID or Its Reverse Form	Specifies whether the associated ID or the reverse of the ID can be part of a valid password. If this setting is enabled and the ID is `admin`, passwords `admin` and `nimda` are allowed. **Note:** This setting is unavailable for Meeting passwords.

Changes to most password policy settings do not take effect until the next time the password is changed. Changes take effect immediately for **Minimum Password Age in Days**, **Maximum Password Age in Days**, and **Password Expiration Warning**. Changing **Minimum Length** from **Off** to some other value also takes effect immediately.

Preventing Account Unauthorized System Access

RealPresence Centro systems provide access controls that prevent unauthorized use. One way someone might try to discover valid user names and passwords is by exhaustively attempting to log in, varying the user name and password data in a programmatic way until discovering a combination that succeeds. Such a method is called a “brute-force” attack.

To mitigate the risk of such an attack, two access control mechanisms are available on the system. The first type of access control, account lockout, protects local accounts from being vulnerable to brute-force attacks, while the second, port lockout, protects login ports themselves from being vulnerable to brute-force attacks.

Account lockout temporarily locks a local account from accepting logins after a configurable number of unsuccessful attempts to log in to that account. It protects only the local system's Admin and User local accounts. When external authentication is used, the Active Directory Server protects Active Directory accounts.

The systems provide separate account lockout controls for each of their local accounts, which are named Admin and User. The account lock can be invoked due to failed logins on any of the following login ports:

- Local interface
- Web interface
- Telnet interface

For examples of how the account lockout feature works, see the following scenarios.

- **Admin Settings** > **Security** > **Local Accounts** > **Account Lockout** > **Lock Admin Account** after **Failed Logins** is set to **4**.
- **Admin Settings** > **Security** > **Local Accounts** > **Account Lockout** > **Admin Account Lock Duration** is set to **1 Minute**.
- **Admin Settings** > **Security** > **Local Accounts** > **Account Lockout** > **Reset Admin Account Lock** After is set to **1 Hour**.

Scenario 1 - Admin account locked due to excessive failed logins

A user fails to log in to the Admin account twice on the system web interface, and the same or another user fails to log in to the Admin account on the local interface. This means that three failed attempts have been made to the Admin account so far. If the next attempt to log in to the Admin account on any login port is unsuccessful, which would mean **4** failed logins, further attempts to access the Admin account are locked out for **1 Minute** (the expiration of the **Admin Account Lock Duration** period). After the **1 Minute** account lock duration has past, logins will once again be allowed. As this example illustrates, the failed login attempts made to an account accumulate across any login port.

Scenario 2 - Successful login resets the failed login attempts counter

A user fails to log in to the Admin account twice on the system web interface, and the same or another user fails to log in to the Admin account on the local interface. This means that three failed attempts have been made to the Admin account so far. If the next login attempt is successful, then the failed login attempts counter for the Admin account is reset to zero and now once again 4 failed attempts can be made before the Admin account would be locked.

Scenario 3 - Failed attempts counter resets after failed login window closes

A user fails to log in to the Admin account twice on the system web interface, and the same or another user fails to log in to the Admin account on the local interface. This means that three failed attempts have been made to the Admin account so far. If no more failed attempts are made within **1 Hour** of the first failed attempt (which is the value of the **Reset Admin Account Lock Counter After** setting), the failed login attempts counter for the Admin account is reset to zero, and 4 failed attempts are allowed again before the Admin account is locked.

Configure Account Lockout

You can configure account lockout to prevent unauthorized access on your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Local Accounts** > **Account Lockout**.
2. Configure these settings for the appropriate account on the Account Lockout screen, then click **Save**.

   You can configure account lock for the admin account, user account, or both accounts.

Setting	Description
Lock Admin/User Account after Failed Logins	Specifies the number of failed login attempts allowed before the system locks the account. If set to **Off**, the system does not lock the account due to failed login attempts.
Admin/User Account Lock Duration	Specifies the amount of time that the account remains locked due to failed login attempts. After this time period has expired, the failed login attempts counter is reset to zero and logins to the account are once again allowed.

Setting	Description
Reset Admin/User Account Lock Counter After	Specifies the “failed login window” period of time, starting with the first failed login attempt, during which subsequent failed login attempts will be counted against the maximum number allowed (**Lock Admin/User Account after Failed Logins**). If the number of failed login attempts made during this window does not reach the maximum number allowed, the failed login attempts counter is reset to zero at the end of this window. **Note:** The failed login attempts counter is always reset to zero anytime a user successfully logs in.

Enable Access to User Settings

You might want to enable user access to User Settings in the RealPresence Centro system local interface. These settings allow users to control some aspects of cameras and meetings; for example, to allow other people in a call to control your camera, or to enable auto answer for point-to-point or multipoint calls.

User Settings contains the following selections, most of which are also available to administrators under **Admin Settings**. These settings are not available in the Maximum Security Profile unless otherwise noted.

- Meeting Password (available in the Maximum Security Profile)
- Backlight Compensation (available in the Maximum Security Profile)
- Mute Auto-Answer Calls
- Allow Other Participants in a Call to Control Your Camera
- Auto Answer Point-to-Point Video
- Auto Answer Multipoint Video
- Allow Video Display on Web

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access**.
2. Enable the **Allow Access to User Settings** setting.

Restrict Access to User and Administrative Settings

You can restrict access to User Settings and Administration settings in the RealPresence Centro system local interface, making them available only through the system web interface.

Procedure

1. In **Admin Settings** > **General Settings** > **Home Screen Settings** > **Home Screen Icons**, disable the **Show Icons on the Home Screen** setting.
2. Click **Save**.

If the following conditions are met, the ability to show icons is automatically enabled and read only:

- Speed Dial is disabled in the **Admin Settings** > **General Settings** > **Home Screen Settings**.

- The Calendar is not displayed because the system is not connected to the Microsoft Exchange Server.
- Remote access through the web, telnet, and SNMP are disabled in **Security** > **Global Security** > **Access**.

Detecting Intrusions

When the RealPresence Centro system detects a possible network intrusion, it logs an entry to the security log. This logging is controlled by the **Enable Network Intrusion Detection System (NIDS)** setting. The security log prefix identifies the type of packet detected, as shown in the following table.

Prefix	Packet Type
SECURITY: NIDS/unknown_tcp	Packet that attempts to connect or probe a closed TCP port
SECURITY: NIDS/unknown_udp	Packet that probes a closed UDP port
SECURITY: NIDS/invalid_tcp	TCP packet in an invalid state
SECURITY: NIDS/invalid_icmp	ICMP or ICMPv6 packet in an invalid state
SECURITY: NIDS/unknown	Packet with an unknown protocol number in the IP header
SECURITY: NIDS/flood	Stream of ICMP or ICMPv6 ping requests or TCP connections to an opened TCP port

Following the message prefix, the security log entry includes the timestamp and the IP, TCP, UDP, ICMP, or ICMPv6 headers. For example, the following security log entry shows an “unknown_udp” intrusion:

```
2009-05-08 21:32:52 WARNING kernel: SECURITY: NIDS/unknown_udp IN=eth0
OUT= MAC=00:e0:db:08:9a:ff:00:19:aa:da:11:c3:08:00 SRC=172.18.1.80
DST=172.18.1.170 LEN=28 TOS=0x00 PREC=0x00 TTL=63 ID=22458 PROTO=UDP
SPT=1450 DPT=7788 LEN=8
```

For information on the **Enable Network Intrusion Detection System (NIDS)** setting, see the following topic.

View Connections to Your System in a Sessions List

You can view a sessions list to see information about everyone logged in to a RealPresence Centro system including:

- Type of connection, for example, Web
- ID associated with the session, typically Admin or User
- Remote IP address (addresses of people logged in to the system from their computers)

Procedure

» In the system web interface, go to **Diagnostics** > **System** > **Sessions**.

Secure API Access

You can access a RealPresence Centro system using the Secure Shell (SSH) protocol. Secure API access is authenticated for local and Active Directory (AD) accounts.

Note: When a password is empty, SSH will not validate credentials and allow a user to log in. Polycom recommends that you consistently use passwords for secure access.

Secure API access using SSH is enabled by default. The sshenable API command and **Enable SSH Access** system web interface setting have been added to enable or disable the feature.

Enable Secure API Access

You can enable SSH for secure API access in the RealPresence Centro system web interface or in an API session.

Procedure

» Do one of the following:

- In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access** and enable the **Enable SSH Access** setting.
- In a system API session, enter `sshenable true`.

Disable Secure API Access

You can disable SSH for secure API access in the RealPresence Centro system web interface or in an API session.

Procedure

» Do one of the following:

- In the system web interface of the system, select **Admin Settings** > **Security** > **Global Security** > **Access** and disable the **Enable SSH Access** setting.
- In a system API session, enter `sshenable false`.

Access the API with SSH

To obtain secure access to the API, you must use an SSH client and connect to the IP address configured for the RealPresence Centro system on port 22. The system allows three attempts to enter correct login credentials. The SSH client program closes after the third failed attempt.

To access the API with SSH:

Procedure

1. Enable remote access.
2. If necessary, enable external authentication.
3. Enable the SSH feature.

4. Start an SSH session using the system IP address and port 22.
5. When prompted, enter the remote access credentials.

Port Lockout

Port lockout protects against brute-force attacks by temporarily locking the login port after a configurable number of unsuccessful login attempts have been made, regardless of which account was used. Port lockout is supported only on the RealPresence Centro system web interface, and only Admin users are allowed to log in to the system web interface. If external authentication *is not* in use, users can successfully log in to the system web interface only by using the local Admin account credentials. However, when external authentication *is* in use, any number of external accounts can be considered to be Admin users on the system. Failed logins to any of these accounts, or to an unknown account, are all counted against the configured number allowed failed login attempts to the system web interface.

The following is an example of how the port lockout feature works.

A system web interface is configured with these settings:

- **Admin Settings** > **Security** > **Global Security** > **Authentication** > **Enable Active Directory External Authentication** is enabled, a valid **Active Directory Server Address** is configured, as are both the **Active Directory Admin Group** and **Active Directory User Group** settings.
- **Admin Settings** > **Security** > **Global Security** > **Access** > **Lock Port after Failed Logins** is set to **4**.
- **Admin Settings** > **Security** > **Global Security** > **Access** > **Port Lock Duration** is set to **1 Minute**.
- **Admin Settings** > **Security** > **Global Security** > **Access** > **Reset Port Lock Counter After** is set to **1 Hour**.

Scenario 1: Web interface locked due to excessive failed logins

A user fails to log in to the local **Admin** account two times on the system web interface, and another user fails to log in to the external Active Directory ‘SuperUser' account in a separate system web interface session. The ‘SuperUser' account is defined as part of the Active Directory Admin Group on the Active Directory Server.

This means that three failed attempts have been made on the system web interface port—two by one user and one by a second user. If the next attempt to log in to the system web interface by either user or some other user is successful, the failed login counter for the system web interface port is reset to zero, allowing 4 more failed attempts to occur on the system web interface.

On the other hand, if after the third failed login attempt, any user makes a fourth unsuccessful attempt to any account on the system web interface, further attempts to access the system web interface using any account credentials from any user are locked out for **1 Minute**, the value of the **Port Lock Duration** period. After the **1 Minute** port lock period has past, logins will once again be allowed. As this example illustrates, the failed login attempts made to the system web interface accumulate across any attempts to any account and/or by any user.

Scenario 2: Failed attempts counter resets after failed login window closes

A user fails to log in to the local **Admin** account two times on the system web interface, and another user fails to log in to the external Active Directory ‘SuperUser' account in a separate system web interface session. The ‘SuperUser' account is defined as part of the Active Directory Admin Group on the Active Directory Server.

This means that three failed attempts have been made on the system web interface port—two by one user and one by a second user. If no more failed attempts are made within **1 Hour** of the first failed attempt (which is the value of the **Reset Port Lock Counter After** setting), the failed login attempts counter is reset to zero, and 4 failed attempts are allowed again before the system web interface is locked.

Configure the Port Lockout Setting

You can configure the port lockout settings to limit the number of failed logins to your RealPresence Centro system. The telnet port has a port lock feature that is enabled regardless of the state of the port lock feature configuration. Specifically, the telnet server disconnects a telnet login session after 5 failed login attempts. If a new session is started, another 5 attempts are allowed.

If the number of failed login attempts made during this window does not reach the maximum number allowed, the failed login attempts counter is reset to zero at the end of this window.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access**.
2. Configure these settings and click **Save**.

Setting	Description
Lock Port after Failed Logins	Specifies the number of failed login attempts allowed before the system locks the system web interface from accepting logins. If set to **Off**, the system does not lock the system web interface due to failed login attempts.
Port Lock Duration	Specifies the amount of time that a system web interface remains locked due to failed login attempts. After this time period expires, the failed login attempts counter is reset to zero and logins to the system web interface are once again allowed.
Reset Port Lock Counter After	Specifies a “failed login window” period of time, starting with the first failed login attempt, during which subsequent failed login attempts will be counted against the maximum number allowed (**Lock Port after Failed Logins**). **Note:** The failed login attempts counter is always reset to zero anytime a user successfully logs in.

Whitelist

When a whitelist is enabled, the RealPresence Centro system web interface and SNMP ports accept connections only from specified IP addresses. The whitelist supports both IPv4 and IPv6 addresses. You can only configure this feature in the system web interface. The system can accept up to 30 IP address entries for the whitelist.

Note: If you use dynamic IP address assignment, ensure that you keep the whitelist up to date with the latest assigned addresses for computers authorized to access the system. Failing to update the whitelist means these computers cannot connect to the system.

Enable a Whitelist

You can enable a whitelist so that you can add specific IPv4 and IPv6 addresses to the approved list for your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access**.
2. Select **Enable Whitelist**.

Add IP Addresses to a Whitelist

You can edit and add specific IP addresses to a whitelist for your RealPresence Centro system.

Procedure

1. Click the **Edit Whitelist** link.
2. Select address type **IPv4** or **IPv6**.
3. In the address text field, enter the IP address of the system you want to allow.

   Follow the format suggested by the address type you selected. Select **Add**.

   Repeat this step for all the IP addresses you want to add. You can add web server and SNMP addresses.

   If you entered an address in error, highlight the address in the list and select **Clear**.

IPv4 Address Formats

The whitelist configuration requires single IP addresses, a range of addresses, or an IP and netmask. The netmask represents the number of valid bits of the IPv4 address to use. The following are valid IPv4 formats for your RealPresence Centro system:

- 10.12.128.7
- 172.26.16.0/24

IPv6 Address Formats

For IPv6 addresses, you can use a Classless Inter-Domain Routing (CIDR) notation to represent a range of IP addresses. The following are valid IPv6 formats for your RealPresence Centro system:

- ::1
- 2001:db8:abc:def:10.242.12.23
- 2001:db8::/48
- 2001:db8:abcd:0012::0/64
- 2001:0db8:85a3:0000:0000:1234:0abc:cdef

Encryption

AES encryption is a standard feature on all RealPresence Centro systems. When it is enabled, the system automatically encrypts calls to other systems that have AES encryption enabled.

If encryption is enabled on the system, a locked padlock icon appears on the monitor when a call is encrypted. If a call is unencrypted, an unlocked padlock appears on the monitor. In a multipoint call, some connections might be encrypted while others are not. The padlock icon might not accurately indicate whether the call is encrypted if the call is cascaded or includes an audio-only endpoint. To avoid security risks, Polycom recommends that all participants communicate the state of their padlock icon verbally at the beginning of a call.

Keep in mind the following points regarding AES encryption:

- AES encryption is not supported on systems registered to an Avaya H.323 gatekeeper.
- For systems with a maximum speed of 6 Mbps for unencrypted calls, the maximum speed for encrypted SIP calls is 4 Mbps.

The following AES cryptographic algorithms ensure flexibility when negotiating secure media transport:

- H.323 (per H.235.6)
    - AES-CBC-128 / DH-1024
    - AES-CBC-256 / DH-2048
- SIP (per RFCs 3711, 4568, 6188)
    - AES_CM_128_HMAC_SHA1_32
    - AES_CM_128_HMAC_SHA1_80
    - AES_CM_256_HMAC_SHA1_32
    - AES_CM_256_HMAC_SHA1_80

The systems also support the use of FIPS 140 validated cryptography, which is required in some instances, such as when used by the U.S. federal government. When the Require **FIPS 140 Cryptography** setting is enabled, all cryptography used on the system comes from a software module that has been validated to FIPS 140-2 standards. You can find its FIPS 140-2 validation certificate here: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747.

Configure Encryption

You can configure encryption settings on your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Encryption**.
2. Configure these settings.

Setting	Description
Require AES Encryption for Calls	Specifies how to encrypt calls with other sites that support AES encryption. • **Off**—AES encryption is disabled. **When Available**—AES encryption is used in calls with systems that support it. Calls without encryption are allowed when connecting to systems that don't support it. For multipoint calls, this means that some systems might be connected with AES encryption while others are connected without it. **Required for Video Calls Only**—AES encryption is used in all video calls. Calls with systems that do not support it are disconnected. Audio calls using an attached SoundStation IP 7000 are allowed to connect. **Required for All Calls**—AES encryption is used in all calls. Calls with systems that do not support it are disconnected. Audio calls using an attached SoundStation IP 7000 are not allowed to connect, since these calls are not encrypted.
Require FIPS 140 Cryptography(system web interface only)	Enables the exclusive use of the FIPS 140-2-validated software cryptography module for cryptographic functions. Also disables all “weak” protocols and ciphers, including: • SSLv2 • SSLv3 • Non-FIPS 140-2 approved TLS cipher suites
Disable TLS v1.0	Disables the TLS v1.0 application; by default, TLS v1.0 is enabled.

Configuring Encryption Settings for SVC Calls

You must complete two tasks to enable encryption for SVC calls on your RealPresence Centro system:

- Set the transport protocol.
- Set AES encryption.

Set the Transport Protocol for SVC Calls

You can set up the transport protocol for SVC calls for your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network**.
2. Click **SIP** to expand the section.
3. In the **Transport Protocol** list, select **TLS**.
4. Click **Save**.

Set Up AES Encryption for SVC Calls

You can set up AES encryption for SVC calls for the RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Global Security**.
2. Click **Encryption** to expand the section.
3. In the Require AES Encryption for Calls list, select **When Available**, **Required for Video Calls Only**, or **Required for All Calls**.
4. Click **Save**.

Verify H.323 Media Encryption

To provide extra security for encrypted H.323 calls, the RealPresence Centro system provides an encryption check code. Both parties in a call can use this check code to verify that their call is not being intercepted by a 3rd party.

The check code is a 16-digit hexadecimal number that is calculated so that the number is the same at both sites in the call. The numbers are identical if, and only if, the key generation algorithm is performed between the two sites in the call and is not intercepted and modified by a 3rd party.

Procedure

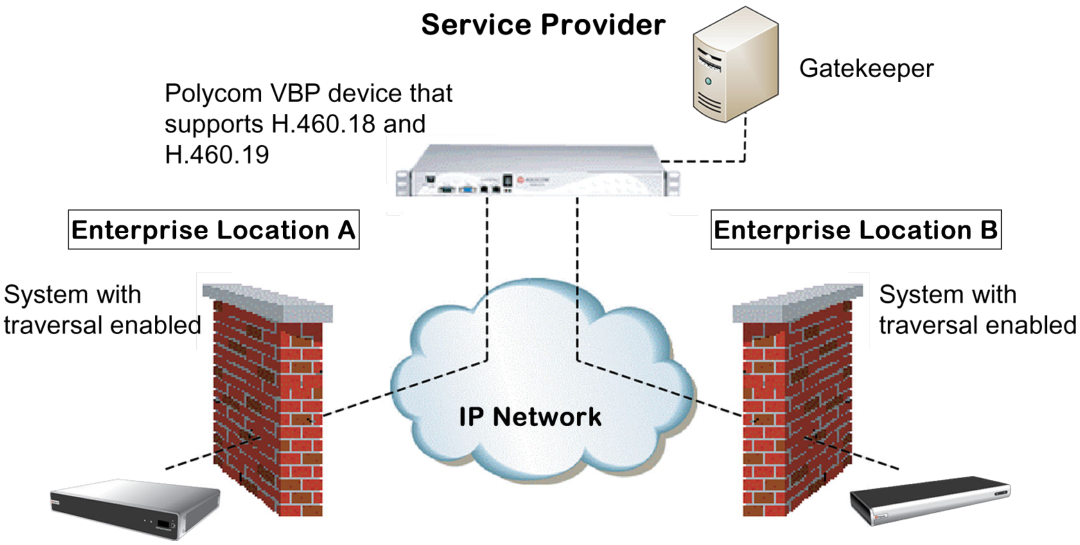
1. Establish an encrypted H.323 call between two sites.
2. At each site, locate the Call Statistics information on the **Place a Call** screen of the system web interface.

   The check code also displays under **Diagnostics > System > Call Statistics** in the **Transmit** column of the **Call Encryption** section.
3. Verbally verify that the code is the same at both sites.
4. Do one of the following:
   - If the codes match, the call is secure. Proceed with the call.
   - If the codes do not match, then there is a possibility that the key exchange is compromised. Hang up the call. Next, check the network path from the local system to the far-end system to determine if the systems are experiencing a *Man in the Middle* attack. This occurs when a foreign device tricks the local system into creating an encryption key using information from the imposter. Then, the imposter can decode the data sent by the local system and eavesdrop on the call.

System Configuration with a Firewall or NAT

You can configure RealPresence Centro systems to use standards-based H.460.18 and H.460.19 firewall traversal, which allows video systems to more easily establish IP connections across firewalls.

The following illustration shows how a service provider might provide H.460 firewall traversal between two enterprise locations. In this example the Polycom Video Border Proxy™ (VBP®) firewall traversal device is on the edge of the service provider network and facilitates IP calls between systems behind different firewalls.


Service Provider
Gatekeeper
Polycom VBP device that supports H.460.18 and H.460.19
Enterprise Location A
Enterprise Location B
System with traversal enabled
System with traversal enabled
IP Network

Ref. Number	Description
1	Polycom Video Border Proxy
2	Gatekeeper
3	IP network
4	Firewall
5	RealPresence Centro system
6	Firewall
7	RealPresence Centro system

Basic Firewall/NAT Traversal Connectivity

Basic Firewall/NAT Traversal Connectivity allows RealPresence Centro systems to connect to the SIP-based RealPresence solutions using the Acme Packet Net-Net family of Session Border Controllers (SBC). A system connects to the Acme Packet Net-Net SBC as a remote enterprise endpoint. The remote enterprise endpoint is registered to the enterprise's SIP infrastructure and connects to an internal enterprise endpoint through the enterprise firewall.

For details about the use and configuration of the Acme Packet Net-Net SBC used in conjunction with this feature, refer to *Deploying Polycom Unified Communications in an Acme Packet Net-Net Enterprise Session Director Environment*.

Polycom systems also provide full mutual TLS support for SIP and XMPP Presence connections. Full mutual TLS support gives administrators the ability to identify and authenticate devices attempting to join conferences from outside the enterprise network.

Configure the H.460 NAT Firewall Traversal

You can enable and configure the H.460 NAT firewall traversal on your RealPresence Centro system.

Procedure

1. Enable firewall traversal on the system.
    a) In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **Firewall**.
    b) Select **Enable H.460 Firewall Traversal**.
2. Register the system to an external Polycom VBP device that supports the H.460.18 and H.460.19 standards.
3. Ensure that firewalls to be traversed allow the system to open outbound TCP and UDP connections.
    - Firewalls with a stricter rule set should allow the systems to open at least the following outbound TCP and UDP ports: 1720 (TCP), 14085-15084 (TCP) and 1719 (UDP), 16386-25386 (UDP).
    - Firewalls should permit inbound traffic to TCP and UDP ports that have been opened earlier in the outbound direction.
4. Configure the following settings.

Setting	Description
Fixed Ports	Lets you specify whether to define the TCP and UDP ports. • If the firewall is not H.323 compatible, enable this setting. The system assigns a range of ports starting with the TCP and UDP ports you specify. The system defaults to a range beginning with port 3230 for both TCP and UDP. **Note**: You must open the corresponding ports in the firewall. For H.323, you must also open the firewall's TCP port 1720; for SIP you must open either UDP port 5060, TCP 5060, or TCP 5061 depending on whether you are using UDP, TCP, or TLS as the SIP transport protocol. • If the firewall is H.323 compatible or the system is not behind a firewall, disable this setting. For IP H.323 you need 2 TCP and 8 UDP ports per connection. For SIP you need TCP port 5060 and 8 UDP ports per connection. **Range of UDP Ports:** Because systems support ICE, the range of fixed UDP ports is 112. The system cycles through the available ports from call to call. After the system restarts, the first call begins with the first port number, either 49152 or 3230. Subsequent calls start with the last port used, for example, the first call uses ports 3230 to 3236, the second call uses ports 3236 to 3242, the third call uses ports 3242 through 3248, and so on. **Fixed Ports Range and Filters**: You might notice that the source port of a SIP signaling message is not in the fixed ports range. When your firewalls are filtering on source ports, in the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **SIP** and enable the **Force Connection Reuse** checkbox. When this setting is enabled, the system uses port 5060/5061 for the source port and for the destination port. These ports are required to be open in the firewall.
TCP Ports **UDP Ports**	Specifies the beginning value for the range of TCP and UDP ports used by the system. The system automatically sets the range of ports based on the beginning value you set. **Note**: You must also open the firewall's TCP port 1720 to allow H.323 traffic.
Enable H.460 Firewall Traversal	Allows the system to use H.460-based firewall traversal for IP calls.

Setting	Description
NAT	Specifies whether the system should determine the NAT Public WAN Address automatically. • If the system is not behind a NAT or is connected to the IP network through a Virtual Private Network (VPN), select **Off**. • If the system is behind a NAT that allows HTTP traffic, select **Auto**. • If the system is behind a NAT that does not allow HTTP traffic, select **Manual.**
NAT Public (WAN) Address	Displays the address that callers from outside the LAN use to call your system. If you chose to configure the NAT manually, enter the NAT Public Address here. This field is editable only when **NAT Configuration** is set to **Manual**.
NAT is H.323 Compatible	Specifies that the system is behind a NAT that is capable of translating H.323 traffic. This field is visible only when **NAT Configuration** is set to **Auto** or **Manual**.
Address Displayed in Global Directory	Lets you choose whether to display this system's public or private address in the global directory. This field is visible only when **NAT Configuration** is set to **Auto** or **Manual**.
Enable SIP Keep-Alive Messages	Specifies whether to regularly transmit keep-alive messages on the SIP signaling channel and on all RTP sessions that are part of SIP calls. Keep-alive messages keep connections open through NAT/ Firewall devices that are often used at the edges of both home and enterprise networks. When a system is deployed or registered in an Avaya SIP environment, Polycom recommends that you disable this setting to allow calls to connect fully.

In environments set up behind a firewall, firewall you can choose to limit access to TCP connections only. Although TCP is an accurate and reliable method of data delivery that incorporates error-checking, it is not a fast method. For this reason, real-time media streams often use UDP, which offers speed but not necessarily accuracy. Within an environment behind a firewall, where firewall administrator has restricted media access to TCP ports, calls can be completed using a TCP connection instead of UDP.

Note: **Caution**: Systems deployed outside a firewall are potentially vulnerable to unauthorized access. Visit the Polycom Security section of the Knowledge Base at Polycom Support for timely security information. You can also register to receive periodic email updates and advisories.

Security Certificates

If your organization has deployed a public key infrastructure (PKI) for securing connections between devices on your network, Polycom recommends that you have a strong understanding of certificate management and how it applies to your RealPresence Centro system before you integrate these products with the PKI.

Systems can use certificates to authenticate network connections to and from the system. Other web applications also use certificates, as you might notice when you navigate the Internet. The system uses configuration and management techniques typical of PKI to manage certificates, certificate signing requests, and revocation checking. ANSI X.509 standards regulate the characteristics of certificates and revocation.

How Certificates are Used

RealPresence Centro systems can generate requests for certificates (CSRs) that are then sent to a certificate authority (CA) for official issuance. The CA is the trusted entity that issues, or signs, digital certificates for others. Once signed by the CA, you can install the certificate on the system for use in all TLS connections used by the system.

Systems support, and typically require, the generation and use of two separate certificates when used in an environment that has a fully deployed PKI:

1. A Server certificate—the system's web server presents this certificate after receiving connection requests from browsers attempting to connect to the system web interface.
2. A Client certificate—the system presents this certificate to a remote server when challenged to provide a certificate as part of authenticating the identity of the system before allowing it to connect to the remote server. Examples of remote servers include the RealPresence Resource Manager system, a SIP proxy/registrar server, or an LDAP directory server.

When systems are deployed in an environment that does not have a fully deployed PKI, you do not need to install these certificates because all systems automatically generate self-signed certificates that can be used to establish secure TLS connections. However, when a full PKI has been deployed, self-signed certificates are not trusted by the PKI and so signed certificates must be used. The following sections describe how to generate and use certificates by using the system web interface.

Certificate Signing Requests

The RealPresence Centro system allows you to install one client and one server certificate for identification of the system to network peers. In order to obtain these certificates you must first create a Certificate Signing Request (CSR) for each certificate. This request, also known as an unsigned certificate, must be submitted to a CA so that it can be signed, after which the certificate can be installed on the system.

Certificate Signing Request Requirements

Whether you need to generate a client-type CSR, a server-type CSR, or both depends on which features and services you intend to use, and whether your network environment supports certificate-based authentication for those services. In most cases, both certificates are needed for RealPresence Centro systems.

For example, if your system is configured to use any of the following features, and the servers providing those services perform certificate-based authentication before allowing access to them, you must create a client-type CSR and add the resulting certificate signed by the CA:

- RealPresence Resource Manager system Provisioning
- RealPresence Resource Manager system Monitoring
- RealPresence Resource Manager system LDAP Directory
- RealPresence Resource Manager system Presence
- Calendaring
- SIP
- 802.1X

The system web server uses the server-type CSR and resulting certificate whenever a user attempts to connect to the system web interface. The web server does so by presenting the server certificate to the browser to identify the system to the browser as part of allowing the browser to connect to the system. The browser's user needs the server certificate if he or she wants to be certain about the identity of the system he or she is connecting to. Settings in the web browser typically control the validation of the server certificate, but you can also validate the certificate manually.

To obtain a client or server certificate, you must first create a CSR. You can create one client and one server CSR and submit each to the appropriate CA for signing. After the CSR is signed by a CA, it becomes a certificate you can add to the system.

Create a Certificate Signing Request

You can create server and client CSRs to identify your RealPresence Centro system to your network peers.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Certificates** > **Certificate Options**.
2. Click **Create** for the type of CSR you want to create, **Signing Request Server** or **Signing Request Client**.

   The procedure is the same for server and client CSRs.
3. Configure these settings on the Create Signing Request screen and click **Create**.

Setting	Description
Hash Algorithm	Specifies the hash algorithm for the CSR. You may select SHA-256 or keep the default SHA-1.

Setting	Description
Common Name (CN)	Specifies the name that the system assigns to the CSR. Polycom recommends the following guidelines for configuring the Common Name: • For systems registered in DNS, use the Fully Qualified Domain Name (FQDN) of the system. • For systems not registered in DNS, use the IP address of the system.Maximum Characters: 64; truncated if necessary. Default is blank
Organizational Unit (OU)	Specifies the unit of business defined by your organization. Default is blank.Maximum Characters: 64 **Note**: The system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.
Organization (O)	Specifies your organization's name. Default is blank.Maximum Characters: 64
City or Locality (L)	Specifies the city where your organization is located. Default is blank. Maximum Characters: 128
State or Province (ST)	Specifies the state or province where your organization is located. Default is blank. Maximum Characters: 128
Country (C)	Displays the country selected in **Admin Settings** > **General Settings** > **My Information**. Not editable.
SAN: FQDN:	Specifies the FQDN assigned to the system. This is the same as the **Common Name (CN)**, but is not truncated. Default is blank.Maximum Characters: 253
SAN: Additional Name:	Specifies an additional name. Default is blank.Maximum Characters: 253
SAN: IPv4 Address:	Default is the IPv4 address of system. Maximum Characters: 15
SAN: IPv4 Address (DNS):	Default is the IPv4 address of system. This field provides the IPv4 address in ASCII format, which is sometimes needed for MSFT server interoperability.Maximum Characters: 15

Setting	Description
SAN: IPv6 Global Address:	Default is the IPv6 Global Address of system. Maximum Characters: 40
SAN: IPv6 Site Local Address:	Default is the IPv6 Site Local Address of system. Maximum Characters: 40
SAN: IPv6 Link Local Address:	Default is the IPv6 Link Local Address of system. Maximum Characters: 40

After you create the CSR, a message indicating that the CSR has been created displays. Two links appear next to the signing request that you just created (**Signing Request Server** or **Signing Request Client**).

- **Download Signing Request** enables you to download the CSR so that it can be sent to a CA for signature.
- **Create** enables you to view the fields of the CSR as they are currently set in the CSR. If you change any of the values you previously configured, you can click **Create** to generate a new CSR that can then be downloaded.

Note: Only a single outstanding CSR of either type can exist at a time. After the CSR is generated, it is important to get it signed and installed before attempting to generate a different CSR of the same type. For example, if you generate a client CSR and then, prior to having it signed and installed on the system, another client CSR is generated, the previous CSR is discarded and invalidated, and any attempt to install a signed version of it will result in an error.

RealPresence Server Address Configuration in PKI-enabled Environments

You can configure server addresses for services listed in **Certificate Validation Settings** that need a client-type CSR, such as SIP, LDAP directory, etc. If the server address is contained in the server certificate that it presents during a connection, you might need to use a particular address format for your RealPresence Centro system. In this case, use the following guidance to configure server addresses:

- If the certificate contains the fully qualified domain name (FQDN) of the server, use the FQDN when configuring the server address.
- If the certificate contains the IP address of the server, use the IP address when configuring the server address.
- If the certificate does not contain any the server's address in any form, you can use either the FQDN or the IP address of the server when configuring the server address.

Enable PKI Certificates

If your RealPresence Centro system will be provisioned by the RealPresence Resource Manager and you plan to use PKI certificates, you must ensure that you configure the **Host Name** setting.

Procedure

1. On the system web interface, go to **Admin Settings** > **Network** > **LAN Properties** > **LAN Options**.
2. At **Host Name**, use the same name that the RealPresence Resource Manager uses to provision the system.

This name must be the same so that certificate signing requests (CSRs) generated during certificate installation have the correct host name information.

Configure Certificate Validation Settings

Certificates are authorized externally when they are signed by the CA. The certificates can be automatically validated when they are used to establish an authenticated network connection. To perform this validation, the RealPresence Centro system must have certificates installed for all CAs that are part of the trust chain. A trust chain is the hierarchy of CAs that have issued certificates from the device being authenticated, through the intermediate CAs that have issued certificates to the various CAs, leading back to a root CA, which is a known trusted CA. The following sections describe how to install and manage these certificates.

A certificate exchange is between a server and a client, both of which are peers. When a user is accessing the system web interface, the system is the server and the web browser is the client application. In other situations, such as when the system connects to LDAP directory services, the system is the client and the LDAP directory server is the server.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Certificates** > **Certificate Options**.
2. Configure these settings on the Certificates screen and click **Save**.

Setting	Description
Maximum Peer Certificate Chain Depth	Specifies how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host to the system when a network connection is being established between the two systems.
Always Validate Peer Certificates from Browser	Controls whether the system requires a browser to present a valid certificate when it tries to connect to the system web interface.
Always Validate Peer Certificates from Server	Controls whether the system requires the remote server to present a valid certificate when connecting to it for services for client-type CSRs, such as provisioning, directory, and SIP. See the following topic for examples.
Installed Certificates	Allows the administrator to either view installed certificates or to add a new certificate.
Signing Request Server	Allows the administrator to create a new server request certificate.
Signing Request Client	Allows the administrator to create a new client request certificate.

Install Certificates

After you have downloaded a CSR and it has been signed by a CA, the resulting certificate is ready to install on the RealPresence Centro system. The following section outlines how to do this, and the procedure is the same to install the client certificate, server certificate, and any required CA-type certificates.

Procedure

1. To open the certificate section, at **Installed Certificates**, click **View and Add**.
2. Next to **Add Certificate**, click **Browse** to search for and select a certificate.

   You might be installing a client or server certificate that has been signed by a CA after having been previously generated as a CSR, or installing a CA certificate needed by the system to validate a certificate it receives from another system.
3. Click **Open**.

   The system checks the certificate data and adds it to the list. If you don't see the certificate in the list, the system was unable to recognize the certificate. This process is sometimes referred to as *installing* a certificate.

   You can select a certificate in the list to view its contents. You can also remove a certificate from the list by clicking **Remove**.
4. If needed, click **Close** to close the certificate section of the screen.
5. Click **Save**.

   When you add a CA certificate to the system, the certificate becomes trusted for the purpose of validating peer certificates.

   Note: If you do not add the server certificate for the system before using the system web interface, you might receive error messages from your browser stating that the security certificate for the web site “Polycom” cannot be verified. Most browsers allow the user to proceed after this warning is displayed. See the Help section of your browser for instructions on how to do this.

Certificate Revocation Settings

When certificate validation is enabled, the RealPresence Centro system tries to validate the peer certificate chain on secure connection attempts for the applicable network services.

Part of the validation process includes a step called revocation checking. This type of check involves consulting with the CA that issued the certificate in question to see whether the certificate is still active or has been revoked for some reason. Revoked certificates are considered invalid because they might have been compromised in some way or improperly issued, or for other similar reasons. The CA is responsible for maintaining the revocation status of every certificate that it issues. The system can check this revocation status by using either of the following methods:

- Certificate revocation lists (CRLs). A CRL is a list of certificates that have been revoked by the CA. A CRL must be installed on the system for each CA whose certificate has been installed on the system.
- The Online Certificate Status Protocol (OCSP). OCSP allows the system to contact an OCSP responder, a network server that provides real-time certificate status through a query/response message exchange.

Note: The systems automatically download CRLs from the Certificate Authorities (CAs) that make CRLs available for retrieval by HTTP. However, for CAs that do not allow HTTP retrieval of CRLs, the system administrator is responsible for manually installing and updating CRLs ahead of their expiration. It is extremely important that CRLs be kept up to date.

Configure the Certificate Revocation List (CRL) Method

You can configure the CRL revocation method settings on the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Certificates** > **Revocation**.
2. Configure these settings on the Revocation screen and click **Save**.

Setting	Description
Revocation Method	To enable the CRL revocation method, select **CRL**.
Allow Incomplete Revocation Checks	When this field is enabled, a certificate in the chain is verified without a revocation status check if no corresponding CRL for the issuing CA is installed. If the system cannot locate an installed CRL, it determines that the certificate is not revoked. If a CRL is installed, the system performs a revocation check when validating the certificate.
Add CRL	• Click **Browse** to search for and select a CRL. • Click **Open** to add the CRL to the list.

3. You can also view automatically and manually downloaded CRLs on this screen.

   To remove a CRL from the list, click **Remove**.

Note: If the **Always Validate Peer Certificates from Browsers** setting is enabled and the expired CRL is for a CA that is part of the trust chain for the client certificate sent by your browser, you can no longer connect to the system web interface because the revocation check always fails. In this case, unless the system web interface can be accessed by a user whose client certificate's trust chain does not include the CA with the expired CRL, you must delete all certificates and CRLS from the system and then reinstall them.

Remove a Certificate and CRL

In some cases, expired certificates or CRLs might prevent you from accessing the RealPresence Centro system web interface. You can use the local interface to reset your system without certificates, to restore access to the system web interface.

Procedure

1. In the local interface, go to **Settings** > **System Information** > **Diagnostics** > **Reset System**.
2. If needed, enter the **Admin ID** and **Password**.
3. Enable the **Delete Certificates** field.
4. Select **Reset System**.

   The system restarts after deleting all installed certificates and CRLs.

Set Up a Security Banner

Security banners consist of text that displays on the Login screen and in a window when you log in remotely to your RealPresence Centro system.

The following is an example of banner text:

```
This machine is the property of Polycom, Inc., and its use is governed by
company guidelines. You have NO right of privacy when using this machine.
```

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Security Banner.**
2. Configure these settings and click **Save**.

Setting	Description
Enable Security Banner	Specifies whether to display a security banner.
Banner Text	**Custom**—Allows you to enter text to use for the banner. **DoD**—Specifies that the system displays a default U.S. Department of Defense security banner. You cannot view or change this text on the local interface, but you can change the text on the system web interface.
Local System Banner Text	If you enable the security banner on the system web interface, enter up to 2,408 single-byte or 1,024 double-byte characters. The text wraps to the next line as you type, but you can press Enter anywhere in a line to force a line break at a specific place.
Remote Access Banner Text	This field is visible only when you use the system web interface. You can type or paste a maximum of 2,408 single-byte or 1,024 double-byte characters. The text wraps to the next line as you type, but you can press Enter anywhere in a line to force a line break at a specific place.

Set a Meeting Password

If you set up a meeting password, users must supply the password to join multipoint calls on the RealPresence Centro system when the call uses the internal multipoint option instead of a bridge.

Remember the following points about meeting passwords:

- Do not set a meeting password if multipoint calls include audio-only endpoints. Audio-only endpoints are unable to participate in password-protected calls.
- Microsoft Office Communicator clients are unable to join password-protected multipoint calls.

- SIP endpoints are unable to connect to password-protected multipoint calls.
- If a meeting password is set for a call, People+Content™ IP clients must enter the password before joining the meeting.
- Meeting passwords cannot contain spaces or be more than 32 characters.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Meeting Password**.
2. Enable and configure the **Meeting Password** setting.

Visual Security Classification

This feature helps the call participants remain conscious of the security classification when in a BroadWorks managed call on the RealPresence Centro system. During and throughout a call, the Visual Security Classification (VSC) provides a visual indication to the system user of the calls security level which is dynamically calculated using the lowest security rating of all users and gateways within the call. During a call, you can override the security classification and assign a lower security classification level.

Keep the following points in mind:

- Each BroadSoft-registered endpoint in the conference has a security classification level.
- BroadSoft Application Server determines the default security classification level for a BroadWorks conference, and that default is the lowest of the levels involved in the conference. VSC is only supported on BroadWorks conferencing systems which are VSC aware and which have visibility of all participants in the call. VSC is not supported on Polycom VMRs, as BroadWorks does not have visibility of the callers on the Polycom MCU.
- The security classification level is shared with all the endpoints that support the Visual Security Classification feature.
- The security classification level of a conference call is re-evaluated whenever an endpoint enters or leaves a conference or when a user modifies the security classification level of an endpoint.

Any user who joins the call from an outside or unknown network is designated an “Unclassified” security classification level.

The Visual Security Classification feature is disabled by default. Enable it with a provisioning server or through the system web interface. Before enabling this feature, ensure the following:

- Register the system to a BroadSoft R20 call server.
- Disable the Multipoint Video Conferencing option key.
- Disable AS-SIP.

Enable Visual Security Classification

You can enable Visual Security Classification on your RealPresence Centro system.

Procedure

1. From the system web interface, navigate to **Admin Settings** > **Security** > **Global Security**.
2. Under Visual Security Classification, select **Enable Visual Security Classification** and click **Save**.
3. Click the **Adjust SIP Settings** link or navigate to **Admin Settings** > **Network** > **IP Network** > **SIP**.
4. Under **Registrar Server Type**, select **Unknown**.

Enable Room and Call Monitoring

Before you can use room and call monitoring, you must enable the feature in the RealPresence Centro system local interface.

Procedure

1. In the local interface, go to ⚙ > **Settings** > **Administration** > **Security** > **Remote Access**.
2. To allow the room or call to be viewed remotely, enable **Allow Video Display on Web**.

Monitor a Room or Call

The monitoring feature in the system web interface allows system administrator to view a call or the room where the system is installed.

Procedure

1. In the system web interface, go to **Utilities** > **Tools** > **Remote Monitoring**.
2. You can perform the following tasks out of a call:
   - To wake the system, click **Wake the system**.
   - To adjust system volume, click **Volume**.
   - To share content, click **Show Content**.
   - To adjust the near camera, click **Near Camera**.
   - To view camera presets, click **Near Camera** or **Far Camera** and click **Presets**.
3. You can perform this additional task in a call:
   - To adjust the far camera, click **Far Camera**.

Send a Message to a System

If you are experiencing difficulties with connectivity or audio, you might want to send a message to the system that you are managing. Only the near-end site can see the message; it is not broadcast to all the sites in the call.

Procedure

1. In the system web interface, go to **Utilities** > **Send a Message**.
2. On the **Send a Message** screen, enter a message (up to 100 characters in length), then click **Send**.

   The message is displayed for 15 seconds on the screen of the system that you are managing.

Configure the OCSP Revocation Method

You can configure the OSCP revocation method settings in the system web interface. For validation of the OCSP response message, if you use OCSP, you might need to install one or more additional CA certificates on the system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Certificates** > **Revocation**.
2. Configure these settings on the Revocation screen and click **Save**.

Setting	Description
Revocation Method	To enable the OSCP revocation method, select **OSCP**.
Allow Incomplete Revocation Checks	When this field is enabled, the system treats the following response from the OCSP responder as a successful revocation check: • If the OCSP responder responds that the status is unknown or if no response is received, the system treats this as a successful revocation check. Regardless of the state of this setting, the following statements apply: • If the OCSP responder indicates a known revoked status, the room system treats this as a revocation check failure and does not allow the connection. • If the OCSP responder indicates a known good status, the room system treats this as a successful revocation check and allows the connection.
Global Responder Address	Specifies the URI of the responder that services OCSP requests, for example, http://responder.example.com/ocsp. This responder is used for all OCSP validation when **Use Responder Specified in Certificate** is disabled, and is sometimes used even when **Use Responder Specified in Certificate** is enabled. Polycom therefore recommends that you always enter a **Global Responder Address** regardless of the value chosen for the **Use Responder Specified in Certificate** setting.
Use Responder Specified in Certificate	In some cases, the certificate itself includes the responder address. When this field is enabled, the system attempts to use the address in the certificate (when present) instead of the **Global Responder Address** specified in the previous field. **Note:** The system supports only the use of HTTP URLs in the AIA field of a certificate when **Use Responder Specified in Certificate** is enabled.

Configuring Call Settings

Topics:

The following topics describe how to configure call settings for your system.

Configure Call Settings

You can configure Call Settings in the system web interface on your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. Configure the settings in the following table.

Setting	Description
Maximum Time in Call	Enter the maximum number of hours allowed for call length. When that time has expired, you see a message asking you if you want to hang up or stay in the call. If you do not answer within one minute, the call automatically disconnects. If you choose to stay in the call at this time, you will not be prompted again. Selecting **Off** removes any limit. This setting also applies when you are viewing the Near video screen or showing content, even if you are not in a call. If the maximum time is reached while viewing Near video, the system automatically returns to the Home screen. If content is being shown, the content stops.

Setting	Description
Auto Answer Point-to-Point Video	Sets the answer mode for when the system is not in a call. This setting has three choices: **Yes**—Instructs the system to automatically answer the incoming point-to-point call. **No**—Instructs the system to force manual answering of the incoming call. **Do Not Disturb**—Instructs the system to reject the incoming call with no notification to the user.
Auto Answer Multipoint Video	Sets the answer mode for when the system is already in a call, regardless of whether the system has multipoint capability. This setting has three choices: **Yes**—Instructs the system to automatically answer the incoming multipoint call. **No**—Instructs the system to force manual answering of the incoming call. **Do Not Disturb**—Instructs the system to reject the incoming call with no notification to the user.
Multipoint Mode	Sets the multipoint viewing mode that applies when the system is the host of a multipoint call. The available settings are as follows: **Auto** **Full Screen** **Discussion** **Presentation**
Display Icons in a Call	Specifies whether to display all on-screen graphics, including icons and help text, during calls.
Enable Flashing Incoming Call Notification	Specifies whether the incoming call notification flashes.

Setting	Description
Preferred 'Place a Call' Navigation	Specifies the default icons that display on the local interface of the Place a Call screen. The available settings are as follows: **Dial Pad**—Displays a list of recently dialed numbers and a dial pad for entering a number to call. **Contacts**—Displays a screen for searching the entire global network directory. The multi-tiered directory (LDAP) root entry displays at the top of the Contacts list. The Contact list combines your search and favorite entries. **Recent Calls**—Lists phone numbers, in chronological order, that have been dialed from the system.
Automatic Self View Control	Specifies whether the **Self View** setting is visible in the local interface. • If **Automatic Self View Control** is enabled, the Self View setting is not displayed in the local interface, and the system automatically chooses when to display the self view window. Whether the self view window is displayed is dependent on available display space, the display mode, and so on. • If **Automatic Self View Control** is not enabled, the user can turn Self View on and off from the local interface.

Setting Call Preferences for SVC

Scalable Video Coding (SVC) conferencing for RealPresence Centro systems provides the following benefits:

- Fewer video resource requirements
- Better error resiliency
- Lower latency
- More flexibility with display layouts

You can make and receive SVC multipoint calls when the system is connected to an SVC-compatible bridge through the Polycom® Distributed Media Application (DMA™). In an SVC-based conference, each SVC-enabled endpoint transmits multiple bit streams, called simulcasting, to the Polycom RealPresence Collaboration Server (RMX). The RealPresence Collaboration Server sends or relays selected video streams to the endpoints without sending the entire video layout. The streams are assembled into a layout by the SVC-enabled endpoints according to each of their different display capabilities and layout configurations.

To make SVC point-to-point calls, the system must be registered to a Skype for Business 2015 server. In a Skype for Business 2015 hosted multipoint or point-to-point call, you can view multiple far-end sites in layouts.

For more information on the features, limitations, and layouts of SVC-based conferencing, refer to the *Polycom RealPresence SVC-Based Conferencing Solutions Deployment Guide* available at Polycom Support.

Configure SVC Dialing Options

Dialing preferences help you manage the network bandwidth used for calls and establish an SVC call configuration on RealPresence Centro systems. You can specify the default and optional call settings for outgoing calls. You can also limit the call speeds of incoming calls.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options**.
2. Configure these settings.

Setting	Description
Scalable Video Coding Preference (H.264)	Specifies whether to use scalable or advanced video coding: • **SVC then AVC**—Use SVC when possible; otherwise, use AVC. • **AVC Only**—This setting disables SVC. This setting is not applicable to Skype-hosted calls, since SVC is negotiated automatically by Skype for Business Server 2015 or the Skype for Business 2015 client.
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this setting if you know that H.239 is supported by the far -end sites you call.
Enable Audio-Only Calls	Specifies one additional outbound audio-only call from the system. This occurs when a multipoint conference call hits the maximum number of calls allowed for the license type.
Video Dialing Order	Specifies how the system places video calls to directory entries that have more than one type of number. • **IP H.323** • **SIP** This setting also specifies how the system places video calls from the Place a Call screen when the call type selection is either unavailable or set to **Auto**. If a call attempt does not connect, the system tries to place the call using the next call type in the list.

Setting	Description
Audio Dialing Order Preference 1	Specifies the first audio preference for calls. The choices are: • **IP H.323** • **SIP** Preference 1 will be attempted first, while Preference 2 will be attempted second.
Audio Dialing Order Preference 2	Specifies the second audio preference for calls. The choices are: • **IP H.323** • **SIP** Preference 2 will be attempted second, while Preference 1 will be attempted first.

Enable SVC Preference (H.264) for Calls

You can enable the order preference for SVC and AVC calls in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options**.
2. From the **Scalable Video Coding Preference (H.264)** list, select **SVC then AVC**.

Enable Automatic Answering of SVC Point-to-Point Calls

A RealPresence Centro system registered to a Skype for Business 2015 server and connected to an SVC-compatible bridge can automatically answer incoming SVC calls. To enable this feature, complete the following tasks on the system:

- Enable Auto Answer Point-to-Point Video
- Enable Scalable Video Coding Preference (H.264)

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. From the **Auto Answer Point-to-Point Video** list, select **Yes**.

Set Preferred Call Speeds

You can configure call speeds in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **Dialing Preference** > **Preferred Speeds**.

2. Configure the following settings.

Setting	Description
Preferred Speed for Placed Calls IP Calls	Determines the speeds to use for IP calls from this system when either of the following statements is true: • The call speed is set to **Auto** on the Place a Call screen • The call is placed from the directory If the far-site system does not support the selected speed, the system automatically negotiates a lower speed. The **SIP (TIP) Calls** setting is available only when the **TIP** setting is enabled.
Maximum Speed for Received Calls IP Calls	Allows you to restrict the bandwidth used when receiving IP calls. If the far site attempts to call the system at a higher speed than selected here, the call is renegotiated at the speed specified in this field.

Configure the Recent Calls List

You can configure a Recent Calls list to display on the Place a Call screen in the RealPresence Centro system web interface. The list includes the following information:

- Site name or number
- Whether call was placed or received
- Date and time

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Recent Calls**.
2. To enable a **Recent Calls** list, configure these settings.

Setting	Description
Call Detail Report	Specifies whether to collect call data for the Call Detail Report. When selected, information about calls can be viewed through the system web interface and downloaded as a .csv file. When this setting is not selected, the system stops writing calls to the report.
Enable Recent Calls	Specifies whether to show **Recent Calls** on the local and system web interfaces.

Setting	Description
Maximum Number to Display	Specifies the maximum number of calls to display in the **Recent Calls** list.

3. To start a new list of recent calls, click **Clear Recent Calls**.
4. Click **Save**.

If you need more details about calls, view or download the Call Detail Report (CDR) from the system web interface.

Set Call Answering Mode

You can configure how your users answer calls when they use the local interface on RealPresence Centro systems.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. Select **Auto Answer Point-to-Point Video** to set the answer mode for calls with one site, or select **Auto Answer Multipoint Video** to set the mode for calls with two or more other sites, and then select one of the following:
   - **Yes**-Answers calls automatically.
   - **No**-Enables users to answer calls manually.
   - **Do Not Disturb**-Disables incoming calls from being processed and routed to the user.

Set the Maximum Call Length

You can set the maximum call length for calls in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. At **Maximum Time in Call**, select a time limit from the drop down list.

Set a Multipoint Viewing Mode

What the far-end site sees during a multipoint call can vary depending on how the RealPresence Centro system is configured, the number of sites participating, the number of monitors being used, and whether content is shared. When you change a layout, you are changing the far-end site layouts only. Video images from multiple sites can be automatically combined on one monitor in a display known as *continuous presence*.

Procedure

1. In the system web interface, select **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. Select a viewing mode from the **Multipoint Mode** list.

The following table describes the available multipoint viewing modes.

Setting	Description
Auto	The view switches between continuous presence and full screen, depending on the interaction between the sites. If multiple sites are talking at the same time, continuous presence is used. If one site speaks uninterrupted for at least 15 seconds, that site appears in full screen on the monitor.
Discussion	Multiple sites are displayed in continuous presence. The current speaker's image is highlighted.
Presentation	The speaker sees continuous presence while the other sites see the speaker in full screen on the monitor.
Full Screen	The site that is speaking is shown in full screen to all other sites. The current speaker sees the previous speaker.

Enable Flashing Incoming Call Alerts

For hearing-impaired users, an attention-getting message displays when an incoming call is received by a RealPresence Centro system. When a call is received, the system displays a message asking if the user wants to answer the call.

For greater visibility, you can have the message text flash between white and yellow. Flashing text is off by default. The incoming call alert settings persists after powering the system off and on.

Procedure

1. In the system web interface, select **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
2. Select the **Enable Flashing Incoming Call Notification** checkbox.

Turn Off Flashing Alerts

You can turn off flashing alerts when the visual cue is not necessary in the RealPresence Centro system web interface.

Procedure

» In the system web interface, select **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.

Clear the **Enable Flashing Incoming Call Notification** checkbox.

Setting Up a Directory

Topics:

- Enable H.323
- Configure the Polycom GDS Directory Server
- Configure the LDAP Directory Server
- Managing Favorites Contacts and Groups
- Setting Up Speed Dial
- Setting Up and Configuring Directory Servers

These topics describe how to manage and configure directory settings in the RealPresence Centro system web interface.

Having groups in the directory can help users find calling information quickly and easily. Polycom systems support global groups and Favorites groups.

Systems support up to 2,000 favorite contacts that users create within Favorites. They can also support one of the following:

- Up to 200 additional contacts with presence, which appear in Favorites, when registered with Skype for Business 2015
- Up to 4,000 contacts from a Polycom GDS server
- An unlimited number of contacts when the system is registered with Skype for Business 2015

Up to 200 Favorites groups that users create within Favorites are supported. If the system is connected to a global directory server, it can also support up to 64 additional groups from the Skype for Business Server 2015, which appear in the Favorites group.

Note: Assistance from Polycom is mandatory for Skype for Business 2015 integrations. For details, please refer to Polycom Collaboration Solutions or contact your local Polycom representative.

Enable H.323

To use GDS in your environment, you must have H.323 enabled and registered on your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **H.323 Settings** and select the checkbox at **Enable IP H.323**.
2. Enter the required registration information as follows.

Setting	Description
Enable IP H.323	Allows the H.323 settings to be displayed and configured.
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The **H.323 Name** is the same as the **System Name**, unless you change it. Your organization's dial plan might define the names you can use.
H.323 Extension (E.164)	Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system. Your organization's dial plan might define the extensions you can use.
Use Gatekeeper	Turn the gatekeeper off or make it automatic.
Require Authentication	Require authentication for IP H.323 connections.
Current Gatekeeper IP Address	The IP address for the current gatekeeper.
Primary Gatekeeper IP Address	The IP address for the primary gatekeeper.

Configure the Polycom GDS Directory Server

You can configure the Polycom GDS Directory Server in the RealPresence Centro system web interface. But first, ensure that H.323 is enabled before you configure the Polycom GDS directory server.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Directory Servers** and select the **Polycom GDS Service Type**.
2. Configure these settings on the Directory Servers screen.

Setting	Description
Server Address	Specifies the IP address or DNS address of the Global Directory Server. You can enter up to five addresses.
Password	Lets you enter the global directory password, if one exists.

Configure the LDAP Directory Server

You can configure the LDAP Directory Server in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Directory Servers** and select the **LDAP Server Type**.
2. Configure these settings on the **Directory Servers** screen.

LDAP Setting	Description
Server Address	Specifies the address of the LDAP directory server. With Automatic Provisioning, this setting is configured by the server and appears as read only.
Server Port	Specifies the port used to connect to the LDAP server. With Automatic Provisioning, this setting is configured by the server and appears as read only.
Base DN (Distinguished Name)	Specifies the top level of the LDAP directory where searches will begin. With Automatic Provisioning, this setting is configured by the server and appears as read only.
Multitiered Directory Default Group DN	Specifies the top level group of the LDAP directory required to access the hierarchical structure. With Automatic Provisioning, this setting is configured by the server and appears as read only.
Authentication Type	Specifies the protocol used for authentication with the LDAP server: NTLM, BASIC, or Anonymous.
Use SSL (Secure Socket Layer)	Enables SSL for securing data flow to and from the LDAP server.
Domain Name	Specifies the domain name for authentication with the LDAP server.
User Name	Specifies the user name for authentication with LDAP server.
Password	Specifies the password for authentication with the LDAP server.

Managing Favorites Contacts and Groups

RealPresence Centro system local interface users can select Contacts from the menu to view favorites and the directory. Users can add favorites from the directory, create new favorite contacts, and create favorite groups.

Types of Favorites Contacts

The RealPresence Centro web system interface displays the following favorite contact types.

Directory Server Registration	Types of Contacts	Presence State Displayed
Polycom GDS	• Directory entries created locally by the user.	Unknown
	• References to Polycom GDS entries added to Favorites by the user. These entries are available only if the system is successfully registered with Polycom GDS. Users can delete these entries from Favorites. Users can copy these entries to other Favorites and remove them from those groups. Users cannot edit these entries.	Online/Offline
LDAP with H.350 or Active Directory	• Directory entries created locally by the user • References to LDAP directory entries added to Favorites by the user. These entries are available only if the system can successfully access the LDAP/Active Directory server. Users can delete these entries from Favorites. Users can copy these entries to other Favorites and remove them from those groups. Users cannot edit these entries.	Unknown
Microsoft	• Skype for Business Server 2015 directory entries are saved as Contacts by the user and stored on the Skype server. Users cannot edit or delete these entries from Favorites using the system. Users can copy these entries to other Favorites and remove them from those groups.	Real-time presence

Create a Favorites Contact

You can create a Favorites contact in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Manage Favorites**.

2. Click **Create New Favorite**.
3. Enter the contact call information and click **Save**.

Create a Favorites Group

You can create a Favorites group in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Manage Favorites**.
2. Click **Create New Group**.
3. Enter a **Name** for the group and click **Save**.

   A success message is displayed.
4. To add contacts to the group, click **Add Contacts** on the success message.
5. Enter a contact name in the search box and click **Search**.
6. In the entry you want to add to the group, click **Add**.
7. Repeat the above steps to add more contacts to the group.
8. Click **Done**.

Edit a Favorites Group

You can edit a Favorites group in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Manage Favorites**.
2. Find the group name in the list of contacts.
3. Next to the group contact name, click **Edit Group**.

   Do one of the following:

   - To add contacts to the group, click **Search to add contacts to this group**, enter a contact name, click **Search,** and then **Add** to add a contact.
   - To remove contacts from a group, next to a contact name, click **Remove**.
4. Repeat the above steps to continue adding or removing contacts.
5. Click **Done.**

Delete a Favorites Group

You can delete a Favorites group in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Manage Favorites**.
2. Next to the group or contact name, click **Delete.**
3. When a message asks you to confirm the delete, select **Delete** or **Cancel**.

Importing and Exporting Favorites

The Import/Export Directory feature enables you to download Favorites from a RealPresence Centro system to local devices, such as computers and tablets, in XML file format. It also allows you to upload Favorites from a device to your system.

- Microsoft Internet Explorer
- Mozilla Firefox

For a list of supported browser versions, refer to the *Polycom RealPresence Centro Release Notes.*

Keep the following points in mind when performing these tasks:

- The size of the uploaded XML file cannot exceed 3 megabytes.
- You can import favorites groups and entries both when you are in a call and when you are not in a call.
- When the uploaded XML file includes favorites groups or entries already on the room system, the duplicate files are added as separate directory entries.

Export Favorites Groups and Contacts

You can export Favorites groups and contacts from a RealPresence Centro system to your local device.

Procedure

1. In the system web interface, go to **Manage Favorites** > **Import/Export** > **Download**.
2. Save the downloaded *directory.xml* file on your local device.

Import Favorites Groups and Contacts

You can import Favorites groups and contacts and upload the directory file to your RealPresence Centro system.

Procedure

1. In the system web interface, go to **Manage Favorites** > **Import/Export** > **Choose File**.
2. In the dialog box, select the *directory.xml* file you want to import and click **Open**.
3. Select **Upload** to upload the directory.xml file to the system.

Setting Up Speed Dial

You use speed dialing to quickly call an IP address designated as a Favorite. Speed Dial contacts are displayed on the RealPresence Centro system's local interface and on a paired RealPresence Touch device.

Enable Speed Dial

You must enable the Speed Dial setting in the RealPresence Centro system web interface before users can use Speed Dial in the local interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **Speed Dial**.
2. Click **Choose Favorites**.
3. Search for contacts that you want to add to **Speed Dial**.
4. Select each contact and click **Add**.
5. After you have selected all of the contacts, click **Save**.

Add Speed Dial Contacts

You can add contacts from the system directory to the Speed Dial contacts list on the RealPresence Centro system's web interface and on a paired RealPresence Touch device.

Procedure

1. In the system web interface at **Speed Dial**, click **Edit**.
2. Enter a contact name and click **Search**.
3. For the contact you want to add, click **Add**.
4. To save your changes, click **Save**.

Image File Requirements for Speed Dial Contacts

You can upload a photo or graphic for contacts in the Speed Dial list for the RealPresence Centro system and for a paired RealPresence Touch device. Note the following requirements for Speed Dial images:

- JPEG format (.jpg or .jpeg extension)
- Image dimensions within a range of 300 to 2000 pixels (both width and height)
- File size less than 5 MB

Upload an Image File for Speed Dial Contacts

You can upload a photo or graphic for contacts in the Speed Dial list on your RealPresence Centro system web interface.

Procedure

1. In the system web interface at **Speed Dial**, click **Edit**.
2. Click **Choose File**, navigate to the file, and click **Open** and **Upload**.
3. To save your changes, click **Save**.

   The image is now displayed for the Speed Dial contact on the system Home screen and on a paired RealPresence Touch.

Remove Speed Dial Contacts

You can remove contacts from the Speed Dial list in the RealPresence Centro system web interface.

Procedure

1. In the system web interface at **Speed Dial**, click **Edit**.
2. For the contact you want to delete, click **Remove**.
3. To save your changes, click **Save**.

Setting Up and Configuring Directory Servers

The global directory provides a list of RealPresence Centro systems that are registered with the Global Directory Server and are available for calls. The other systems appear in the directory, allowing users to place calls to participants by selecting their names.

Configuring a Directory Server

You can configure the RealPresence Centro system to use one of the following directory servers in standard operating mode.

Directory Servers Supported	Authentication Protocols	Global Directory Groups	Entry Calling Information
Microsoft Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: • SIP address (SIP URI)
LDAP with H.350 or Active Directory	Any of the following: • NTLM v2 only • Basic • Anonymous	Not Supported	Might include: • H.323 IP address (raw IPv4 address, DNS name, H.323 dialed digits, H. 323 ID, or H.323 extension) • SIP address (SIP URI) • ISDN number • Phone number*
Polycom GDS	Proprietary	Not Supported	Might include: • H.323 IP address (raw IPv4 address, DNS name, or H.323 extension) • ISDN number

* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats:

- +Country Code.Area Code.Number
- +Country Code.(National Direct Dial Prefix).Area Code.Number

You can configure the system to use the following directory server when the system is automatically provisioned by a RealPresence Resource Manager system.

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: • SIP address (SIP URI)

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats: • +Country Code.Area Code.Number • +Country Code.(National Direct Dial Prefix).Area Code.Number			

Configuring Audio Settings

Topics:

- Configure General Audio Settings
- Configure Audio Input Settings
- Test StereoSurround
- Acoustic Fence Technology
- USB Headset Support

Configure General Audio Settings

You can configure audio settings in the RealPresence Centro system web interface. Some audio settings are unavailable when a SoundStructure digital mixer is connected to a Polycom video conferencing system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio**.
2. At **General Audio Settings**, configure the Audio settings described in the following table.

Setting	Description
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.
Ringtone	Specifies the ring tone used for incoming calls.
User Alert Tones	Specifies the tone used for user alerts.
Audio Mute auto-answered Calls	Specifies whether to mute incoming calls. Incoming calls are muted until you press the Mute button on the microphone or on the remote control. **Note:** You must first enable **Auto Answer Point-to-Point Video** or **Auto Answer Multipoint Video**. These settings are in **Admin Settings** > **General Settings** > **System Settings** > **Call Settings**.
Enable Keyboard Noise Reduction and Polycom NoiseBlock™	Specifies whether the system mutes audio from the connected microphones when keyboard tapping sounds or other extraneous noises are detected, but no one is talking. NoiseBlock unmutes the system when speech is detected, regardless of the existence of background noise. Note: Polycom MusicMode™ is disabled when this setting is enabled. If an external echo canceller is used, keyboard noise reduction is not available.

Setting	Description
Transmission Audio Gain (dB)	Specifies the audio level, in decibels, at which to transmit sound. Unless otherwise advised, Polycom suggests setting this value to 0 dB.
Enable Audio Mute Reminder	Specifies whether to display a notification as a reminder to unmute the connected microphone when speaking is detected.
Enable Join and Leave Tones	Plays an audible tone when a participant in a multipoint call joins or leaves the call. Note: This setting is available only when the multipoint option key is installed.
Enable Acoustic Fence	Specifies whether Acoustic Fence can be used or not.
Acoustic Fence Sensitivity	Specifies the microphone sensitivity for Acoustic Fence Technology. You can set a value between 0 and 10, where 0 is the minimum sensitivity and 10 is the maximum sensitivity. Higher settings increase the radius of the fence area around the primary microphone.

Configure Audio Input Settings

You can configure audio input settings for your RealPresence Centro system type.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio** > **Audio Input**.
2. Configure the audio settings.

The RealPresence Centro system audio input settings are described in the following table.

Setting	Description
Type	Displays the 3.5mm connector for line-level stereo audio input.
Audio Input Level	Sets the 3.5 mm audio input level.
Associate with Video Content Ports	When enabled, the 3.5 mm audio input is only heard when the VGA or HDMI content video port is active. When disabled, audio is not controlled by content video port activities.
Type	Displays embedded audio from the HDMI connector.
Audio Input Level	Sets the audio input level.

Setting	Description
Audio Meter	Displays the audio level for the HDMI input port, left and right channels.

3.5mm Audio Input

You can select how to enable 3.5mm audio input from the RealPresence Centro system 3.5mm audio port in the system web interface.

In active calls, you can enable 3.5mm audio input on the near-end conference site. After you enable audio 3.5mm input for use during active calls, 3.5mm audio input is heard during active calls from the system speakers and from all far-end sites.

If you enable 3.5mm audio input for use when content sharing is active, 3.5mm audio input is only active when either HDMI or VGA video input is active.

When HDMI or VGA video input is active and the system is in an active call, 3.5mm audio input is heard from the system speakers and from all far-end sites. If audio is part of active HDMI or VGA content, the 3.5mm audio input mixes in with the HDMI or VGA audio input.

Test StereoSurround

After you configure the system to use Polycom StereoSurround, test the system configuration and place a test call.

Procedure

1. Make sure the microphones are positioned correctly.
2. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio** > **Audio Input**.
3. Gently blow on the left leg and right leg of each Polycom microphone while watching the bar meters to identify the left and right inputs.
4. Test the speakers to check volume and verify that audio cables are connected.

   If the system is in a call, the far site hears the tone.

   Exchange the right and left speakers if they are reversed.

   Adjust the volume control on your external audio amplifier so that the test tone sounds as loud as a person speaking in the room. If you use a Sound Pressure Level (SPL) meter, it should measure about 80-90 dBA in the middle of the room.
5. Repeat the steps above for **Admin Settings** > **Audio/Video** > **Audio** > **Audio Output**.

Acoustic Fence Technology

Polycom® Acoustic Fence Technology™ uses standard Polycom microphone arrays to build a virtual fence around a user or multiple users. The audio is automatically muted when all sounds originate outside a boundary. If a speaker is talking inside the fence, the volume is not altered, but sounds outside the fence are lowered by 12 dB. Once the speaker leaves the fenced area, the audio is muted.

In addition to the primary Polycom microphone array, one or more fence microphone arrays are required. You can use up to 3 ceiling microphones with the RealPresence Centro system.

The boundary radius can be two feet to several feet around the following Polycom peripherals:

- Polycom microphone array
- Desktop microphones
- Ceiling microphones
- Polycom® EagleEye Acoustic camera

This feature works in mono mode only. If StereoSurround is enabled when you enable the Acoustic Fence feature, a notification is displayed. “Enabling Acoustic Fence will disable Polycom StereoSurround.”

Configure the Acoustic Fence

Before you can use the Acoustic Fence, you must configure settings in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio**.
2. Select the **Enable Acoustic Fence** checkbox.
3. Set **Acoustic Fence Sensitivity** from 0 to 10, where 0 is the minimum microphone sensitivity and 10 is the maximum microphone sensitivity.

   Higher values increase the radius of the fence area around the primary microphone.

For more details on the setup and the associated scenarios, search the Polycom Knowledgebase for "acoustic fence" and a white paper is listed at http://support.polycom.com/PolycomService/knowledgebase/search.htm.

USB Headset Support

USB headsets, Bluetooth headsets with USB adapters, are supported as audio input/output devices with RealPresence Centro systems. The headset functions automatically without any required configuration or intervention. After verifying the headset hardware and software is supported, plug in the headset to an available USB port on the system, or enable pairing mode and plug in the USB adapter.

You can hear and control audio on your device while your headset is connected to the system. The USB headset audio controls do not change the system audio functions such as mute or volume control.

Only a single headset can connect to the system at one time. Once connected, the headset is used as the primary audio input and output device for the system. Headsets with these sampling rates are supported: 8 kHz, 16 kHz, 24 kHz, 32 kHz or 48 kHz.

The USB 2.0 ports support USB headsets.

For a list of supported headsets, refer to the *Polycom RealPresence Centro Release Notes* at Polycom Support.

Configuring Video Settings

Topics:

The following topics describe how to configure video settings in the system web interface.

Maximize HDTV Video Display

When you use a television as your monitor, some HDTV settings might interfere with the video display or quality of your calls. To avoid this potential problem, disable all audio enhancements in the HDTV menu, such as SurroundSound.

In addition, many HDTVs have a low-latency mode called Game Mode, which could lower video and audio latency. Although Game Mode is typically turned off by default, you might have a better experience if you turn it on.

Before attaching your RealPresence Centro system to a TV monitor, ensure the monitor is configured to display all available pixels. This setting, also known as “fit to screen” or “dot by dot,” enables the entire HD image to be displayed. The specific name of the monitor setting varies by manufacturer.

Monitor Profiles

Monitor Profiles set the preferences for which video layout panel views are shown on each monitor connected to the system. You can customize the monitor configuration to match your environment or your desired meeting experience. The Monitor Profile settings are just preferences. What you see can vary depending on layout panel views, whether content is being shown, the number of active monitors, and so on.

The layout view names provide hints on the priority of the panels. So, for example in the **Content, then Far, then Near** layout view, the system displays the panels in this order: Content first, then any remote speakers (Far), then the local camera (Near). The panel that is listed first is the largest panel. In this example, the Content panel is larger than the far or the near panels.

The RealPresence Centro system supports the following number of panels in the layouts:

- Number of Panels in the Internal MCU Layouts: 6 (all participants are displayed)
- Number of Panels in the Far-End Site Layouts: 4 (Up to 4 latest speakers)

Configure Monitor Profile Settings

You can configure monitor layout profile settings for each of the four monitors on the RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors** > **Monitor Profile**.
2. For each monitor connected to the system, you can configure the following settings.

Monitor Profile Name	Description	Monitor 1	Monitor 2
Content, then Far, then Near	Sets Monitor 1 or 2 to share content. The system displays the panels in this order of priority: Content first in the largest panel, then any remote speakers (Far), then the local camera (Near). Default for Monitor 1 if only one monitor is connected to the system. Default for Monitor 2 if 2 monitors are connected to the system.	Yes	Yes
Far, then Near	Sets Monitor 1 or 2 to show the far-end in the largest panel, then the near-end. Default for Monitor 1 if there are 2 or more monitors connected to the system.	Yes	Yes
Far Only	Sets Monitor 1 or 2 to show the far-end only.	Yes	Yes
Content, then Near	Sets Monitor 2 to display shared content in the larger panel. If no content is displayed, the monitor shows the person speaking at the near-end.	No	Yes

Monitor Profile Name	Description	Monitor 1	Monitor 2
Content, then Far	Sets Monitor 1 or 2 to display shared content in the larger panel. If no content is shared, the monitor displays the far-end speaker panel only.	Yes	Yes
Content Only	Sets Monitor 2 to display shared content as the only panel. If no content is shared, the monitor shows the room background.	No	Yes
Far, then Content, then Near	Sets Monitors 1 or 2 to share content. The system displays the panels in this order of priority: remote speakers first (Far), then any content in the largest panel, and then the local camera (Near).	Yes	No
Near Only	Sets Monitor 2 to show the near-end site only. Another name for this view is Self View.	No	Yes

The Automatic Self View setting can also affect what displays on the monitors.

Configure Call Settings

Prevent Monitor Burn-In

You can configure when you want a system to go to sleep after a period of inactivity. Monitors and systems provide display settings to help prevent image burn-in. Plasma televisions can be particularly vulnerable to this problem. Refer to your monitor's documentation or manufacturer for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Ensure that static images are not displayed for long periods.
- Set the **Time before system goes to sleep** to 60 minutes or less.
- To keep the screen clear of static images during a call, disable the following settings:
  - **Display Icons in a Call** (**Admin Settings** > **General Settings** > **System Settings** > **Call Settings**)
  - **Show Time in Call** (**Admin Settings** > **General Settings** > **Date and Time** > **Time in Call**)
- Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Sleep**.
2. At **Display**, select whether you want to display black video or a no signal message.
3. At **Time Before System Goes to Sleep**, select the number of minutes the system can be idle before it goes to sleep.
4. At **Enable Mic Mute in Sleep Mode**, select this checkbox to mute the system microphone during sleep mode.

Adjust Brightness for Room Lighting

In certain environments, bright content from displays, windows, or light fixtures can cause the camera's autoexposure setting to darken the exposure beyond what is preferred. To remedy the issue, you can optimize the highlights and lowlights using the **Brightness** setting.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs** > **[Input Name]Brightness**.
2. Set **Brightness**to the minimum value.
3. Move the camera so that only a few very dark portions are shown; include at least one portion with an acceptable exposure.
4. If the setting needs more adjustment, increase the value at slight intervals.

CEC Monitor Controls

Consumer Electronics Control (CEC) monitor controls allow administrators to wake up monitors and place the system on standby for power saving. You can enable CEC on external monitors connected via HDMI, if they support the CEC protocol.

The following CEC features are available:

- **One Touch Play**-Use the system remote to wake up the monitors. All connected CEC-capable monitors are powered on, and their displays are switched to room system input.
- **System Standby**-When the room system enters sleep mode, all connected CEC-capable monitors are switched to standby mode for power saving. When waking up, the monitors are powered up before they display system video.

Note the following points about using CEC controls with Polycom systems:

- If you connect to the monitor with an HDMI splitter, ensure the HDMI splitter is CEC-capable. Due to HDMI splitter limitations, monitors behind a 1xM (one-input multiple-output) HDMI splitter powers on, but might not switch to the correct input when it wakes up.
- The system does not respond to CEC commands issued by a television remote control.
- If a CEC-capable monitor is connected to a room system and another endpoint, the monitor displays the active endpoint when the system is in standby mode.

CEC functionality is enabled by default on the four primary monitors of RealPresence Centro systems. Any monitors connected externally to the system must also support CEC, so that the feature can operate with the system. Not all HDMI monitors support CEC commands. Refer to the following list of CEC-enabled monitors: CEC-XBMC

To verify that CEC is enabled, navigate to your monitor CEC settings. Many monitors also have sub-feature settings under the main CEC setting that control whether or not the monitor responds to CEC commands. For example, CEC Auto Power Off controls whether or not the monitor powers off when receiving a CEC standby command. Make sure to enable all CEC sub-features.

Each monitor brand might have different CEC feature and sub-feature settings. Ensure that all monitors connected to the system are all enabled for CEC.

Note that on the HDMI channel, the system is identified as Polycom.

Enable CEC Controls

You can enable CEC settings in the system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors** > **Consumer Electronics Control**.
2. At **Enable Consumer Electronics Control**, select the checkbox.

Disable CEC Controls

You can disable CEC settings in the system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors** > **Consumer Electronics Control**.
2. At **Enable Consumer Electronics Control**, clear the checkbox.

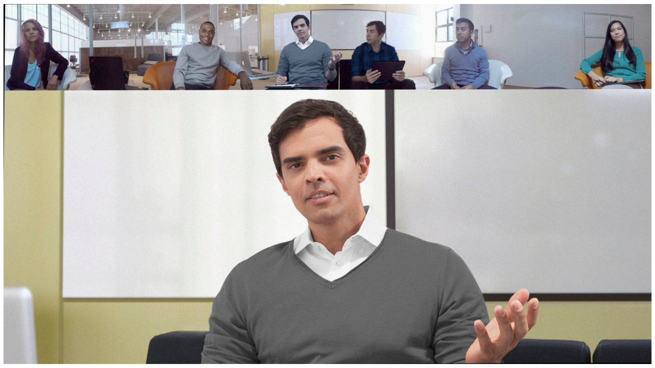
Panoramic Video Layout for RealPresence Centro Systems

By default, the 360-degree high definition panoramic camera is designed to provide an enhanced video collaboration experience where the camera captures every room participant in a panoramic filmstrip while focusing on the active speaker.

The panoramic filmstrip can either display at the top of the screen, the bottom, alternating between the top or bottom depending on the position of the speaker, or not at all.

The following figure shows the active speaker with the panoramic view of all in-room participants at the top of the screen.

Panoramic filmstrip and active speaker view



Video Input Settings for RealPresence Centro Systems

Settings for each video input connected to your RealPresence Centro system are available in the system web interface at **Admin Settings** > **Audio/Video** > **Video Inputs**. Settings that don't apply to the selected video input are not displayed. For example, if a specific camera is not connected to your room system, the related settings are not displayed.

Configure Video Input Settings

You might need to configure video input settings for your RealPresence Centro system.

Procedure

» Configure the following video input settings for the system.

Input 1: Panoramic Camera

Setting	Description
Model	Displays the device name using the video input port (read only)
Optimized for	Specifies **Motion** or **Sharpness** for the video input. • **Motion**—This setting is for showing people or other video with motion. • **Sharpness**—The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is required for HD calls between 512 kbps and 2 Mbps.
Brightness	Specifies the adjustment for a bright background. This setting is best used in situations where the subject appears darker than the background.

Setting	Description
Panoramic Overlay	Determines where the panoramic filmstrip displays for the far-end site during calls. The default is Automatic. • **Automatic** - The filmstrip moves automatically depending upon the position of the speaker. For example, the filmstrip displays at the top of the screen by default, but if the speaker stands up, the filmstrip moves to the bottom of the screen. • **Off** - The filmstrip does not display. • **Top** - The filmstrip always displays at the top of the screen. • **Bottom** - The filmstrip always displays at the bottom of the screen.
Camera Head Position Mode	Determines the camera position in and out of a call. The default is Automatic. • **Automatic** - The camera automatically moves up during calls or when Self View is shown; out of a call, it automatically moves down. • **Up** - The camera is always up regardless of controls, except when the system is powered off or has restarted. • **Up (Sleep Mode)** - The camera is always up except when in sleep mode, the system is off, or the system has restarted.
Camera Head Position Timeout (seconds)	Determines when the camera moves down (goes to sleep) after it is no longer in use. The default is 120 seconds.

Input 2: Content Camera

Setting	Description
Enable	Specifies the video input type as HDMI or VGA. Choose **Auto** to automatically select the video input type.
Name	Displays the default name of the video input. You can also enter your own name for the device.

Setting	Description
Display as	Specifies whether the video input is to be used for **People** or **Content**. The selection you make determines the available settings for the device in the embedded interface. For example, a People source has settings for PTZ and near/far camera control, but a Content source has different settings.
Input Format	Specifies the source type of the device. This setting is read only unless the system does not detect the device.
Optimized for	Specifies **Motion** or **Sharpness** for the video input. • **Motion**—This setting is for showing people or other video with motion. • **Sharpness**—The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is required for HD calls between 512 kbps and 2 Mbps.

Configure RS-232 Serial Port Settings

You can configure RS-232 serial port settings in the system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Serial Ports**.
2. Configure the following settings in the sections on the **Serial Ports** screen.

Setting	Description
RS-232 Mode	Specifies the mode used for the serial port. Available settings depend on the system model. • **Off**—Disables the serial port. • **Pass Thru**—Passes data to an RS-232 device, such as a serial printer or certain types of medical devices, connected to the serial port of the far-site system. Only available in point-to-point calls. • **Closed Caption**—Receives closed captions from a dial-up modem or a stenographer machine through the RS-232 port. • **Camera Control**—Passes data to and from a third-party camera. • **Control**—Receives control signals from a touch-panel control. Allows any device connected to the RS-232 port to control the system using API commands.
Baud Rate, Parity, Data Bits, Stop Bits	Set these to the same values that they are set to on the serial device.
RS-232 Flow Control	This setting works with RS-232 modes that are not currently available. The setting is not currently configurable.
Login Mode	Specifies the credentials necessary for a control system to connect to the RS-232 port. • **Admin password only**—Requires the admin password, if one has been set, when the control system connects. (default) • **Username/Password**—Requires the user name and the admin password, if one has been set, when the control system connects. • **None**—No user name or password is required when the control system connects. **Note:** This setting only displays when RS-232 Mode is set to **Control**.

Configuring Monitor Settings

You cannot configure the 4 main monitors, but can configure an external monitor. To display content, the system supports a maximum of one external monitor that can be connected at a time.

Note: Ensure that the system is powered off before you connect any devices.

Configure Secondary Monitors for Content

If you have a multiple monitor setup with more than one touch monitor, and you want to use touch to control content on secondary monitors, you must configure settings on both the local and system web interfaces. The primary touch monitor is the one that you use to control the system's local interface. Secondary monitors are any additional monitors connected to the system. If only one touch monitor is connected to the system, the following configuration steps are not necessary.

Procedure

1. In the local interface, use a remote control to navigate to ⚙ **Settings** > **Administration** > **Touch Monitor** > **Configure**.
2. Under **Enable touch interaction on this monitor**, click **Start**.
3. Click the screen on the area indicated.

   The system recognizes the monitor as a touch monitor.
4. In the system's web interface, go to **Admin Settings** > **Audio/Video** > **Monitors**.
5. For Monitor 1 at **Enable**, select **Auto** or **Manual**.

   At **Monitor Profile**, select **Far, Then Near or Far Only**.
6. For Monitor 2, at **Monitor Profile**, select **Content Only** or one of the other content profiles.

   If you have 3 monitors, follow the steps above for monitors 1 and 2 and select **Far Only, Content Only**, or **Near Only** for monitor 3.

   Now you can use the primary monitor to control the system's local interface, and a secondary monitor to show content.

Configuring a Camera or Camera Control System

Topics:

- Configure Camera Settings
- Setting Up a Polycom EagleEye IV Camera
- Setting Up a Polycom EagleEye Producer System
- Polycom EagleEye Director II Camera System
- Set Up the Polycom EagleEye Director
- RealPresence Centro System Camera
- Camera Presets

If you connect a supported PTZ camera, the system detects the camera type and sets the appropriate configuration. Ensure that the system is powered off before you connect devices to it.

All Polycom cameras can receive IR signals. RealPresence Centro systems have built-in IR receivers to receive signals from the remote control. Point the remote control at the system or your Polycom camera to control it.

The system can provide power to the EagleEye III and EagleEye IV cameras through an HDCI connector. The cameras do not require any additional power supply or IR extender.

If the camera IR is the only exposed IR and you normally power the system on and off with the remote control, use one of these solutions:

- Provide direct power to the EagleEye III or EagleEye IV camera with the elective EagleEye camera power supply, 1465-52748-040. This allows the IR sensor to remain powered on, so that the camera is capable of receiving IR commands from the remote control.
- Position the system so that the IR receiver on the front of the system has a line-of-sight to the remote control.
- Use a third-party IR extender to extend the IR signal from the room to the IR receiver on the front of the system.

Sleep and wake states are supported, where the system provides power to the EagleEye IV or EagleEye III camera. This allows the cameras to wake from a Sleep state through a signal received by the camera's IR sensor. The camera does not require any additional power supply or IR extender.

Configure Camera Settings

You can configure camera settings for cameras connected to your system. Although you can connect devices that are not automatically discovered, the available choices in the interface might not be the same as they would for automatically discovered devices. For example, if you connect an unsupported camera, the system attempts to show video. Polycom does not guarantee that the results will be optimal or that you can set up the camera the same as for a supported camera.

Procedure

» In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**.

Configure the following settings as needed:

Setting	Description
Power Frequency	Specifies the power line frequency for your system. In most cases, the system defaults to the correct power line frequency, based on the video standard used in the country where the system is located. This setting allows you to adapt the system in areas where the power line frequency does not match the video standard used. You might need to change this setting to avoid flicker from the fluorescent lights in your conference room.
Make This Camera Your Main Camera	Specifies which is the primary camera. You specify the main camera when you set up the RealPresence Centro system, but you can also change the selection here. Input 1 is the panoramic camera and input 2 is the content camera.
Enable People+ContentIP™	Enables the ability to use the People+Content IP application.
Enable Camera Preset Snapshot Icons	Enables the use of snapshot icons that represent camera preset configurations. The default setting is controlled by the Security Profile, but you can change the default here. If you change your security profile setting from **Low** or **Medium** to **High** or **Maximum**, or if you disable the setting, the system replaces each preset image with a blue, striped box. Presets that have not been configured show as empty rectangles. When you disable the **Enable Camera Preset Snapshot Icons** setting in the system web interface, the blue, striped boxes in the local interface show you which presets are configured, but enabling the setting does not redisplay the snapshot icons. You can see snapshot icons that represent preset configuration images only when you configure a preset with the **Enable Camera Preset Snapshot Icons** setting enabled.

Setting	Description
Camera Sleep Mode	Specifies a sleep mode for your camera. **Fast Wake Up**: Provides an image from the camera as soon as the monitor is awake. In a sleep condition, the camera faces forward and has power so that it is held in that position. Set the **Sleep Display** mode to **Black** for a quicker video image on the display, but be aware that this mode uses maximum power. Setting the **Sleep Display** mode to **No Signal** requires the display to synchronize with the video output; this can take a few seconds, but depending upon the monitor, this could conserve energy, since this is low power mode. **Save Energy**: Removes power from the camera; it spins to the rear and faces down, but the camera can still move. When the **Sleep Display** mode is set to **No Signal**, by the time the display synchronizes with the system, the camera is sending an image. When **Sleep Display** mode is set to **Black**, it takes a few seconds for the camera to send an image. **Save Energy** applies only when a camera is connected to the system, but not when the EagleEye Producer or EagleEye Director is connected to the system.

Setting Up a Polycom EagleEye IV Camera

The Polycom EagleEye IV cameras are digital with a 4k sensor that is specifically designed to work with RealPresence Centro systems. These cameras have an available privacy cover, wide-angle lens, and digital extender.

For information about setting up these cameras, refer to *Installing the Polycom EagleEye IV Wide Angle Lens*, *Setting Up the Polycom EagleEye IV Cameras*, *Setting Up the Polycom EagleEye IV Camera Privacy Cover*, and *Setting Up the Polycom EagleEye Digital Extender* which are available at Polycom Support.

EagleEye IV Camera Orientation

After you have connected your EagleEye IV camera, you might want to change the camera's orientation.

EagleEye IV cameras can be mounted upside down to accommodate special video conferencing situations. The orientation of the video display and pan/tilt functions work transparently so that the inverted position is transparent to end users. The default orientation is normal, or not inverted.

Enable an Inverted Camera Position for the EagleEye IV Camera

You might want to invert the EagleEye IV camera in your environment.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**, and choose **EagleEye IV camera**.

2. At **Orientation**, select **Inverted** and click **Save**.

Enable a Normal Camera Position

You might want to disable the inverted camera position in your environment.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**, and choose **EagleEye IV camera**.
2. At Orientation, select **Normal** and click **Save**.

Setting Up a Polycom EagleEye Producer System

The Polycom® EagleEye™ Producer system is an add-on for the EagleEye cameras that enables participant counting. Position the EagleEye Producer system on a level surface, ideally on top of a monitor. You can mount the Polycom® EagleEye™ III, the Polycom® EagleEye™ IV and the Polycom® EagleEye™ Director cameras on top of the EagleEye Producer.

The EagleEye Producer system is a camera-peripheral technology that works with Polycom® EagleEye™ III and IV cameras to provide room framing and participant counting. Using facial recognition technology, the device continually scans the room and commands the movable camera to pan, tilt, and zoom. EagleEye IV cameras are available with either 4x or 12x zoom capability. The EagleEye Producer includes a ‘bunk bed' mount for use with the universal camera mounting solution. Available accessories include the EagleEye Digital Extender and the Digital Breakout Adapter.

Ensure that the EagleEye Producer field of view includes the all conference participants. For more information on positioning the EagleEye Producer refer to the *Set Up the Polycom Eagle Eye Producer* document on Polycom Support.

Information on required cables and how to set up EagleEye Producer are included in *Set Up the Polycom EagleEye Producer.*

You can connect one EagleEye Producer to a RealPresence Centro system at a time. Multiple EagleEye Producer connections are not supported.

Calibration

The EagleEye Producer internal camera is aligned with the EagleEye camera. If the alignment changes, group framing is not accurate.

Automatically Calibrate the Room View

Deviations in tracking results can occur when the EagleEye Producer is being installed or moved. In these instances, EagleEye Producer attempts to perform automatic calibration by automatically detecting deviations and adjusting itself to display the best views. To automatically calibrate the room view, no movement can be detected during the calibration period.

Procedure

1. From the RealPresence Centro system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs** > **General Camera Settings** and select the input used by the EagleEye Producer.

   Select the **Automatic Image Calibration** checkbox.
2. Enable **Tracking**.

3. Have one person sit so they are framed in a webcam view.

Manually Calibrate

You can realign the EagleEye Producer camera and EagleEye camera to display the best view of the room for group framing by manually calibrating the room view.

Note: If you are using a touch panel, you need a RealPresence Centro remote control to manually calibrate the room view.

Before you manually calibrate the room view ensure that the EagleEye camera is properly attached to the EagleEye Producer as shown in *Set Up the Polycom EagleEye Producer*.

Procedure

1. Ensure that the **Make This Camera Your Main Camera** video input setting in administration settings in the Group system web interface specifies the EagleEye Producer as the main camera.
2. Turn **Self View** on in the local interface of the system to view the room in the self view window.
3. Press the **Home** ⌂ button on the system remote control for five seconds to get to the Home screen.

   The EagleEye Producer LED changes to a fast blue blink when on the Home screen.
4. Press the **Up** and **Down** arrow buttons on the remote control to align the webcam with the EagleEye camera to show the best room view when group framing.
5. To exit the Home screen, press any key on the remote control except the **Up** or **Down** arrow button.

   If no action is taken for five seconds, the system will automatically the Home screen. The LED turns to blue.

Camera Tracking

The Polycom EagleEye Producer detects the people in the room and provides framing during a conference. Frame Speaker with a Normal tracking speed and Medium view is enabled by default. When an EagleEye Producer is connected to a RealPresence Centro system, camera tracking starts automatically when you initiate a call and stops automatically when you hang up from a call. You can also manually start camera tracking in the local interface of the system. EagleEye Producer detects the people in the room and sets up framing. You can set the tracking mode and speed, and specify the type of group framing, which enables automatic tracking of group participants in the room and frames the active speaker.

Polycom recommends calibrating the Polycom EagleEye Producer before adjusting camera features. For instructions on how to calibrate the Polycom EagleEye Producer, refer to the *Polycom RealPresence EagleEye Producer User Guide* at Polycom Support.

Change Camera Tracking Settings

You can change camera tracking settings in the system web interface.

- In the system web interface of the RealPresence Centro system, go to **Admin Settings** > **Audio/ Video** > **Video Inputs** > **General Camera Settings** and select the input used by the Polycom EagleEye Producer.

  Configure the following settings.

Enable Camera Tracking

You can enable EagleEye Producer camera tracking in the local interface. If camera tracking is enabled, when you start a call, camera tracking starts automatically; when you end a call, camera tracking stops automatically and group framing is disabled.

Procedure

» In the local interface of the RealPresence Centro system, go to **Camera** and select **Camera Tracking On**.

Disable Camera Tracking

You can disable camera tracking in the local interface.

Procedure

» In the local interface of the RealPresence Centro system, go to **Camera** and select **Camera Tracking Off**.

Change the EagleEye Camera

You can change the EagleEye camera attached to the EagleEye Producer to another EagleEye camera. You must power off the EagleEye Producer before changing cameras.

Procedure

1. Power off the EagleEye Producer.
2. Disconnect and remove the existing EagleEye camera.
3. Connect in the new EagleEye camera.

   For information about how to connect an EagleEye camera, see the *Set Up the Polycom EagleEye Producer*.
4. Power on the EagleEye Producer.

Update EagleEye Producer Software

Updates to the EagleEye Producer software are included with RealPresence Centro system software updates. No license number or key code is required to update the EagleEye Producer. Software for an EagleEye IV camera is automatically updated when the camera is attached to the system with an EagleEye Producer.

Procedure

» Connect the EagleEye Producer to the system.

The system detects the EagleEye Producer and updates it, if necessary.

Update the EagleEye Producer System Image

If you are unable to automatically update the EagleEye Producer system software by connecting to a RealPresence Centro system, you can update EagleEye Producer system manually by updating the system image.

To update the EagleEye Producer system image, use a USB device with at least 200MB of space and make sure the USB file system is in FAT32 format to perform a full system update.

Note: Do not unplug the USB drive during the update process.

Procedure

1. Create a folder named `plcm-eep-cmd` in the USB root directory.
2. Create a subfolder named `update` in the `plcm-eep-cmd` folder.
3. Copy the EagleEye Producer update image (`polycom-eagleeyeproducer-xxx-1.0.0.xx-xxxx.img`) into the `update` folder.
4. Plug in the EagleEye Producer power cable to power it on and allow it to fully boot up.

   The LED turns solid blue.
5. Plug the USB drive into EagleEye Producer.

   The LED blinks amber and then turns solid blue in a few seconds.
6. Unplug the EagleEye Producer power cable, but leave the USB drive plugged in.
7. Plug in the EagleEye Producer power cable and allow it to boot up.

   The LED turns solid blue. The EagleEye Producer starts the image update and the LED blinks blue and amber. The image update takes approximately ten minutes to complete. The EagleEye Producer automatically reboots when the image update is complete. The camera tilts up and then down during the reboot and the LED returns to solid blue.
8. Remove the USB drive.

   The update log is saved in `[USB root directory]/eepout/[EEP SN]/log`.

EagleEye Producer Indicator Lights

A light-emitting diode (LED) is integrated into the front of the EagleEye Producer device. These LED lights emit colors that refer to various system states and allow you to identify the current state for the EagleEye Producer system. Detailed LED and system states mappings are shown in the following table.

Download System Logs and Configurations

EagleEye Producer system logs and configurations are not uploaded to RealPresence Centro. You must use an empty USB drive and make sure the USB file is in FAT32 format to download the EagleEye Producer system logs and configurations. You can use logs and configurations to troubleshoot EagleEye Producer system software issues.

Procedure

1. Create a folder named `plcm-eep-cmd` in the USB root directory.
2. Create a subfolder named `log` in the `plcm-eep-cmd` folder.
3. Create a blank text file named `downloadlogflg` in the `log` folder.
4. Plug the USB drive into the EagleEye Producer.

   The LED blinks amber and then turns solid blue.
5. Remove the USB drive.

   The downloaded files are located in the following locations.

   - The application logs and system information are in the `[USB root directory]/eepout/[EEP SN]/log/` folder.

- Configuration files are in the `[USB root directory]/eepout/[EEP SN]/config/` folder.
- The system current running status is recorded in a file called `sysstatus` and is in the `[USB root directory]/eepout/[EEP SN]/` folder. The system status file includes current CPU/memory usage and current running process information.

Participant Count CDR Details

When used with a RealPresence Centro system and an EagleEye camera, the camera system tracks the number of conference participants in a room. Call information is collected in a Polycom RealPresence Resource Manager Call Detail Report (CDR) and provides detailed data to system administrators.

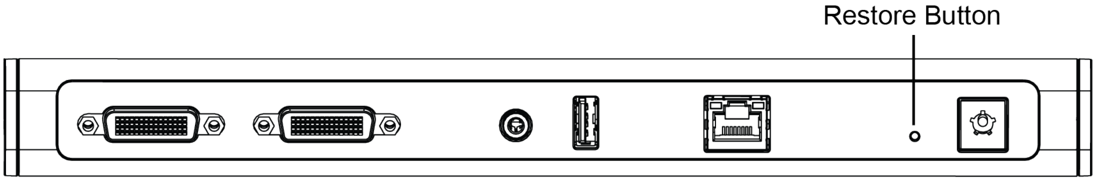
Note: To get the most accurate result of participant count data, the number of participants in a single room should be 10 people or less.

Participant Count

Participant	Description
People Minutes	The total people count for each minute of the call. For example, if there are ten people in the meeting and the meeting lasts for ten minutes, the total People Minutes will be 100 minutes.
People Count (call begin)	Number of people on the call during the first minute of the call, tracked with EagleEye Director II camera system.
People Count (peak value)	Peak number of people participating in the call, tracked with the EagleEye Director II camera system.
People Count (call end)	Number of people participating on the call during the last minute of the call, tracked with the EagleEye Director II camera system.

Perform a Factory Restore

You can use the hardware restore button on the EagleEye Producer system to perform a factory restore of the RealPresence Centro system. A factory restore completely erases the system and restores it to the software version and default configuration stored in its factory partition. During a factory restore, the LED indicator on the front of the system blinks blue and amber.



Procedure

1. While the EagleEye Producer system is powered off, insert a straightened paper clip through the pinhole and press and hold the **Restore** button.
2. While holding the **Restore** button, plug in the power cable to power on the EagleEye Producer.
3. Hold the **Restore** button for five additional seconds, and then release it when the LED alternates amber and blue.

   The EagleEye Producer enters factory restore mode. The factory restore takes approximately eight minutes to complete. The EagleEye Producer automatically reboots when the process is complete.
4. Calibrate the room view when the reboot is complete.

   Note: Keep the Polycom EagleEye Producer powered on during the factory restore process.

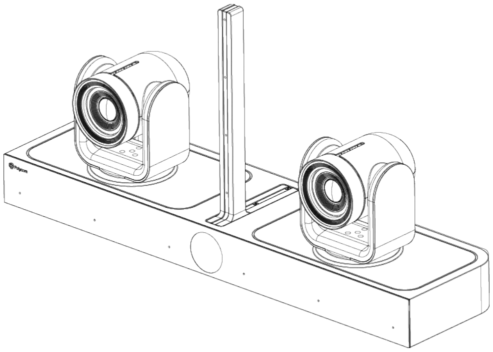
Polycom EagleEye Director II Camera System

The Polycom® EagleEye™ Director II camera system is the next version of the Polycom EagleEye Director camera; it combines the functionality of the EagleEye Producer camera and EagleEye Director camera to enrich the video conference experience.

This automatic camera positioning system works in conjunction with a RealPresence Centro system to provide accurate close-up views of the person who is speaking. The EagleEye Director II camera system also provides smooth transitions between the close-up view of the person who is speaking and the group view when there is no active speaker.

When the EagleEye Director II camera system is in tracking mode or when the analytics camera is in tilt position, the analytics camera captures group view video only. At the same time, the two EagleEye IV cameras in active state have a display a LED light. In any state, the analytics camera does not send video to RealPresence Centro system.

Note: The Polycom EagleEye Director II camera system is compatible with Polycom EagleEye IV cameras.

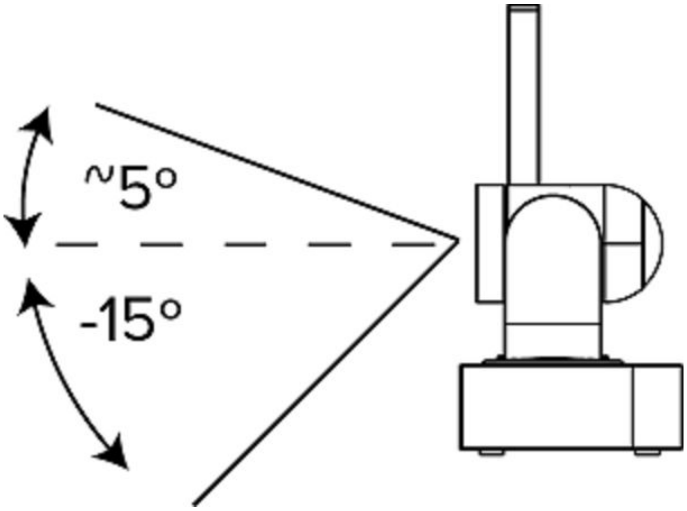


The EagleEye Director II camera uses a dual-camera system. Initially, the current view is captured by one camera, while the other camera will be searching and tracking the next target. If two persons speak alternately, the camera will track the person who is speaking, while the other camera will be tracking the other person who is speaking. By providing automatic and intelligent views in various speaking scenarios during a conference, the EagleEye Director II camera system delivers a user experience similar to a newscast video production.

Position the Polycom EagleEye Director II Camera System

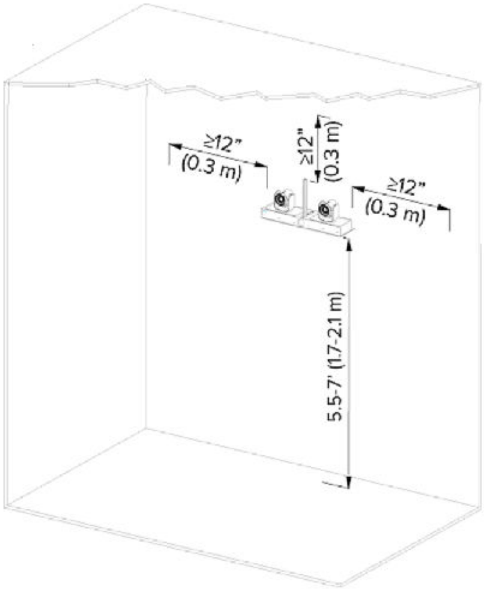
Follow these guidelines when you use the EagleEye Director II camera system with your RealPresence Centro system.

- Make sure the EagleEye Director II camera system is on a level surface or mounting bracket.
- The camera’s viewing angle is approximately 9 degrees above and 30 degrees below its direct line of sight as shown below.

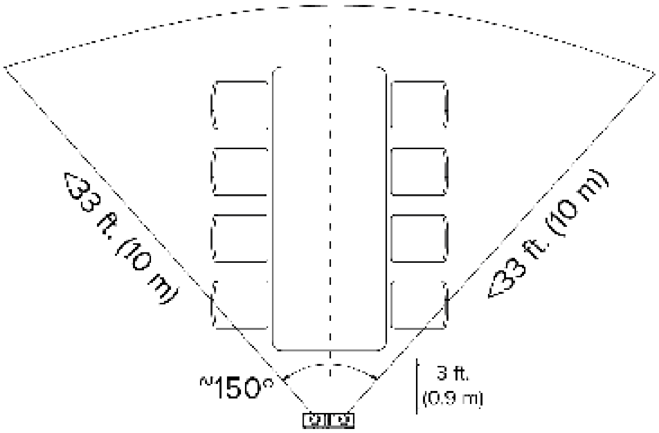


- To ensure the optimal performance of the EagleEye Director II camera system facial recognition feature, follow these suggestions:
    - Provide ample lighting on faces of participants. This allows the EagleEye Director II camera system to correctly frame faces, using the eyes, noses, and mouths as guidelines.
    - Allow only minimal backlighting.
- To ensure the best view from the EagleEye Director II camera system voice-tracking feature, follow these suggestions:
    - Make sure ambient room noise is quiet enough to allow the EagleEye Director II camera system to locate the participant who is speaking.
    - Be sure to set up the audio connection from theRealPresence Centro system to the EagleEye Director II camera system, whether you connect it directly to the audio output of the RealPresence Centro system or to an audio processor managing the room audio.
    - Set the EagleEye Director II camera system on top of a monitor. Ideally, place the camera between 5.5 and 7 feet from the ground.

The following figure shows placement of EagleEye Director II camera system:



Ensure that people are sitting within the viewing range of between 3 and 33 feet from the device. The following figure shows the viewing range of EagleEye Director II camera system.



Note: Before powering on the EagleEye Director II camera system, connect the camera system to the RealPresence Centro system using a HDCI cable. This will prevent the camera system from automatically entering sleep mode after three minutes.

Change the EagleEye Camera

If you want to change the EagleEye camera attached to the EagleEye Director II camera system to another EagleEye camera, perform the following steps.

The RealPresence Centro system will not detect the new camera unless you power off the EagleEye Director II camera system.

Procedure

1. Power off the EagleEye Director II camera system.
2. Disconnect and remove the existing EagleEye camera.
3. Connect the new EagleEye Camera. For more information about how to connect an EagleEye camera, see the Polycom EagleEye Director II Set Up Sheet.
4. Power on the EagleEye Director II camera system.

Note: The cameras on the EagleEye Director II camera system must be an EagleEye IV camera.

Configure Camera and Video Settings

You can configure the EagleEye Director II camera system that is connected to your RealPresence Centro system.

Procedure

» In the web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**. Configure the following settings as needed.

Configure General Camera Settings

Setting	Description
Allow Other Participants In a Call to Control Your Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this setting is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site. This is sometimes also called Far End Camera Control (FECC).
Power Frequency	Specifies the power line frequency for your system. In most cases, the system defaults to the correct power line frequency, based on the video standard used in the country where the system is located. This setting allows you to adapt the system in areas where the power line frequency does not match the video standard used. You might need to change this setting to avoid flicker from the fluorescent lights in your conference room.
Make This Camera Your Main Camera	Specifies the primary camera. You specify the main camera when you set up the system, but you can change that selection here. Input 1 is typically your main camera.
Enable People+Content IP™	Enables the ability to use the **People+Content IP** application.

Setting	Description
Enable Camera Preset Snapshot Icons	Enables the use of snapshot icons that represent camera preset configurations. The default setting is controlled by the Security Profile, but you can change the default here. If you change your security profile setting from **Low** or **Medium** to **High** or **Maximum**, or if you disable the setting, the system replaces each preset image with a blue, striped box. Presets that have not been configured show as empty rectangles. When you disable the **Enable Camera Preset Snapshot Icons** setting in the system web interface, the blue, striped boxes in the local interface show you which presets are configured, but enabling the setting does not redisplay the snapshot icons. You can see snapshot icons that represent preset configuration images only when you configure a preset with the **Enable Camera Preset Snapshot Icons** setting enabled.

Change Camera Tracking Settings

The EagleEye Director II camera system detects the participants in the room and provides framing during a conference. Frame Speaker with a Normal tracking speed and Medium view are enabled by default. To change camera tracking settings, follow the steps below:

Procedure

1. Do one of the following:

    a) In the local interface of the RealPresence Centro system, go to **Settings** > **Administration** > **Camera Tracking** > **Settings**.

    b) In the web interface of the RealPresence Centro system, go to **Admin Settings** > **Audio/ Video** > **Video Inputs** > **General Camera Settings** and select the input used by the EagleEye Director II camera system.
2. Configure the following settings:

Setting	Description
Tracking Mode	Specifies the tracking mode: **Frame Speaker** - This is the default setting. During a conference, this mode frames the active speaker, then when someone else starts speaking, the camera view changes to frame the new speaker. **Note:** When the tracking mode is set to **Frame Speaker** and the local microphone is muted, the camera tracking mode automatically switches to **Frame Group**. **Frame Group** - Enables automatic tracking and framing of the group participants in the room without displaying the camera motion between frames. **Off** - Disables automatic tracking. All camera control must be handled manually.
Tracking Speed	Specifies the tracking speed: **Slow** - Detects meeting participants at a slow speed rate. **Normal** - This is the default tracking speed. Detects meeting participants at a normal speed rate. **Fast** - Detects meeting participants at a fast speed rate.
Framing Size	Specifies the framing view: **Wide** - Establishes a wide view of meeting participants. **Medium** - This is the default group framing view. Establishes a medium view of meeting participants. **Tight** - Establishes a close-up view of meeting participants.
Picture in Picture	Specifies the picture in picture: **Checked:** When turned on, the room view from the analytics camera is shown in the bottom right corner along with the speaker view. **Unchecked**: No room view. The default option is **ON**. **Note:** Setting is available only when you have installed an EagleEye Director II camera system.

Improve Camera Tracking Performance

Tracking performance can be affected by room lighting. If the room is too bright for camera tracking to work properly, you can improve the tracking performance by adjusting the **Backlight Compensation** setting on the **Cameras** screen.

To change the **Backlight Compensation** setting, follow the steps below:

Procedure

1. In the web interface, go to **Admin Settings** > **Audio/Video**.
2. Click on **Video Inputs** and select the appropriate input.

EagleEye Director II Camera System Group Framing

The RealPresence Centro system continuously scans the room and commands the movable camera to pan, tilt, and zoom, framing users with facial recognition technology.

Participant Count CDR Details

When used with a RealPresence Centro system and an EagleEye camera, the camera system tracks the number of conference participants in a room. Call information is collected in a Polycom RealPresence Resource Manager Call Detail Report (CDR) and provides detailed data to system administrators.

Note: To get the most accurate result of participant count data, the number of participants in a single room should be 10 people or less.

Participant Count

Participant	Description
People Minutes	The total people count for each minute of the call. For example, if there are ten people in the meeting and the meeting lasts for ten minutes, the total People Minutes will be 100 minutes.
People Count (call begin)	Number of people on the call during the first minute of the call, tracked with EagleEye Director II camera system.
People Count (peak value)	Peak number of people participating in the call, tracked with the EagleEye Director II camera system.
People Count (call end)	Number of people participating on the call during the last minute of the call, tracked with the EagleEye Director II camera system.

Update Polycom EagleEye Director II Camera System Software

Updates to Polycom EagleEye Director II camera system are included with RealPresence Centro system software updates. No license number or key is needed to update the system.

To update your EagleEye Director II camera system, use a USB drive with at least 200MB of available space. Make sure the file system is in FAT32 format.

Procedure

1. Create a folder named `plcm-eed2-cmd` in the USB root directory.
2. Create a subfolder named `update` in the `plcm-eed2-cmd` folder.
3. Copy the EagleEye Director II update image

`(polycom-eagleeyedirector II-xxx-1.0.0.xx-xxxx.img)` into the `update` folder.

4. Plug in the EagleEye Director II camera system power cable to power it on and allow it to fully boot up.

   The LED turns solid blue.
5. Plug the USB drive into EagleEye Director II camera system.

   The LED blinks amber and then turns solid blue in a few seconds.

   Note: Do not unplug the USB drive during the software update process.
6. Unplug the EagleEye Director II camera system power cable, but leave the USB drive plugged in.
7. Plug in the EagleEye Director II camera system power cable and allow it to boot up.

   The LED turns solid blue. The EagleEye Director II camera system starts the image update and the LEDs blink blue and amber. The image update takes approximately ten minutes to complete. The EagleEye Director II camera system automatically reboots when the image update is complete. The camera tilts up and then down during the reboot and the LED returns to solid blue.
8. Remove the USB drive.

   The update log is saved in `[USB root directory]/eed2out/[EED2 SN]/log`.

   Note: When the EagleEye Director II camera system is in update state, the amber and blue LEDs blink alternatively.

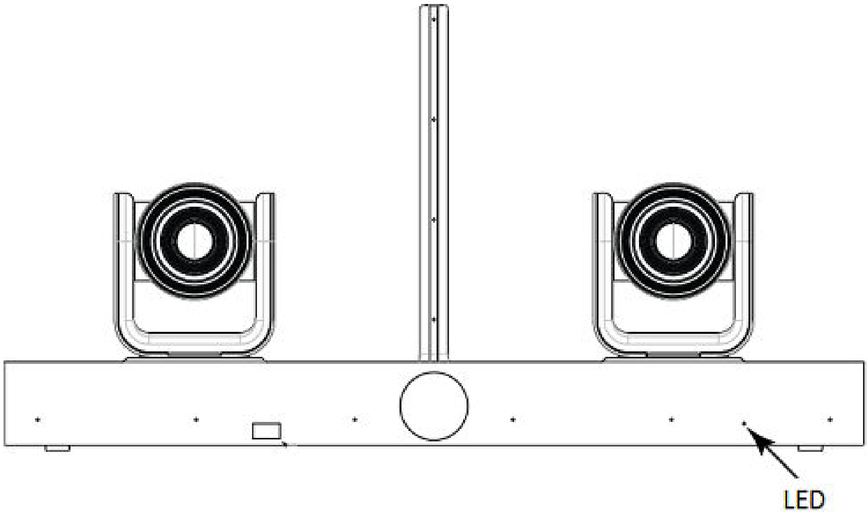
   Software for an EagleEye camera is automatically updated when the camera is attached to a RealPresence Centro system with an EagleEye Director II camera system.

Indicator Lights

Indicator lights and power sensors display when the EagleEye Director II camera system is powered on.

A light-emitting diode (LED) is integrated into the front of the EagleEye Director II camera system. These LED lights emit colors that refer to various system states and allow you to identify the current state of the EagleEye Director II camera system.

The following table shows the LED status of EagleEye Director II camera system with its corresponding behavior.



LED Color	Behavior
Blue	Power On, EagleEye Director II camera system is in active state
Blinking Blue	Receive IR, EagleEye Director II camera system boot up
Fast Blinking Blue	Power On, MCU is being initialized, Adjust Analytics camera status
Amber	Standby/Asleep
Alternate Amber and Blue	Software update, Factory restore, USB image update
Blinking Amber	USB plugged in
Green	In a call
Blinking Green	Receive IR in a call
Fast Blinking Red	EagleEye Director II camera system error

View System Status for EagleEye Director II Camera System

You might need to view the system status of an EagleEye Director II camera system on a RealPresence Centro system interface.

Procedure

» Do one of the following:

a) In the local interface, go to **Settings > System Information > Status**.

b) In the web interface, go to **Diagnostics > System > System Status**.

You cannot view the system status if the EagleEye Director II camera system is not connected or is not selected as the current camera source.

System Status

Diagnostic Screen	Description
Active Alerts	Displays the status of any device or service listed within the Status screens that has a current status indicator of red. Alerts are listed in the order they occurred.
Call Control	Displays the status of the Auto-Answer Point-to-Point Video and Meeting Password settings.
Audio	Displays the connection status of audio devices such as microphones, Polycom SoundStation IP conference phone, and Polycom SoundStructure card.
Camera	Displays the connection status of the camera that is connected. If the camera is not connected or is not selected as the current camera source, this choice is not visible on the screen. In addition, the details of the EagleEye cameras attached to the EagleEye Director II camera system are displayed.
LAN	Displays the connection status of the IP Network.
Servers	• Always displays the Gatekeeper and SIP Registrar Server. • Displays the active Global Directory Server, LDAP Server, or Microsoft Server. • If enabled, displays the Provisioning Service, Calendaring Service, or Presence Service.
Log Management	Displays the status of the Log Threshold setting. When a system device or service encounters a problem, you see an alert next to the **System** button on the menu.

EagleEye Director II Camera System Diagnostics

Most diagnostic information is available on both the web and the local interface, but some information is specific to one or the other interface. From the web interface, go to **Diagnostics** > **Audio and Video Tests** > **Camera Tracking**.

The screen includes the following diagnostic information for your camera system.

Diagnostic Screen	Description
Speaker Test	Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct. If you run the test from the system during a call, the far site will also hear the tone. If you run the test from the system web interface during a call, the people at the site you are testing will hear the tone, but you will not.
Audio Meters	Measures the strength of audio signals from ten internal microphones, far-site audio, and any device connected to the audio line in. Meters function only when the associated input is enabled. **Note**: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system.
Camera Tracking	Provides diagnostics specific to the EagleEye Director II camera system. **Audio** Verifies microphone functionality. To use this feature, speak aloud and verify that you can see dynamic signal indications for four vertical microphones and six horizontal microphones. If no signal indication appears for a specific microphone, manually power off the EagleEye Director II camera system and then power it back on. Also verifies the reference audio signal: Set up a video call. Let the far side speak aloud and verify that you can see dynamic signal indications for the two reference audio meters. If no signal indication appears for a specific microphone, make sure the reference cable is connected firmly. After you verify microphone functionality, calibrate the camera again. **Video** • **Left Camera** shows video from the left camera. • **Right Camera** shows video from the right camera. • **Analytics Camera** shows video from the analytics camera. • **Color Bars** displays the color bar test screen. **Note**: If the EagleEye Director II camera system is connected but is not selected as current camera source, this choice is not visible on the screen.

Download System Logs and Configurations

You can use an empty USB storage device to save the EagleEye Director II camera system logs and configurations. Make sure the file is in FAT32 format.

Procedure

1. Create a folder named `plcm-eed2-cmd` in the USB root directory.
2. Create a sub folder named `log` in the `plcm-eed2-cmd` folder.
3. Create a blank text file named `downloadlogflg` in the `log` folder.
4. Insert the USB storage device into the EagleEye Director II camera system. The LED blinks amber and then turns solid blue.
5. Remove the USB drive.

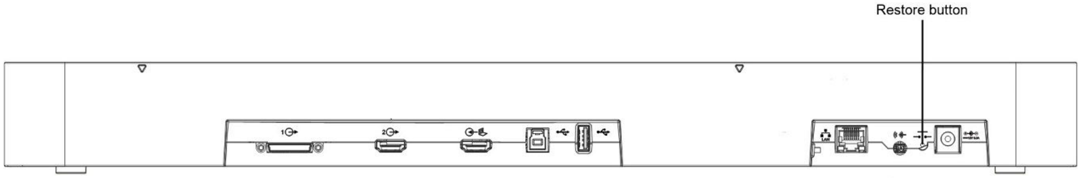
The application logs and system information are downloaded to the `[USB root directory]/eed2out/[EED2SN]/log/` folder.

The configuration files are downloaded to the `[USB root directory]/eed2out/[EED2 SN]/config/` folder.

The system current running status is recorded in a file called *sysstatus* and is in the `[USB root directory]/eed2out/[EED2 SN]/` folder. The system status file includes current CPU/memory usage and current running process information.

Perform a Factory Restore

You can use the hardware restore button on the EagleEye Director II camera system to perform a factory restore. A factory restore completely erases the system and restores it to the software version and default configuration stored in its factory partition. During a factory restore, the LED indicator on the front of the EagleEye Director II camera system blinks blue and amber.



Note: Do not power off the EagleEye Director II camera system during the factory restore process.

Procedure

1. While the EagleEye Director II camera system is powered off, insert a straightened paper clip through the pinhole and press and hold the **Restore** button.
2. While holding the **Restore** button, plug in the power cable to power on the EagleEye Director II camera system.
3. Hold the **Restore** button for an additional five seconds, and then release it when the LED alternates amber and blue.

   The EagleEye Director II camera system enters factory restore mode. The factory restore takes approximately eight minutes to complete. The EagleEye Director II camera system automatically reboots when the process is complete.

Set Up the Polycom EagleEye Director

You can use the remote control or the RealPresence Centro system web interface to set up the EagleEye Director. You cannot configure the EagleEye Director using a Polycom touch device, but you can start and stop camera tracking.

For detailed setup instructions, refer to *Set up the Polycom EagleEye Director* on Polycom Support.

Procedure

1. Power on the EagleEye Director.

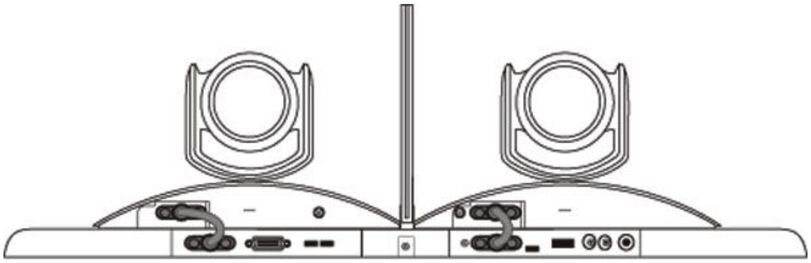
   You can verify that the device is detected and compatible with the system's software on the System Status screen.

   - In the system web interface, go to **Diagnostics** > **System** > **System Status** > **EagleEye Director**.If you see **EagleEye Director** among the status settings, the device has been detected.
2. Calibrate the cameras.

   If you notice that the speaker is not framed accurately, ensure that the vertical bar of the EagleEye Director is vertical. Placing the EagleEye Director on a horizontal surface can help to ensure that the vertical bar is vertical. You might also need to recalibrate the cameras.
3. Adjust the room view.

EagleEye Director Indicator Light

The following figure shows the location of the power indicator light on the back of the EagleEye Director.



This indicator light provides the following information.

Adjust the Room View

You can adjust the room view on the EagleEye Director to get the best perspective for your video calls.

Procedure

1. Do one of the following:
   - From the local interface, go to ⚙ > **Settings** > **Administration** > **Camera Tracking** > **Calibration**, and then select **Begin Calibration**.
   - From the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**, and then select the **Input** used by the EagleEye Director.

2. Do one of the following:
    - In the local interface, select **Skip** to move to the Adjust Room View screen.
    - In the system web interface, select **Adjust Room View**.
3. Use the arrow buttons and zoom controls on the remote control or system web interface to show the room view you want far site participants to see.
4. Select **Finish** to save the settings and return to the Camera Settings screen.

Enable Camera Tracking for EagleEye Director

If EagleEye Director tracking is enabled, the camera follows the person or people who are speaking. While one camera tracks the person who is speaking, the other camera captures the room view. The EagleEye Director shows the room view while the camera moves from one speaker to another. When the tracking camera locates a person who is speaking, the EagleEye Director camera switches to a close-up of that person. This tracking action, also called automatic camera positioning, can be manually started.

Procedure

» Do one of the following:

- In the local interface, go to > **Settings > Administration > Camera Tracking > Settings**.
    - For the **Tracking Mode** setting, select **Voice**. This is the default tracking mode. In this mode, the camera automatically tracks the current speaker in the room using a voice tracking algorithm.When you select the **Voice Tracking Mode**, you can also choose the **Tracking Speed**. This speed determines how quickly the camera moves to each person who speaks. The default speed is **Normal**.If voice tracking does not work as expected, make sure the microphones are functioning properly.
- In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**, and then select the **Input** used by the EagleEye Director.
    - Enable the **Use Voices to Track People** setting.
- If the RealPresence Centro system is paired with a Polycom touch device, follow these steps:
    1. On the touch device, touch **Cameras** on the Home screen or the Call screen.
    2. If the EagleEye Director is not currently selected, select it.
    3. Touch **Select Cameras** and select the EagleEye Director camera.
    4. Touch **Control Camera**.
    5. Select **Start Camera Tracking**.

Disable Camera Tracking for EagleEye Director

You can manually stop EagleEye Director tracking, which is also called automatic camera positioning.

Procedure

» Do one of the following:

- In the local interface, go to > **Settings** > **Administration** > **Camera Tracking** > **Settings**.
    - For the **Tracking Mode** setting, select **Off**. In this mode, the tracking function is disabled. You must manually move the camera using the remote control or a touch device.

- In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs**, and then select the **Input** used by the EagleEye Director.
    - Disable the **Use Voices to Track People** setting.
- If the RealPresence Centro system is paired with a Polycom touch device, touch **Cameras** on the Home screen or the Call screen and select **Stop Camera Tracking.**

Camera Tracking in the Local Interface

You can start or stop camera tracking in the local interface. Whether you are or are not in a call, go to **Menu** > **Cameras** and select **Start Camera Tracking** or **Stop Camera Tracking**.

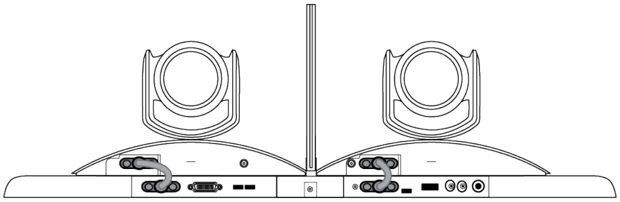
Camera tracking can also start or stop automatically, based on the following actions:

- Camera tracking starts automatically when you make a call.
- Camera tracking stops after you hang up a call.
- Camera tracking temporarily stops when you mute the RealPresence Centro system in a call. It resumes when you unmute the system. If camera tracking is disabled, pressing Mute on the remote control does not affect tracking.

Perform a Factory Restore for the EagleEye Director

If the EagleEye Director is not functioning correctly or you need to recover from a corrupted partition, you can use the restore button to reset the device. This operation completely erases the camera's settings and reinstalls the software. Keep the EagleEye Director powered on during the factory restore process.

The following figure shows you the location of the restore button on the back of the EagleEye Director.



Procedure

1. Press and hold the restore button on the back of the EagleEye Director for 2-3 seconds while the power light cycles.

   When normal video content is displayed on the monitor instead of a blue screen, the EagleEye Director has been successfully restored.
2. Release the restore button.

Troubleshooting EagleEye Director Camera Tracking

Tracking performance can be affected by room lighting. If the room is too bright for camera tracking to work properly, you can improve the tracking performance by adjusting the Backlight Compensation setting on the Cameras screen. To find this setting in the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs** and select the appropriate Input.

Troubleshooting EagleEye Director Camera Calibration

When the system first detects the EagleEye Director, a calibration wizard starts. If the EagleEye Director is not detected, try one of the following solutions:

- Ensure all cables are tightly plugged in, then attempt camera detection again. If you are using EagleEye Director version 1.0 software, you might need to ensure that the ball stubs are tightly pressed into the hole on the base after checking the cables.
- Ensure that all seven EagleEye Director tracking microphones are working correctly. Five of those microphones are horizontal and two are vertical reference audio microphones. Calibration fails if any of the microphones do not work.
- Restart the RealPresence Centro system.

Manually power off the EagleEye Director by unplugging its power supply and unplugging the HDCI cable from the RealPresence Centro system. Then power on the EagleEye Director, plug the HDCI cable into the system, and attempt camera detection again.

Transfer EagleEye Director Logs

The Polycom EagleEye Director logs contain important status and debug information that is not included in the logs available for the RealPresence Centro system.

Procedure

1. Attach a USB storage device formatted in FAT32 to the back panel of the EagleEye Director.
2. Restart the EagleEye Director by following these steps:

   a) Unplug the 12v adaptor attached to the side of the EagleEye Director.

   b) Wait a 5 seconds.

   c) Plug the 12v adaptor into the side of the EagleEye Director.

      It could take up to two minutes for the EagleEye Director to restart.
3. Remove the USB storage device.

   A log file using the name format of eagleeyedirector_info_xxxxx.tar.gz is generated on the USB storage device.

EagleEye Director Software Updates

Updates to EagleEye Director software is included with the RealPresence Centro system software updates. No license number or key is needed to update the camera software.

To update your EagleEye Director, connect it to the system before you run a software update. The software update program detects the device and updates it if necessary.

RealPresence Centro System Camera

By default, the 360-degree camera is motorized and set to be up when the solution is in use or in a call. The camera is down when the solution is off, in standby mode, or not in a call.

System Status and Camera Position

You can configure the camera's behavior along with where the panoramic filmstrip displays and the duration the camera remains up after a call has ended.

The following table includes the default camera position when the Camera Head Position setting is set to Automatic. When the camera's position is set to Up, the camera is always Up unless the solution is off or restarting. When the camera's position is set to Up (Sleep Mode), the camera is always Up unless the solution is in sleep mode, off, or restarting.

System State	Call State	Additional Controls	Camera Position
Off			**Down**
On	**Video call**	**Camera On**	**Up**
On	**Video call**	**Hide Self View**	**Up**
On	**Video call**	**Camera Off**	**Up**
On	**Audio call**		**Up**
On	**Not in a call**	**Camera controls and settings**	**Up**
On	**Not in a call**	**Show Self View**	**Up**
On	**Not in a call**	**Hide Self View/Camera Off**	**Down**

Camera Presets

Camera presets are stored camera positions that you can create in the RealPresence Centro system local interface before or during a call. Presets allow you to do the following:

- Automatically point a camera at pre-defined locations in a room.
- Select a video source.

If your camera supports pan, tilt, and zoom movement, and it is set to People, you can create up to 10 preset camera positions for it using the remote control or a touch device, such as the RealPresence Touch. Each preset stores the camera number, its zoom level, and the direction it points (if appropriate). RealPresence Centro systems support these presets for far-end site cameras only.

If a Polycom touch device is paired with a system, you must use the touch device to create presets. For more information about creating and using presets, refer to the *Polycom RealPresence Centro User Guide.* Once presets are in place, you can view them in the system web interface by going to **Utilities** > **Tools** > **Remote Monitoring**.

Configure FECC on the Far-end Site Camera

If far-end camera control (FECC) is allowed, you can create 10 presets for a far-site camera. These presets are saved only for the duration of the call. You might also be able to use presets created at the far site to control the far-site camera.

Procedure

» In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs** > **General Camera Settings** and select **Allow Other Participants in a Call to Control Your Camera**.

For details on how to create camera presets, or how to move a camera to a stored preset, refer to the *Polycom RealPresence Centro User Guide.*

Configuring Remote Control Behavior

Topics:

Configure Remote Control Behavior

By configuring settings in the RealPresence Centro system web interface, you can customize the remote control behavior for your end users. This information is for both Polycom and third party remote control devices.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Remote Control, Keypad, and Power**.
2. Configure these settings.

Setting	Description
Keypad Audio Confirmation	Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad.
Numeric Keypad Function	Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones). If this is set to **Presets**, users can generate DTMF tones by pressing the # key on the remote while on a video screen.
Use Non-Polycom Remote	Configures the system to accept input from a programmable, non-Polycom remote control. In most cases the Polycom remote works as designed, even when this feature is enabled. However, try disabling this feature if you experience difficulty with the Polycom remote.
Channel ID	Specifies the IR identification channel to which the room system responds. Set the Channel ID to the same channel as the remote control. The default setting is 3. If the remote control is set to channel 3, it can control a room system set to any Channel ID.

Setting	Description
Hang-up Button Long Press	Specifies the behavior of the remote control **Hang-up** button when you press it for a long time: • **Hang-up / Power Off**—Holding down the **Hang-up** button powers off the room system. • **Hang-up / Sleep**—Holding down the **Hang-up** button puts the system to sleep. • **Hang-up Only**—Holding down the **Hang-up** button has no function other than hanging up the call.
# Button Function	Specifies the behavior of the **#** button on the remote control: • **#, then @**—Pressing the # button once on the keypad displays the hash sign. Pressing the # button twice, quickly, displays the commercial at (@) symbol. • **@, then #**—Pressing the # button once on the keypad displays the @ symbol. Pressing the # button twice, quickly, displays the # sign.

Programming the Remote Control

Use the remote control to power on and off your system, or to put the system to sleep or wake it. For details about how to use the remote control, refer to the *Polycom RealPresence Centro User Guide* .

You can customize the behavior of the remote control to support the user's environment. Note the following regarding remote control behavior:

- If the system is paired and connected with a RealPresence Touch, the remote control can perform some limited functions.
- The room system remote control IR transmits a modulated frequency of 38 kHz.
- When a USB keyboard is connected to a room system, you can enter only numbers with the remote control on the system's local interface on the **Place a Call** > **Keypad** or **Place a Call** > **Contacts** screens.

Set the Remote Control Channel ID

You can set the remote control channel ID in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Remote Control, Keypad, and Power**.
2. Select the **Channel ID**.
3. Click **Save**.

To find the Channel ID for your monitor, check the connection label on the monitor, or refer to the monitor's manufacturer documentation.

Set the Remote Control Channel ID for a Specific System

You can configure the Channel ID so that the remote control affects only one RealPresence Centro system, even if other systems are in the same room.

If the remote control is set to channel 3, it can control a room system set to any Channel ID. If the system does not respond to the remote control, set the remote control channel ID to 3 starting with step 3 in the following procedure. Then follow the entire procedure to configure the system and remote control channel ID settings.

While performing the following procedures, blocking the IR signal from the remote control can prevent the signal from being received by the system, causing the system to take an action that corresponds to any of the remote control button presses.

Procedure

1. While blocking the IR signal from the remote control using your hand or some other object, press and hold 🔇 and 📞 for 2-3 seconds.
2. After the red LED on the remote control comes on, release both keys.

   The LED remains lit for 10 seconds.
3. While the LED is lit, enter a 2-digit ID between 00 and 15.

   If you do not enter the ID during the 10 seconds the LED is lit, the LED flashes six times and you must repeat steps 1 and 2. Be sure to enter the ID during the next 10-second window.

If the channel ID is saved successfully, the LED flashes twice. Otherwise, the LED flashes six times and you must repeat steps 1 - 3.

Confirm the Channel ID

You can confirm the correct channel ID to control your RealPresence Centro system.

Procedure

1. While blocking the IR signal from the remote control using your hand or some other object, press and hold 🔇 and ☎ for 2-3 seconds.
2. After the LED on the remote control comes on, release both keys.

   The LED remains lit for 10 seconds.
3. While the LED is lit, enter the 2-digit ID between 00 and 15 that you believe is the channel ID.

   If you do not enter the ID during the 10 seconds the LED is lit, the LED flashes six times and you must repeat steps 1 and 2. Be sure to enter the ID during the next 10-second window.
4. If you entered the current channel ID, the LED flashes twice.

   Otherwise, the LED flashes six times and allows you to repeat step 3.

Using the RealPresence Centro System Remote Control

The remote control enables you to operate the RealPresence Centro system and control the system with touch monitors or a touch device. You can place calls, adjust the volume, and navigate menus. To control the system, point the remote control toward the monitors.

Recharge the Remote Control Battery on the RealPresence Centro System

When the remote control battery power is low, a notification displays on the RealPresence Centro Home screen. You can use the USB ports on the base of the solution to charge the battery. Recharging the battery can take from 20 minutes up to multiple hours.

Procedure

1. Pull the battery out of the end of the remote control.
2. Insert the USB plug of the battery into a USB port on the system.
3. Wait until the status light on the battery turns green before removing it from the port.
4. Insert the charged battery into the remote control.

Enabling Mobile Devices as Controllers

Topics:

- Enabling RealPresence Mobile

You can customize how to use various controllers for the system. For more information, see the following topics.

Enabling RealPresence Mobile

Polycom SmartPairing™ allows you to detect and pair a RealPresence Centro system from the RealPresence Mobile application on an Android or Apple iPad tablet. After you pair the application and the system, you can use the RealPresence Mobile application to perform two basic functions:

- Use the application as a remote control for the room system.
- Swipe to transfer a call from the RealPresence Mobile application to the room system.

SmartPairing Prerequisites

Telnet must be enabled before you can use SmartPairing on RealPresence Centro systems. Because telnet is disabled by default in all Security Profiles, SmartPairing is also disabled by default. The setting to enable telnet is not configurable when the **Security Profile** is set to Maximum or High.

Security Profiles and SmartPairing

Security Profile	Telnet Setting Default	SmartPairing Available?
Maximum / High	Disabled, Not Configurable	No
Medium / Low	Disabled, Configurable	Yes. To use SmartPairing, do the following: 1 Enable telnet. In the system web interface, go to **Admin Settings** > **Security** > **Global Security** > **Access** and at **Enable Telnet Access**, select the checkbox. 2 Send an API command or use the system web interface.

Configure SmartPairing

You can configure SmartPairing so that users can pair mobile devices to the RealPresence Centro system.

Procedure

1. In the RealPresence Centro system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **SmartPairing**.

2. Configure these settings.

Setting	Description
SmartPairing Mode	Specifies the method used to pair with the room system, if SmartPairing is enabled: • **Disabled** • **Automatic** • **Manual**
Signal Volume	Specifies the relative signal strength of the ultrasonic signal within the loudspeaker audio output signal. The selections are Auto, and levels are 1 to10.

Enabling Content Sharing

Topics:

To prepare for sharing content, see the following topics.

Configure Content Sharing

You can configure content sharing in the RealPresence Centro system web interface. For content to display properly, the system's Monitor 2 must support Progressive mode, and the output resolution should be set to a Progressive setting, such as 1280x720p or 1920x1080p. Interlaced output for Monitor 2 is not supported. Do not use the resolution setting 1920x1080i.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Video Inputs** and select the input you want to configure for content.
2. For the **Display as** setting, select **Content** for the input that will display content.

   When you connect a content-sharing device such as a laptop to the input, the content starts displaying. If the content-sharing device is already connected, you must manually show the content from the local interface. For more information about sharing content, refer to the *Polycom RealPresence Centro User Guide*.

   If default values for other settings in the system have not changed, you are ready to share content on your system. However, if you disabled the H.239 protocol, you must enable the program for content sharing by following these steps:
3. In the system web interface, go to **Admin Settings** > **Network** > **Dialing Preference**.
4. Enable **H.239**.

   Note: While in a call, you cannot enable or disable H.239.

Adjust Audio Level for Content

You can adjust the audio level for content in the RealPresence Centro system web interface.

If the audio level of the call using content sharing needs to be adjusted, follow these steps to change the level:

- In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio** > **Audio Input**.
- Set the **Audio Input Level**.

Configure Monitor 1 as the Content Monitor

To use the VisualBoard application on your RealPresence Centro system's Monitor 1, you must configure monitor settings on the system web interface. If you are using a touch monitor as Monitor 1, you can run the VisualBoard application on the monitor and touch the screen to interact with the application.

Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use **Game Mode**, if that setting is available.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors**.
2. Under Monitor 1 for the **Enable** setting, select **Manual.**
3. For the Monitor Profile setting, select **Content, then Far, then Near** or **Content, then Far.**

Configure Monitor 2 as the Content Monitor

The VisualBoard application runs on Monitor 2 by default, but you might want to make configuration changes to the monitor settings in the RealPresence Centro system web interface. Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use **Game Mode**, if that setting is available.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors**.
2. To configure monitor 1, go to **System** > **Admin Settings** > **Monitors**.

   At **Enable**, select either **Auto** or **Manual**. If you chose **Manual**, select any of the available profiles, except **Content, then Far, then Near** or **Content, then Far.**
3. To configure monitor 2, at **Monitor Profile**, enable one of the content profiles, such as **Content, then Far, then Near**, **Content, then Far**, **Content, then Near**, or the **Content Only** profile.

Setting Up a Polycom Content Display Application

The People+Content IP application enables a presenter to show content from a computer to other sites in a video conference using only an IP network connection. The presenter can show PowerPoint® slides, video clips, spreadsheets, or any other type of content from a computer. People+Content IP supports any computer desktop resolution with color set to 16-bit or higher.

If the system is paired with a RealPresence Touch , People+Content IP does not require installation. After you connect the PC to the USB connection on the device, a version of People+Content IP launches automatically.

Before a presenter can use a computer to show content with People+Content IP, do the following:

- Download the People+Content IP software application from the Polycom web site to the computer or computers that the presenter will use to show content.

  You don't need to change the computer resolutions and you don't need special cables or hardware, but each computer must meet these requirements:

  - Operating System: Windows 7 or 8
  - Minimum computer: 500 MHz Pentium® III (or equivalent); 256 MB memoryRecommended computer: 1 GHz Pentium III (or equivalent); 512 MB memory
- Connect the computer or computers to the IP network.

Configure Closed Captioning

You can provide real-time text transcriptions or language translations of the video conference by displaying closed captions on your RealPresence Centro system. When you provide captions for a conference, the captioner may be present, or may use a telephone or web browser to listen to the conference audio. When the captioner sends a unit of text, all sites see it on the main monitor for 15 seconds. The text then disappears automatically.

Closed captions are supported between Polycom systems with software version 4.1.3 or later, including a system hosting a multipoint call, HDX systems with any software version, and Polycom VSX® systems with software version 7.0 or later.

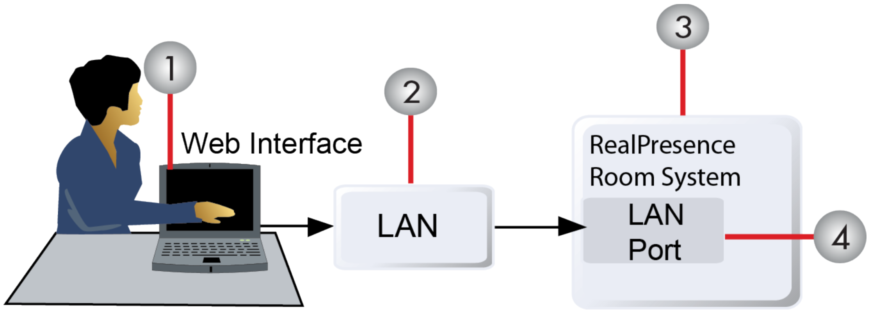
Captions may be provided in any language that uses the Latin alphabet.

Depending on the capabilities of the system, the captioner may enter caption text using one of the following methods:

- Remotely, through a dial-up connection to the system's serial RS-232 port
- In the room using equipment connected directly to the serial port
- In the room or remotely, using the system web interface

Enter Closed Captions on the Web Interface

Closed captioners can provide captions from inside the conference room, or from a remote location, by entering the captions directly into the RealPresence Centro system web interface, as shown in the following diagram.



Ref. Number	Description
1	Web interface
2	LAN
3	RealPresence Centro system
4	LAN port

Procedure

1. In the system web interface, go to **Utilities** > **Tools** > **Closed Caption**.
2. Log in using this information if prompted:

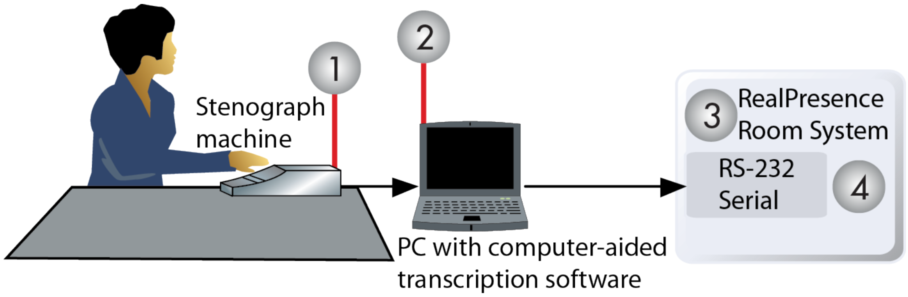
   User Name: Your user name defined for the video conferencing system.

   Password: Meeting password defined for your video conferencing system.
3. In the **Closed Caption** screen, type the caption text into the text field.

   Text wraps to the next line after 32 characters.
4. Press **Send** to send the text to the sites in the conference.

Enter Closed Captions Using Equipment Connected to a Serial RS-232 Port

Closed captioners can provide captions from inside the conference room, using equipment connected directly to the serial port of the RealPresence Centro system, as shown in the following diagram.



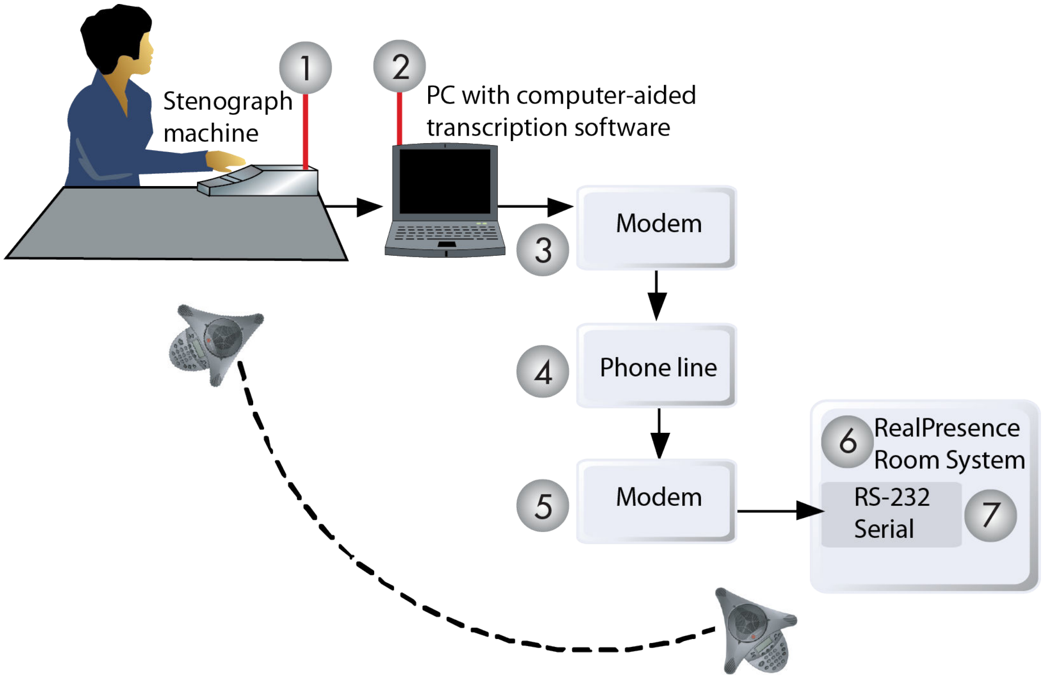
Ref. Number	Description
1	Stenographer machine
2	PC with computer-aided transcription software
3	RealPresence Centro system
4	RS-232 serial port

Procedure

1. Ensure that the computer and the system are configured to use the same baud rate and parity settings.
2. In the system web interface, go to **Admin Settings** > **General Settings** > **Serial Ports**.
3. Set the RS-232 mode to **Closed Caption**.
4. On the computer, start the transcription application.
5. Enter text using the stenographic machine connected to the computer.
6. To stop sending closed captions, close the transcription application.

Dial-Up Connection to the System's RS-232 Serial Port

Closed captioners can provide captions from inside the conference room, or from a remote location, via a dial-up connection to the serial port of the RealPresence Centro system, as shown in the following diagram.



Ref. Number	Description
1	Stenograph machine
2	PC with computer-aided transcription software
3	Modem
4	Phone line
5	Modem

Ref. Number	Description
6	RealPresence Centro system
7	RS-232 serial port

Procedure

1. Ensure that the computer and the system are configured to use the same baud rate and parity settings.
2. In the system web interface, go to **Admin Settings** > **General Settings** > **Serial Ports**.
3. Set the RS-232 Mode to **Closed Caption**.
4. Establish a dial-up connection between the computer and the system.
    a) Connect a null modem adapter to the RS-232 serial port.
    b) Connect an RS-232 cable to the modem and to the null modem adapter.
    c) Connect the modem to a phone line.
    d) Configure the modem for 8 bits, no parity.

    You may need to configure the modem to answer automatically. You may also need to configure it to ignore DTR signals.
5. On the computer, start the transcription application.
6. Enter text using the stenographic machine connected to the computer.
7. To stop sending closed captions, close the transcription application.

Enable VisualBoard Content Sharing

You must enable the VisualBoard application before you can use it with the RealPresence Centro system.

Procedure

1. From the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **VisualBoard/RDP**.
2. Select **Enable**, and then select **Save**.

Prerequisites for the VisualBoard Application

Before you can begin using the VisualBoard application, ensure that you have done the following:

- Installed and configured one of the following: USB mouse or UC Board hardware
- Enabled the VisualBoard/RDP setting on the RealPresence Centro system web interface
- When setting up the VisualBoard application, note that only one USB storage device can be connected to one host port, whether it is connected directly or through a hub.

Configure the Polycom UC Board

With the Polycom® UC Board, you can show and annotate content in real-time from RealPresence Centro systems by using the stylus and receiver included with the UC Board hardware. You can use either a second monitor or a whiteboard and projector. For flat, cold surfaces such as white boards with projectors, Polycom suggests that you use the Polycom UC Board.

Two monitors are required to use the Polycom UC Board. The second monitor can be either a projector used with a whiteboard, or a monitor.

Polycom recommends the following installation tips:

- Use LED backlit, LCD displays instead of CFL LCD displays.
- Do not use plasma backlit displays.
- The UC Board hardware sensor and pen are designed for cold surfaces, such as white boards with projectors.
- Mount the hardware sensor on the top of the display device. Room lights can interfere with the sensor when it is mounted on the bottom of the display.

The UC Board sensor supports one stylus at a time. It does not support using two styluses simultaneously.

For more information on setting up and using the UC Board, refer to the *Polycom UC Board Quick Start Guide*, available with the UC Board hardware and at Polycom Support.

To set up two monitors and configure to show content:

1. To configure monitor 1, in the system web interface, go to **Admin Settings** > **Audio/Video** > **Monitors**. At **Enable**, select either **Auto** or **Manual**. If you chose **Manual**, select any of the available profiles.
2. To configure monitor 2, at **Monitor Profile**, enable one of the content profiles.

   To improve performance, configure your monitor or projector to use **Game Mode**, if that setting is available.

Sharing Content During Calls

You can present content during calls when you use sources such as the following:

- A DVD player connected directly to a video input on a system
- People+Content IP installed on a computer, with any system
- A computer connected directly to a system or a Polycom touch device

RealPresence Centro systems achieve maximum content frame rate of 30 fps for 1080p with a 1080p Resolution option key installed, and 60 fps for 720p. If you use **Content** as the **Quality Preference** in your network IP settings, you can achieve a content frame rate of 60 fps for 1080p with the 1080p Resolution option key installed.

RealPresence Centro systems can achieve maximum content frame rate of 60 fps for 1080p, while the camera sends a maximum frame rate of 1080p 30 fps.

For more information about sharing content during a call, refer to the *Polycom RealPresence Centro User Guide*.

Configuring DVD Player Settings

On RealPresence Centro systems, you can connect a DVD player to an HDMI or VGA input to play content.

Adjust DVD Audio Settings for Content

DVD inputs are active when you select the camera source configured as DVD. This means that both the audio and video inputs are active—you cannot select one or the other. Because the microphone inputs remain active while the DVD player is playing, call participants might want to mute the microphones while playing DVDs. You can configure DVD audio settings in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Audio/Video** > **Audio** > **Audio Input**.
2. Set **Line In Level** for playback volume of the DVD player relative to other audio from the system.

   Enable **DVD Audio Out Always On** unless you have the DVD inputs and outputs both connected to the same device to play and record.

Configuring Call Recording

Topics:

- Polycom RealPresence Media Suite Recording

The following topics describe how to configure call recording and how to record calls.

Polycom RealPresence Media Suite Recording

Users can use Polycom® Media Suite solution to record calls directly from the RealPresence Centro system, remotely log in to Polycom RealPresence Media Suite to record or live stream calls.

RealPresence Media Suite is an enterprise recording, streaming and video content management solution that offers users and administrators a self-service user portal to record calls on their systems.

Enable Recording Controls

You can use a system to record the audio and video of a call.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **Recording Service**.
2. At **Enable RealPresence Media Suite**, select the checkbox.
3. Enter the connection information in the following settings.

Setting	Description
Domain Name	Enter the server domain name for RealPresence Media Suite.
User Name	Enter the server user name for RealPresence Media Suite.
Password	Enter the server password for RealPresence Media Suite.
Server Address	Enter the IP address for the RealPresence Media Suite server.

4. Click **Save** to save the connection settings.

Recording Calls Remotely

From RealPresence Media Suite's User Portal, any user can start recording, create a live stream event, and share video files. The Polycom RealPresence Media Suite is also a streaming and recording system that participates in standards-based video and telepresence calls.

The RealPresence Media Suite solution allows users to record and live stream a call by dialing into a RealPresence Centro system from a RealPresence Media Suite portal. If users have access to a RealPresence Media Suite portal, they can log in to the portal to dial in to a system from which they want to record a call. This method is also ideal for an administrator of a remote system. For information about using this method, refer to the *Polycom RealPresence Media Suite, Appliance Edition User Guide* or *Polycom RealPresence Media Suite, Virtual Edition User Guide* at support.polycom.com.

Users can also remotely record calls in the following ways:

- **Dial RealPresence Media Suite directly**: Use the default recording settings defined by a RealPresence Media Suite administrator. Before recording a call using this method, users must obtain the IP address, H.323 extension, or SIP URL of the RealPresence Media Suite.
- **Dial a RealPresence Media Suite Video Recording Room (VRR)**: A VRR is a virtual capture server with a specific recording profile that is defined by a RealPresence Media Suite administrator. Before recording a call using this method, users must obtain the VRR number and the IP address, H.323 ID, or SIP address of the RealPresence Media Suite.

When a recording is initiated remotely from the RealPresence Media Suite user portal, users cannot control the recording from the system.

For more information on recording with these two methods, refer to the *Polycom RealPresence Centro User Guide*.

If you have access to a RealPresence Media Suite portal, you can use additional features, such as copying the URL for a recording to share with others. For more features, see the *Polycom RealPresence Media Suite User Guide* at support.polycom.com.

The following connection methods are supported for dialing a RealPresence Media Suite.

Media Suite Type	Connection Method	Example
Media Suite system	If the both the video conferencing system and the RealPresence Media Suite system are not registered to the gatekeeper or to a SIP server, dial the RealPresence Media Suite IP address.	10.11.12.13
	If both the video conferencing system and the RealPresence Media Suite system are registered to a gatekeeper, dial the RealPresence Media Suite E.164 extension for H.323.	1234
	If both the video conferencing system and the RealPresence Media Suite system are registered to a SIP server, dial the RealPresence Media Suite SIP address.	CS123

Media Suite Type	Connection Method	Example
VRR	For SIP calls: [VRR number]@[RealPresence Media Suite IP] or [SIP peer prefix][VRR number]	If the RealPresence Media Suite IP is 11.12.13.14 and the VRR number is 4096,dial 11.12.13.14##4096. If the SIP peer prefix of the RealPresence Media Suite is 8888 and the VRR number is 4096, dial 88884096.
	For H.323 calls: [RealPresence Media Suite IP]##[VRR number] or [RealPresence Media Suite E.164 prefix][VRR number]	If the RealPresence Media Suite IP is 11.12.13.14 and the VRR number is 4096,dial 11.12.13.14##4096. If the RealPresence Media Suite E.164 prefix is 8888 and the VRR number is 4096, dial 88884096.

Customizing the Local Interface

Topics:

- Change the Background Image on the Home Screen
- Change the Startup Image on the Home Screen
- Set Up the Address Bar

These topics describe how to configure your system by using the configuration screens on the local interface. If you are in the room with the system, you can navigate the screens and enter information by using the remote control and the onscreen keyboard. When you reach a text field, press the **Select** button on the remote control to display the onscreen keyboard. Note that the onscreen keyboard is automatically displayed when you reach the **System Name** field in the setup wizard.

Be aware that only those configuration screens needed to get the system connected are included in the local interface. Most of the administrative settings are available only in the system web interface.

In the system's local interface, go to ⚙ > **Settings** > **Administration**. The local interface has a subset of the administration settings that are available in the system web interface.

If you enable a provisioning service, any settings provisioned by the RealPresence Resource Manager system might be displayed as read-only settings in the system web interface **Admin Settings**. For more information about automatic provisioning, refer to the RealPresence Resource Manager system documentation at support.polycom.com.

Change the Background Image on the Home Screen

You can upload a custom image to display as the background of all monitors on the RealPresence Centro system. The image must have a pixel size of 1920 x 1080 (width by height) in a .jpg file format, and a file size less than 5 MB.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **Background**.
2. Browse to the desired image file and click **Choose File** > **Upload**.

   The custom image displays on all four monitors.

Change the Startup Image on the Home Screen

The system local interface displays a default background image when the RealPresence Centro system first powers on. You cannot delete this image, but you can upload your own image to replace it. When you change the image in the system web interface, the new image also appears on the RealPresence Touch device.

You must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **Startup Background**.
2. Click **Choose File** to search for and select the image you want to upload.
3. When the image name appears next to **Choose File**, click **Upload**.

Set Up the Address Bar

You can customize where address bar elements appear on the Home screen of the RealPresence Centro system local interface.

The system local interface displays an address bar at the bottom of the Home screen. The address bar can contain the following information:

- None
- IP Address
- H.323 Extension
- SIP Address
- Pairing Code

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **Address Bar**.
2. Configure the following settings.

Setting	Description
Address Bar (Left Element)	Allows you to select which element you want displayed on the left side of the address bar on the local interface. The choices are: • None • IP Address • 323 Extension • Pairing Code
Address Bar (Right Element)	Allows you to select which element you want displayed on the right side of the address bar on the local interface. The choices are: • None • SIP Address • 323 Extension • Pairing Code

Calling

Topics:

The following topics describe how to make calls.

Call a Favorite Contact

In the RealPresence Centro system web interface, at **Place a Call**, you can call a favorite contact.

Procedure

1. In the **Contacts** section, enter a name and click **Search**.
2. Select a contact name and click **Call**.

Call a Speed Dial Contact

In the RealPresence Centro system web interface on the **Place a Call** screen, you can call Speed Dial contacts and can edit the **Speed Dial** contact list. After you have enabled **Speed Dial**, users can use it as a shortcut for calling a contact.

Procedure

» In the **Speed Dial** section, select a contact from the list and click **Call**.

To place a call within your company's telephone system, enter the internal extension instead of the full number.

Call a Recent Call Contact

On the RealPresence Centro system web interface Place a Call screen, you can place calls to Recent Call contacts.

Procedure

» In the system web interface Place a Call screen's **Recent Calls** section, do one of the following:

- Find an entry and click the **Call** link next to the entry.

- Click **More** to view a list of calls with more details, then select an entry and click **Call**.

Place a Call

In the RealPresence Centro system web interface, at **Place a Call**, you can place a call manually.

Procedure

1. Click **Manual Dial**.
2. Enter the number.
3. Click **Call**.

   The call is placed according to the default settings you selected in **Admin Settings** > **Network** > **Dialing Preferences**. You can select settings other than the defaults in the two lists below the text entry field.
4. To require a password, select **Meeting Password** and enter a password in the field that displays below the check box.

Searching Directory Contacts to Call

Directory contacts are called “global contact entries” in the RealPresence Centro system local interface. These global contact entries are assigned to a default global Favorites group named Global Entry. The global directory contains address book entries downloaded from an enabled global directory server.

You can search the global directory to return a list of all global directory entries that match your search criteria, then select contacts in the global directory to call. Up to 200 search results can be displayed at a time from a Polycom Global Directory Service (GDS) or Lightweight Directory Access Protocol (LDAP) global directory.

To browse LDAP global directory entries, LDAP must be enabled through Polycom RealPresence Resource Manager. If LDAP is not enabled through RealPresence Resource Manager, you can still search the global directory, but you cannot browse the global directory.

Browse Global Contact Entries to Call

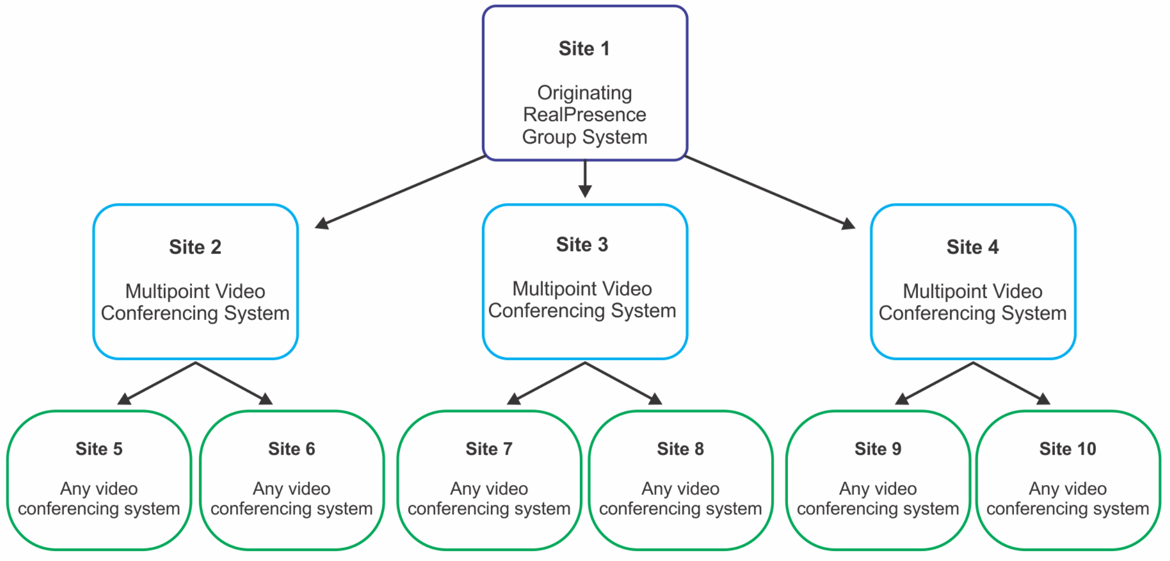
You can browse the global contact entries to call in the global directory in the RealPresence Centro system web interface.

Procedure

1. **In the system web interface, s**elect **Place a Call** > **Contacts**.
2. At **Search**, enter a contact name and click **Search**.
3. Select **Call** to place a call or select an entry to view the contact's information.

Place a Cascaded Call

From your RealPresence Centro system, you can include multiple sites in a cascaded call if the sites you call have internal multipoint capability.


Site 1
Originating RealPresence Group System
Site 2
Multipoint Video Conferencing System
Site 3
Multipoint Video Conferencing System
Site 4
Multipoint Video Conferencing System
Site 5
Any video conferencing system
Site 6
Any video conferencing system
Site 7
Any video conferencing system
Site 8
Any video conferencing system
Site 9
Any video conferencing system
Site 10
Any video conferencing system

Keep the following points in mind regarding cascaded calls:

- H.239 is not supported in cascaded calls.
- Cascaded multipoint is not supported in SIP calls.
- HD and SD multipoint are not supported when the system hosts a cascaded call.
- You cannot change the near-end layout.
- The encryption padlock icon might not accurately indicate whether a cascaded call is encrypted.
- You cannot call a group of contacts by using Speed Dial or Favorites to call the group.
-

Procedure

1. Create and call a group in the directory, or place calls one at a time to several other sites.
2. Ask each far site to call additional sites.

   Along with these additional sites, each far site in the original multipoint call can add one audio-only connection.

Setting Up a Polycom RealPresence Touch Device

Topics:

The following topics provide information on how to enable and set up a Polycom RealPresence Touch device.

Positioning the RealPresence Touch Device

Ensure that the RealPresence Touch is conveniently located for use during a meeting, such as on a conference table, so that systems can be controlled by the Polycom RealPresence Touch device. Place the device in a location where you can easily touch the screen and see the RealPresence Centro system monitor displays. The RealPresence Touch device can be positioned horizontally at either a 30 degree or 65 degree viewing angle.

Run the RealPresence Touch Device Setup Wizard

Before you can pair the RealPresence Touch device to a RealPresence Centro system, you must set up the hardware and use the set up wizard.

Procedure

1. Ensure that you have completed the setup wizard on the system.
2. Connect the Ethernet cable to the RealPresence Touch.
3. Plug the Ethernet cable into the wall outlet:

- If your room provides Power Over Ethernet, you can connect the Ethernet cable directly to a LAN outlet.
- If your room does not provide Power Over Ethernet, you must connect the Ethernet cable to the power supply adapter. Then connect the power supply adapter to a LAN outlet and power outlet.The RealPresence Touch powers on and displays the language selection screen.

4. Choose your language and follow the onscreen instructions.
5. After the RealPresence Touch connects to the network, enter the system IP address at **Device Address**, then enter the **Admin ID** and **Password**.
6. Tap **Pair**.

   If the system is configured to allow pairing and you entered the IP address, admin ID and password for the system correctly, the RealPresence Touch device pairs with the system. When pairing is successful, the RealPresence Touch splash screen is displayed, followed by the home screen.

Power Off the RealPresence Touch

If you need to move your RealPresence Touch device to another area, power off the device before you disconnect the Ethernet cable.

Procedure

1. On any screen, tap ☰ **Menu**, **Settings**, and then **Administration**.
2. Sign in using your Admin ID and password.
3. Scroll down to **Power and Pairing**.
4. Touch RealPresence Touch Power until a Shutting down... message displays.

   The RealPresence Touch is powered off.

Wake the RealPresence Touch

The RealPresence Touch goes to sleep after two minutes of inactivity. To wake it, you can touch the screen.

Procedure

» Touch the screen.

The last screen that was displayed before the sleep state is displayed.

Enable the RealPresence Touch Device

Before your users can control the system with the RealPresence Touch device, you must enable the device on the RealPresence Centro system's web interface. Once the device is enabled, you can pair it to the system.

Procedure

1. On the system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **Polycom Touch Device**.

2. Select the **Enable Polycom Touch Device** check box and click **Save**.

   Note that only one device can be paired to a system at a time.

Pairing the Device

When you configure the RealPresence Touch to pair with a particular RealPresence Centro system, the RealPresence Touch makes an IP connection to the room system. If the connection is lost, the RealPresence Touch automatically attempts to restore the connection.

After you have completed RealPresence Touch setup, you can pair to a different system using RealPresence Touch settings.

Pairing States

The following table describes the pairing and connection states:

State	Description
Unpaired	The RealPresence Touch is not associated with a system.
Paired and Connected	The RealPresence Touch is associated with a system through the pairing process. This is normal operating mode. A RealPresence Touch can be connected to only one system at a time.
Paired and Disconnected	The RealPresence Touch is associated with a system, but communication is disrupted, usually because of a system power off or LAN issue. Communication is automatically restored when a system and the touch device are successfully connected to the LAN.

Pair For the First Time

To pair your RealPresence Touch with a RealPresence Centro system that has not been paired before, you must enter the system's credentials before connection can be established.

Procedure

1. After completing the out-of-box (OOB) setup wizard, the RealPresence Touch displays the pairing screen.
2. Tap the **Manually Pair** tab.
3. Enter the **IP Address**, **Admin ID**, and **Password** for the system.
4. Tap **Pair**.

   The pairing connection begins, and the Home screen displays when the pairing is successful.

Pair to a Previously Paired System

If you have paired with a RealPresence Centro system before, you can select it from a previously paired list of systems. You do not have to enter the system credentials again, unless the credentials have changed.

Procedure

1. On the Home screen, tap ☰ **Menu**, **Settings**, then **Administration**.
2. Sign in using your admin ID and password.
3. Scroll down to **Power and Pairing** and tap **UNPAIR AND RETURN TO PAIRING SCREEN**.
4. On the **Recently Paired** tab, tap the system that you want to pair with.

   The pairing connection begins, and the Home screen displays when the pairing is successful.

   If you unpair from the system, any current calls on the system are still active. To hang up the calls, repair to the room system and select **More Options**, then **Participants**, **More Options**, and **Remove** or **Remove All**.

After the room system and the RealPresence Touch are paired, the system web interface and the RealPresence Touch interface display information about each other and about their connection status.

Unpair a RealPresence Touch

You can unpair the RealPresence Touch and a RealPresence Centro system.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **Polycom Touch Device**.
2. Clear the check box next to **Enable Polycom Touch Device**.
3. Click **Save**.

   The system cannot pair with any touch device while the **Enable Polycom Touch Device** check box is cleared.

Remove a System from the Paired System List

After attempting to pair a device, a “Cannot Pair as a Dedicated Device” message might be displayed. This means that another device is already paired to the same RealPresence Centro system. An administrator can determine which device is paired and can unpair the device using the system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **Polycom Touch Device**.
2. Click **Forget this Device**.
3. Click **Save**.

   Now you can pair another system.

Managing the RealPresence Touch Device

You can remotely manage certain features of your RealPresence Touch when it is paired to a RealPresence Centro. For a list of supported browsers, refer to the *Polycom RealPresence Centro Release Notes*.

You can manage the following features remotely:

- **Download Logs**: Downloads the RealPresence Touch logs to the location specified in the device.
- **Network Settings**: Specifies whether the system acquires an IP address automatically or manually. With the manual method, the other settings that are available from the RealPresence Touch become available on the web.
- **Pair**: Pairs and unpairs from systems. Before you can connect to or pair with a device, you must know the device's IP Address and the User Name and password used to connect.
- **Security**: Changes the admin ID and password of the RealPresence Touch.
- **Software Updates**: Updates the RealPresence Touch software. You can update from the default Polycom server or your own server by entering the appropriate IP address.
- **View RealPresence Touch Screens**: Shows the screen currently being displayed on the RealPresence Touch. You can click **Refresh** at any time to see if the screen has changed.

Open a Remote Management Window

You can open a remote management window for your RealPresence Touch in a RealPresence Centro system web browser.

Procedure

1. In a web browser, enter the IP address of the RealPresence Touch device.
2. In the login window, enter the **ID** and **Password** you use to access the administrative features of the RealPresence Touch.

   You can access the remote management features by using the Navigation menu or the Dashboard. To return to the **Dashboard**, click the Home icon.

Pair Using RealPresence Touch Web Interface

To pair your RealPresence Touch with a RealPresence Centro system, you must enter the system's credentials before connection can be established.

Procedure

1. In the RealPresence Touch web interface, click **Pairing**.
2. At **Device**, select **RealPresence Centro**.
3. Enter the **IP Address or Host Name**, **User Name**, and **Password** for the system.
4. Click **Pair**.

   The pairing connection begins, and the Home screen displays when the pairing is successful.

Unpair Using the RealPresence Touch Web Interface

You can unpair the RealPresence Touch and a RealPresence Centro system.

Procedure

1. In the RealPresence Touch web interface, click **Pairing**.
2. Click **Unpair**.

Change the RealPresence Touch User Name and Password

You can change the security credentials for the RealPresence Touch device.

Procedure

1. In the RealPresence Touch web interface, click **Security**.
2. At **Admin ID**, enter your admin ID.
3. At **Current Password**, enter the current password.
4. At **Password**, enter the new password.
5. At **Confirm Password**, reenter the new password.
6. Click **Save**.

Enable Recent Calls and Speed Dial

You can enable the recent calls and speed dial icons in the RealPresence Centro system web interface.

- **Recent Calls**: In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Recent Calls**. Select the **Enable Recent Calls** checkbox.
- **Speed Dial**: In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **Speed Dial**. Select the **Enable Speed Dial** checkbox.

Customize the RealPresence Touch Screens

You can use the RealPresence Centro system web interface to configure how information is displayed on the Home screen of the RealPresence Touch device. These settings are included in the System settings profile, and included in bundled provisioning when using RealPresence Resource Manager.

You can configure the RealPresence Touch home screen in the system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **RealPresence Touch Home Screen Configuration**.
2. Configure the settings on the Home Screen Settings screen that are described in the following topics.

Choose the Home Screen Icons

You can choose home screen icons for your RealPresence Centro system local interface. By default, two icon buttons appear in the lower center of the RealPresence Touch Home screen; users see only the **Place a Call** and **Show Content** icons. However, you can customize the number of screens and Home screen icons in a preferred order. Once you customize the Home screen configuration, users can scroll through one to three Home Screens, with up to three icons on each screen.

Procedure

1. In the web user interface, go to **Admin Settings** > **General Settings** > **Pairing** > **RealPresence Touch Home Screen Configuration**.

2. Under **Configure Home Screen**, click **Configure Home Screen Options**.
3. At **Home screen 1** > **Button 1,** select one to three icon buttons to appear per screen in your preferred order.

   You can select from the following icon buttons:

   - None (no icon)
   - Place a Call
   - Show Content
   - Keypad
   - Contacts
   - Speed Dial
   - Recent
   - System Information
   - User Settings
   - Administration
4. If you want to include more than one Home screen, continue selecting icon buttons for **Home Screen 2** and **Home Screen 3** until all screens are configured.

   For example, **Home Screen 1** > **Button 1** > **Recent Call Button 2** > **Place a Call** > **Button 3** > **Contacts**.
5. To save your selections, click **Save**.

   Your new selections should display on the Home screens of the RealPresence Touch device.

Choose the Place a Call Screen Icons

You can customize the **Place a Call** screen to display certain icon buttons for your RealPresence Centro system. Since there are four ways to place a call by default, after you tap the **Place a Call** button, all the selections display on the screen. You can customize one of the icon buttons to be the default. All of the other **Place a Call** icon buttons continue to display at the top of the screen.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Pairing** > **RealPresence Touch Home Screen Configuration**.
2. Under **Configure Home Screen**, click **Place A Call Screen**.
3. Under **Select Preferred Sub Menu**, choose from the following:
   - Keypad
   - Contacts
   - Recent Calls
   - Speed Dials
4. Click **Save**.

   Your new selections should display on the RealPresence Touch Place a Call screen.

   To revert back to the default icons, at **Configure Home Screen**, select **Default Configuration**, and click **Save**.

Change the Background Image

The RealPresence Touch device allows you to upload a custom background image that is separate from the RealPresence Centro system monitor background. If a custom image is not loaded, the image from the primary system screen displays as the RealPresence Touch device background when it is paired with the system (default behavior). To create a custom background on the RealPresence Touch, you must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format that is less than 5 MB.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **Home Screen Settings** > **RealPresence Touch Background**.
2. Browse to the desired image file and click **Choose File** > **Upload.**

   The custom image displays paired RealPresence Touch Home screen.

Setting Up and Configuring Directory Servers for the RealPresence Touch

The global directory provides a list of other systems that are registered with the Global Directory Server and available for calls.

The other systems appear in the directory, allowing users to place calls to other users by selecting their names.

Set Up Directory Servers for the RealPresence Touch

You can use the RealPresence Touch device to set up directory servers.

Procedure

1. In the RealPresence Touch web interface, go to **Admin Settings** > **Servers** > **Directory Servers**.
2. Configure the following settings:

Directory Servers Supported	Authentication Protocols	Global Directory Groups	Entry Calling Information
Microsoft Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: • SIP address (SIP URI)

Directory Servers Supported	Authentication Protocols	Global Directory Groups	Entry Calling Information
LDAP with H.350 or Active Directory	Any of the following: • NTLM v2 only • Basic • Anonymous	Not Supported	Might include: • 323 IP address (raw IPv4 address, DNS name, H.323 dialed digits, H. 323 ID, or H. 323 extension) • SIP address (SIP URI) • ISDN number • Phone number*
Polycom GDS	Proprietary	Not Supported	Might include: • 323 IP address (raw IPv4 address, DNS name, or H.323 extension) • ISDN number

* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats:

- +Country Code.Area Code.Number
- +Country Code.(National Direct Dial Prefix).Area Code.Number

You can configure the system to use the following directory server when the system is automatically provisioned by a RealPresence Resource Manager system.

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: • SIP address (SIP URI)

* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats:

- +Country Code.Area Code.Number
- +Country Code.(National Direct Dial Prefix).Area Code.Number

Updating Software

The RealPresence Touch must run a software version that is compatible with the software version on the RealPresence Centro system.

The RealPresence Touch, after pairing with the system, verifies the compatibility of the RealPresence Touch panel and operating system software and requests a software update.

For additional details on software compatibility, refer to the appropriate version of the release notes available at Polycom Support.

If you need to update your system at the same time you update the Polycom touch device, update the system software first.

Update files for the RealPresence Touch are located on the Polycom support server. You can store the update files on a USB device, RealPresence Resource Manager system, or on your own web server. No license number or key is needed to update the RealPresence Touch.

You can configure the Polycom touch device to get software updates using any of the following methods:

- A Polycom RealPresence Resource Manager system
- A server on your network
- The online software server hosted by Polycom
- A USB 2.0 storage device in FAT32 format that you connect to the side of the device

Dynamic Polycom Touch Device Software Updates

You can post software for a Polycom touch device on a RealPresence Resource Manager system. Then, configure the device to get updates from the applicable RealPresence Centro system by entering the Production URL or Trial URL on the device Software Update screen.

When using a RealPresence Resource Manager system to automatically update the software for a system with an associated Polycom touch device, use the same management server for the touch device updates. This helps you control the version of software installed on the touch device.

When a Polycom touch device is connected to a provisioned system, a RealPresence Resource Manager can receive status updates from and provide software updates to the touch device. For supported RealPresence Resource Manager versions, go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html and click **Current Interoperability Matrix**.

For information about configuring production and trial versions of software update packages, refer to the *Polycom RealPresence Resource Manager System Operations Guide* available at support.polycom.com.

Configure Your Web Server as the Update Site

You can post software to your web server and then configure the RealPresence Touch device to receive updates.

Procedure

1. Make sure that your server enables clients to download files with the following extensions or with no extension:
   - `.tar.gz`
   - `.txt`

   - `.sig`
   - .plcm
2. Define a URL on your server that the RealPresence Touch can use for software updates, and create a corresponding root directory to it.
3. Go to support.polycom.com, and navigate to the page for the system that you use with the RealPresence Touch.
4. Save and extract the RealPresence Touch operating system software package (.tar file) from the Polycom website to the root directory of the web server.

Managing Polycom Touch Device Software on Your Server

When checking for software updates on your server, Polycom touch devices check only for what is referred to as the “current” release of the RealPresence Centro system software. By default, the current release is the software distribution package that was most recently extracted on your server.

Over time, you might extract other versions of the software on your server, resetting the current release with every extraction. In addition, you could accumulate multiple versions of the same software.

Each software distribution package contains two commands that you can use to maintain all of the software extracted on your server.

- The `setcurel` command sets a specific version of software as the current release.
- The `removerel` command removes a specific version of a software release from your server.

Set a Software Version as Current

Use the `setcurrel` command to set a specific version of RealPresence Touch software as the current release on your server.

Procedure

1. Run the `setcurrel` command with X.X.X-XXX as the software version you want to set as the current release:
   - Unix or Linux: `<root dir>/vega/platform/setcurrel.sh X.X.X-XXX`
   - Windows: `<root dir>\vega/platform/setcurrel.bat X.X.X-XXX`
2. Follow the onscreen instructions for setting the current release.

Remove a RealPresence Touch Software Version

Use the `removerel` command to remove a specific version of a RealPresence Touch software release from your server.

Procedure

1. Run the `removerel` command with X.X.X-XXX as the software version you want to set remove from the server:
   - Unix or Linux: `<root dir>/vega/platform/setcurrel.sh X.X.X-XXX`
   - Windows: `<root dir>\vega/platform/setcurrel.bat X.X.X-XXX`
2. Follow the onscreen instructions for setting the current release.

Update Software from the Web Interface

Using the RealPresence Centro system web interface, you can update the RealPresence Touch software from the Polycom server or your own server.

Procedure

1. Open a supported browser.
2. Configure the browser to allow cookies.
3. In the browser address line, enter the IP address of the RealPresence Touch using the format http://IPaddress (for example, http://10.11.12.13).
4. If necessary, enter the Admin ID as the user name (default is admin), and then enter the Admin remote access password, if one is set.

   The default password is the RealPresence Touch serial number.

   The first time you open the system web interface each day, you might need to enter a user name and password after you select any of the interface options.
5. On the Home Page, click **Software Update**.
6. Enter the server address for the update.

   The default server address, `polycom`, is the address for the Polycom public soft-update repository and has the latest released software version available.
7. Click **Save** to save these changes.
8. Click **Check for Software Updates**.
9. Click **Download and Install Software**.

   Download progress is displayed during installation.

Update Software from the Local Interface

Using the RealPresence Touch interface, you can update the RealPresence Touch software from the Polycom server or your own server.

Procedure

1. From the Home screen, touch ⚒ **Administration** and then touch **Software Update**.
2. Enter the path and address of the update site where you posted the RealPresence Touch software in the in the Server Address field.

   To use the Polycom server, enter `polycom`.
3. Touch **Check for Software Updates**.
4. Touch **Download and Install Software**.

Update RealPresence Touch Software from a USB Storage Device

You can update the RealPresence Touch quickly using a USB storage device without updating the RealPresence Touch factory restore partition.

Procedure

1. Open a browser and navigate to support.polycom.com.
2. Under **Documents and Downloads**, select T**elepresence and Video**.
3. Navigate to the page for the system that you use with the RealPresence Touch.

4. Save the RealPresence Touch operating system software package (.tar) file from the Polycom website to the root directory of the USB device.
5. Ensure the RealPresence Touch Ethernet cord is connected and the RealPresence Touch is powered on.
6. Connect the USB device to the side of the RealPresence Touch.
7. An automatic prompt asks you if you want to update the platform software.

   Touch **Yes**.

Update the Software and the Factory Restore Partition From a USB Storage Device

You can use a USB storage device to update RealPresence Touch software and the RealPresence Touch factory restore partition.

If you cannot update your RealPresence Touch device using a server or with RealPresence Resource Manager, you can load the software onto a USB storage device and use that to update the device. Another benefit of using a USB device is that you can choose to perform both a factory restore and update your device software simultaneously.

The following attributes ensure that your USB device supports the software update procedure:

- Use USB 2.0 devices (some USB 3.0 devices might not work with the RealPresence Touch).
- Format the primary partition as FAT32.
- Place all software update data into the root directory of the primary partition.

Procedure

1. Open a browser and navigate to support.polycom.com.
2. Under **Documents and Downloads**, select **Telepresence and Video**.
3. Navigate to the page for the version of the system that you use with the RealPresence Touch.
4. Save the RealPresence Touch operating system software package (.tar) file from the Polycom website to the root directory of the USB device.
5. Disconnect the Ethernet power cable from the RealPresence Touch.
6. Connect the USB device to the side of the RealPresence Touch.
7. Press and hold the RealPresence Touch factory restore button with a bent paper clip for ten seconds and simultaneously reconnect the Ethernet power cable to the RealPresence Touch.
8. Follow the on-screen instructions of the setup wizard to complete the update.

   The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the factory restore button.

Restart the RealPresence Touch Device

You can restart the RealPresence Touch device when it is paired with a RealPresence Centro system from the touch device.

Procedure

1. On the RealPresence Touch device, navigate to **Settings** > **Administration**.
2. Enter the administrator password.
3. Tap **Restart Touch Controller**.

Restart a System from a RealPresence Touch Device

When the RealPresence Centro system is paired with a RealPresence Touch device and is enabled for Skype for Business, you can restart the room system using the RealPresence Touch device.

Procedure

1. On the RealPresence Touch device, navigate to **Settings** > **Administration**.
2. Enter the administrator password.
3. Under RealPresence Centro, tap **Restart Room System**.

Troubleshooting on the RealPresence Touch Device

You might need to do some troubleshooting on your RealPresence Touch device. For information on troubleshooting, see the following topics.

View System Details and Connection Status

You can view certain RealPresence Centro system details about the paired system on the RealPresence Touch; this information might be useful for troubleshooting or for technical support.

Procedure

1. On any screen on the RealPresence Touch, tap **Menu** and then **Settings**.

   The **System Information** screen is displayed.
2. Under **Device Connection Status**, tap the room system that you want information on.

System details and connection status information is listed for the connected room system.

View Call Statistics

When your RealPresence Centro system is paired with a RealPresence Touch, you might want to view certain call statistics, such as bitrates, compression formats, and packet loss during a call.

Procedure

1. During a call, on any screen, tap **Call Statistics** (located at the top left of your screen).

   Call statistics for each stream in the current call are now displayed.
2. To view statistics for another call participant, switch to that participant and tap **Call Statistics** again.

   To view more information about a specific stream, navigate to the desired stream and tap **More Information**.

Download RealPresence Touch Logs

You can download RealPresence Centro system logs using the RealPresence Touch.

Procedure

1. In the RealPresence Touch web interface, click **Download Logs**.

2. A .tar file is downloaded to your local computer.

   You can extract the file and open it to review the log information.

Transfer RealPresence Touch Logs to a USB Storage Device

You might find log files useful when troubleshooting. You can transfer RealPresence Touch logs to a USB storage device. The USB storage device must be in FAT32 format.

Procedure

1. Insert a USB storage device into the RealPresence Touch device.
2. On the RealPresence Touch device, do one of the following:
   - Tap **Administration** and enter the user name and password for the device.
   - Tap **Menu > Administration** and enter your user name and password.
3. Tap **Transfer RealPresence Touch Logs to USB Device**.

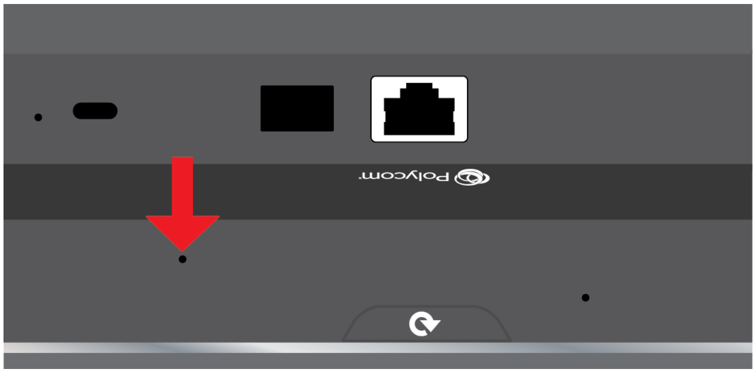
   A message displays while the logs are being transferred to the USB storage device.

   After a success message displays, click **OK**.

Perform a Factory Restore on the RealPresence Touch

If the RealPresence Touch device is not functioning correctly or you have forgotten the Administration password, you can use the factory restore button to reset the device. This operation completely erases the RealPresence Touch device's settings and reinstalls the default platform and applications. Do not power off the device during the factory restore process.

The restore button pinhole is on the back of the RealPresence Touch, as shown in the following figure.



Procedure

1. Disconnect the ethernet cable to power off the device.
2. Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
3. Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
4. Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
5. Follow the instructions on the setup wizard.

   When the process is complete, the device displays the splash screen and then the home screen.

Perform a Factory Restore Using a USB Storage Device

If you want to install a particular software build on the RealPresence Touch, you can perform a a factory restore using a USB storage device. Do not power off the device during the factory restore process.

Procedure

1. Copy a build package (`.tgz` file) to the root directory of a USB storage device.
2. Disconnect the ethernet cable to power off the device.
3. Insert the USB storage device into the side USB port of the device.
4. Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
5. Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
6. Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
7. Follow the instructions on the setup wizard.

   When the process is complete, the device displays the splash screen and then the home screen.

Test the Software Download URL

If your RealPresence Centro system or Polycom touch device is not updating properly, and you entered `polycom` as the Server Address, the system resolves downloads.polycom.com to an IP address. The system then checks for a software update using http.

Procedure

1. Open a browser.
2. Try to access the appropriate URL for your system or device.

System or Device	Test URL
RealPresence Touch	http://downloads.polycom.com/video/rp_touch/vega/info.txt
RealPresence Centro	https://downloads.polycom.com/video/centro/rseries/info.txthttps://downloads.polycom.com/video/centro/millennium/info.txt

3. If the computer returns `platform`, or `apps` and `platform`, you can reach the Polycom software server from your location and the URL is working.

System Maintenance

Topics:

The following topics describe how to set up a system profile, perform a factory restore, and upgrade the system software.

Managing System Profiles

If you manage systems that support multiple applications, you can use profiles to change RealPresence Centro system settings. You can store a system profile on a computer as a `.profile` file using the system web interface. The number of profiles you can save is unlimited. Polycom recommends only using profiles as a way to back up system settings. Attempting to edit a stored profile or upload a stored profile from one system to a different system can result in instability or unexpected results.

The following settings are included in a profile:

- Home screen settings
- User access levels
- Icon selections
- Option keys
- System behaviors

Passwords are not included when you store a profile.

Store a Setting Profile

You can store the current setting profile on your computer.

Procedure

1. In the system web interface, go to **Utilities** > **Services** > **Profile Center**.
2. Click **Download** next to **Current Settings Profile** to download the profile file from the RealPresence Centro system.
3. Save the file to a location on your computer.

Upload a Profile

You can upload a setting profile from your computer.

Procedure

1. Reset the RealPresence Centro system to restore default settings.
2. In your web browser address line, enter the system's IP address.
3. In the system web interface, go to **Utilities** > **Services** > **Profile Center**.
4. Next to **Upload Settings Profile**, click **Browse** and browse to the location of the profile .csv file on your computer.
5. Click **Open** to upload the .csv file to your system.

Resetting and Restoring a RealPresence Centro System

If the RealPresence Centro system is not functioning correctly or you have forgotten the Admin Room Password, you can reset the system with **Delete System Settings** enabled. This procedure effectively refreshes your system, deleting all settings except the following:

- Current software version
- Remote control channel ID setting
- Directory entries
- CDR data and logs

Reset a RealPresence Centro System

You can reset a RealPresence Centro system in the local interface.

Procedure

1. Go to **Settings > System Information > Diagnostics > Reset System**.
2. Enable **Delete System Settings**.
3. Click **Reset System**.

   After about 15 seconds, the system restarts and displays the setup wizard.

Perform a Factory Restore on the RealPresence Centro System

If the RealPresence Centro system is not functioning correctly, you can use the factory restore button to reset the system.

The factory restore operation completely erases the system's flash memory and reinstalls the software version and default configuration stored in its factory partition. The following items are erased from the system:

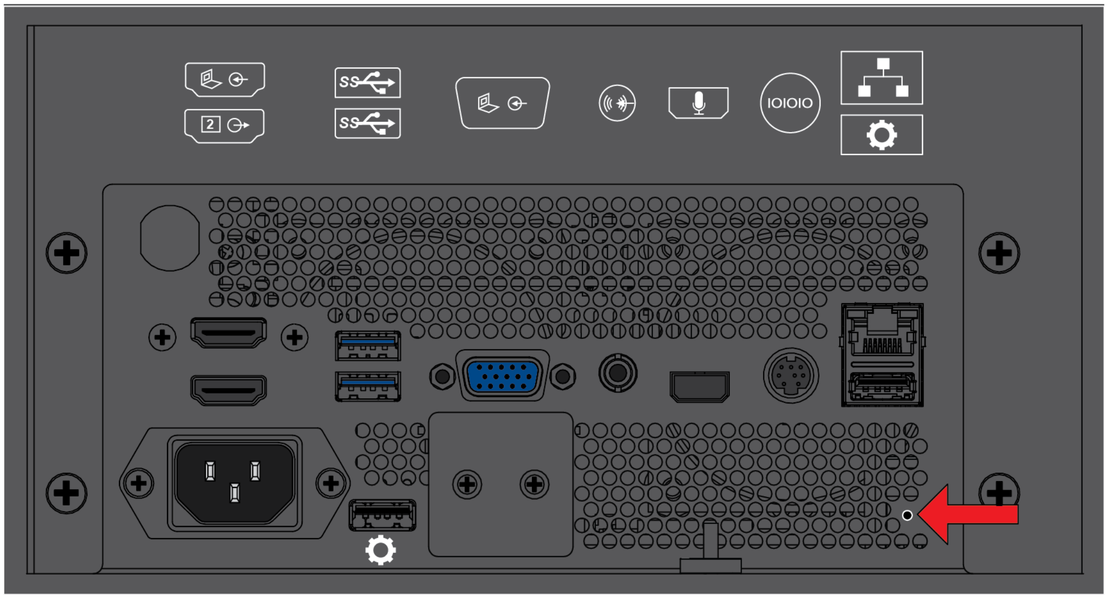
1. Software updates
2. All system settings including option keys and the remote control channel ID
3. Directory entries
4. CDR data

Procedure

1. Power off the system by using the power button on the front of the system. Do not unplug the power cord.

2. Straighten a paper clip and use the paper clip to press and hold the factory restore button.

   The restore button is located on the base of the system beneath the LAN port, as shown in the following figure.



3. While continuing to hold the restore button, press the power button and power on the system.
4. Continue holding the restore button until the base flashes blue and amber lights, then release it.

   The screen might stay blank for up to 3 minutes, and then displays the softupdate progress until the factory restore is complete. During this process, do not power off the system. When it is complete, the system restarts automatically.

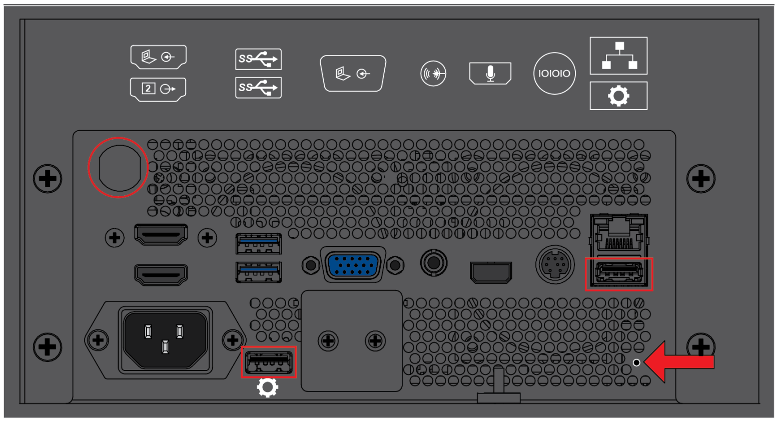
Perform a Factory Restore Using a USB Storage Device

When you use the restore button to perform a factory restore, the system is restored to the software version placed on the system in the factory. You can perform a factory restore on the RealPresence Centro using two USB storage devices if you want to restore the system to the current software version, an earlier software version that is not the factory version, or change the default restore software version. The USB storage device must be in FAT32 format.

Procedure

1. Copy the software package (.tar file) and the software key (sw_keys.txt file) to the root directory of two different USB storage devices.
2. Power off the system. The power button is shown with a red circle in the following figure.
3. Insert the two USB storage devices into two service USB ports on the system. These ports are shown with red rectangles in the following figure.
4. Straighten a paper clip and use the paper clip to press and hold the restore button.

   The restore button is shown with the red arrow in the following figure.



5. While continuing to hold the restore button, press the power button and power on the system. During the factory restore process, the system indicators flash blue and amber, and the softupdate progress screen displays until the restore is complete. Do not power off the system during the factory restore process. When the process is complete, the system restarts automatically.
6. When the LEDs have stopped flashing and the install wizard (out of box) screen displays, the factory restore process is complete.

After the factory restore process is complete, remove the USB storage devices from the system. If you used a software version later than the factory software version, the software version used during the restore is now the default version for a factory restore of the system.

Delete Data and Configuration System Files

You can remove sensitive data and configuration information from the RealPresence Centro system for security purposes.

Procedure

1. Power off the RealPresence Centro system by holding down the Power sensor for 3 to 5 seconds.
2. Unplug all network connections.
3. Perform a factory restore.
4. Wait for the system to start up and display the setup wizard.
5. Power off the system.

System Log Files

System log files are essential when troubleshooting RealPresence Centro system issues. System log files contain information about system activities and the system configuration profile. After setting up system logging, you can retrieve a system log file.

View Log File Status

You can view the log file status for your RealPresence Centro system in the system web interface.

Procedure

» In the system web interface, go to **Diagnostics > System > System Status** and select the **More Info** link for **Log Threshold**.

Configure System Log Management

When the RealPresence Centro system log fills up past the threshold, the following actions are triggered:

- Transfers the log to the USB device if Transfer Frequency is set to “Auto at Threshold”
- Creates a log entry indicating that the threshold has been reached
- Displays an alert on the home screen
- Displays an indicator on the System Status screen

Note: When the Log Threshold system status indicator is red, automatic log transfers cannot be completed and data might be lost. You must manually transfer the logs to a USB storage device.

Procedure

1. In the system web interface, go to **Admin Settings > Security > Log Management**.
2. Configure these settings and click **Save**.

Setting	Description
Current Percent Filled	Displays how full the log file is, as a percentage of the total size.
Percent Filled Threshold	Specifies a threshold for the percent filled value. Reaching the threshold triggers an alarm, creates a log entry, and transfers the log if **Transfer Frequency** is set to **Auto at Threshold**. **Off** disables logging threshold notifications.
Folder Name	Specifies the name to give the folder for log transfers. Select one of the following: • **System Name and Timestamp**—Folder name is the system name and the timestamp of the log transfer, in the date and time format specified on the Location screen. For example, if the system name is “Marketing”, the folder name could be marketing_MMddyyyymmssSSS. • **Timestamp**—Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example yyyyMMddhhmmssSSS. • **Custom**—Elective folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.

Setting	Description
Transfer Frequency	Specifies when the logs are transferred: **Manual**—The transfer starts when you click the **Start Log Transfer** button, which is visible only on the local interface. If the log fills before being transferred, new events overwrite the oldest events. **Auto at Threshold**—The transfer starts automatically when the Percent Filled Threshold is reached.

Configure System Log Level and Remote Logging

The RealPresence Centro system log captures devices and server events in a consistent manner. You determine the log level, whether to enable remote logging, and whether to log additional SIP or H.323 details.

Procedure

1. In the system web interface, go to **Diagnostics > System > System Log Settings**.
2. Configure these settings.

Setting	Description
Log Level	Sets the minimum log level of messages stored in the room system's flash memory. `DEBUG` logs all messages, and `WARNING` logs the fewest number of messages. Polycom recommends leaving this setting at the default value of `DEBUG`. When **Enable Remote Logging** is on, the log level is the same for both remote and local logging.
Enable Remote Logging	Specifies whether remote logging is enabled. Enabling this setting causes the room system to send each log message to the specified server in addition to logging it locally. The system immediately begins forwarding its log messages after you click **Save**. Remote logging encryption is supported when TLS transport is the transport protocol. If you are using UDP or TCP transport, Polycom recommends remote logging only on secure, local networks.

Setting	Description
Remote Log Server Address	Specifies the server address and port. If the port is not specified, a default destination port is used. The default port is determined by the configured **Remote Log Server Transport Protocol** setting as follows: • UDP: 514 • TCP: 601 • TLS: 6514 The address and port can be specified in the following formats: • **IPv4 Address** (Example: 10.11.12.13:<port>, where <port> is the elective destination port number in the range 1.65535) • **IPv6 Address** (Example: [2001::abcd: 1234]:<port>, where <port> is the elective destination port number in the range 1.65535) • **FQDN** (Example: logserverhost.company.com:<port>, where <port> is the elective destination port number in the range 1.65535)
Remote Log Server Transport Protocol	Specifies the type of transport protocol: • UDP • TCP • TLS (secure connection)
Enable H.323 Trace	Logs additional H.323 connectivity information.
Enable SIP Trace	Logs additional SIP connectivity information.
Send Diagnostics and Usage Data to Polycom	Sends crash log server information to Polycom to help us analyze and improve the product. Click the **Polycom Improvement Program** button to view information about how your data is used.

Retrieving Log Files

You might find log files useful when troubleshooting. You can generate log files for the RealPresence Centro systems and touch devices. The following related topics explain how to retrieve those log files.

Download System Log Files

You can use the RealPresence Centro system web interface to get system logs. The date and time of system log entries are shown in GMT.

Procedure

1. Go to **Diagnostics > System > Download Logs**.
2. Click **Download system log** and then specify a location on your computer to save the file.

   In the dialog boxes that appear, designate where you want the file to be saved.

Transfer System Log Files

You can transfer a system log file in the RealPresence Centro system local interface.

Procedure

1. Go to > **Settings > Administration > Security > Log Management**.
2. Click **Transfer System Log to USB Device**.
3. The system saves a file in the USB storage device named according to the settings in the system web interface.
4. Wait until the system displays a message that the log transfer has completed successfully before you remove the storage device.

SNMP Condition Reports

SNMP (Simple Network Management Protocol) versions 1, 2c, and 3 are supported on RealPresence Centro systems. A system sends SNMP reports to indicate conditions, including the following:

- All alert conditions found on the system alert screen
- Details of jitter, latency, and packet loss
- Low battery power is detected in the remote control
- A system powers on
- Administrator logon is successful or unsuccessful
- A call fails for a reason other than a busy line
- A user requests help
- A telephone or video call connects or disconnects

SNMP features specific to version 3 include the following:

- Allows for secured connectivity between the console and the SNMP agent
- Supports both IPv4 and IPv6 networks
- Logs all configuration change events
- Supports a user-based security model
- Supports trap destination addresses

Configure SNMP Management

You can configure SNMP Management to give RealPresence Centro system administrators access to manage the system remotely.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **SNMP**.
2. Configure these settings on the SNMP screen, then click **Save**.

Setting	Description
Enable SNMP	Allows administrators to manage the system remotely using SNMP.
Enable Legacy Notifications	Supports sending notifications that are compatible with the legacy MIB.
Enable New Notifications	Supports sending notifications that are compatible with the new MIB.
Version1	Enables the use of the SNMPv1 protocol.
Version2c	Enables the use of the SNMPv2c protocol.
Version3	Enables the use of the SNMPv3 protocol. You must select this setting to use the subsequent settings that apply only to SNMPv3.
Read-Only Community	Specifies the SNMP management community in which you want to enable this system. The default community is `public`. **Note:** Polycom does not support SNMP write operations for configuration and provisioning; the read-only community string is used for both read operations and outgoing SNMP traps.
Contact Name	Specifies the name of the person responsible for remote management of this system.
Location Name	Specifies the location of the system.
System Description	Specifies the type of video conferencing device.
User Name	Specifies the SNMPv3 User Security Model (USM) account name that will be used for SNMPv3 message transactions. The maximum length is 64 characters.
Authentication Algorithm	Specifies the type of SNMPv3 authentication algorithm used: • SHA • MD5
Authentication Password	Specifies the SNMPv3 authentication password. The maximum length is 48 characters.
Privacy Algorithm	Specifies the type of SNMPv3 cryptography privacy algorithm used: • CFB-AES128 • CBC-DES

Setting	Description
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.
Engine ID	Specifies the unique ID of the SNMPv3 engine. This setting might be needed for matching the configuration of an SNMP console application. The Engine ID is automatically generated, but you can create your own ID, as long as it's between 10 and 32 hexadecimal digits. Each group of 2 hex digits can be separated by a colon character (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (therefore, ***:F:*** is equivalent to ***:0f:***). The ID cannot be all zeros or all Fs.
Listening Port	Specifies the port number SNMP uses to listen for messages. The default listening port is 161.
Transport Protocol	Specifies the transport protocol used: • TCP • UDP
Destination Address1 **Destination Address2** **Destination Address3**	Specifies the IP addresses of the computers you intend to use as your network management station and to which SNMP traps will be sent. Each address row has four settings: 1 IP Address (accepts IPv4 and IPv6 addresses, host names, and FQDNs) 2 Message Type (Trap, Inform) 3 SNMP protocol version (v1, v2c, v3) 4 Port (the default is 162) Disabling the **Port** setting disables the corresponding Destination Address.

Download MIBs for SNMP Management

To allow your SNMP management console application to resolve SNMP traps and display human readable text descriptions for those traps, you need to install Polycom MIBs (Management Information Base) on the computer you intend to use as your network management station. The MIBs are available for download from the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings** > **Servers** > **SNMP**.
2. Click the desired link:
    - **Download Legacy MIB**
    - **Download MIB**

Upgrading RealPresence Centro System Software

Polycom recommends that you upgrade your software to the latest available release. You can easily update your RealPresence Centro system software and system options by performing a few tasks outlined here.

Be aware of these points when performing system upgrades:

- If you did not purchase additional system options, you need only to provide a serial number to activate the software. You do not need an option key.
- If you do not have a support agreement, contact an authorized Polycom dealer to get an upgrade key.
- For DoD Unified Capabilities Approved Product List (UC APL) software releases, go to www.polycom.com/solutions/industry/federal_government/certification_accreditation.html.

Ensure you have the required information ready before you begin installing and activating software updates or options:

- License numbers and system serial numbers.
- Software or option keys. Obtain these by logging in to Polycom Support and requesting them from the Activation/Upgrade link. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.

RealPresence Centro systems perform several internal restarts while running software updates. Each restart takes about 2 or 3 minutes and improves the reliability of the update process by freeing up memory. If you are updating a system using a web browser, the internal restart is not visible from the system web interface.

You can downgrade software to an earlier version at any time.

You need an account on Polycom Support before you begin. Be sure to set up an account if you don't already have one.

Ensuring System Compatibility with the RealPresence Touch

If your RealPresence Centro system is used with a RealPresence Touch, you must ensure that the version of the system is compatible with the peripheral software version.

For additional details on software compatibility, see the release notes for the system version you are going to use at Polycom Support.

If you need to update your Polycom system and a RealPresence Touch device, complete your updates in this order:

- RealPresence Centro system
- RealPresence Touch device

Serial and License Numbers

Make a note of your RealPresence Centro system serial number and license number. You must provide these numbers in order to get the keys that activate software updates and system options.

- The 14-digit *serial number* is the unique number that identifies your system. You can find it on the System Information screen and on a label on the system. Serial numbers are case sensitive.
- The *license number* is the number that you receive when you purchase a software update or system option. License numbers have the following format:

Software update license: `U1000-0000-0000-0000-0000`

System option license: `K1000-0000-0000-0000-0000`

Create a Serial and License Number File for Multiple Systems

If you have multiple RealPresence Centro systems, you can save time when your request keys for purchased software updates or system options from Polycom. To do this, create a text file that has all of the necessary information in it before you visit the Polycom support site. This saves you the time of entering each serial and license file number individually on the site. Instead, you can just upload your text file.

Procedure

1. Create a new file in a text editor.
2. Do one of the following:
   - If you do not have a software service plan on all of your systems, enter the license numbers and serial numbers of your systems in the text file.
   - If you do have a software service plan on all of your systems, enter only the serial numbers of the systems in the text file.
3. Save and close the text file.

   Use the following format for text files that contain license numbers and serial numbers:

   license number<TAB>system serial number

   A text file with software update license numbers and serial numbers might look like this:

   ```
   U1000-000-000-0000<TAB>82040903F01AB1
   U1000-000-000-0000<TAB>82043604G18VR2
   ```

   A text file with system option license numbers and serial numbers might look like this:

   ```
   K1000-000-000-5001<TAB>82040903F01AB1
   K1000-000-000-5003<TAB>82043604G18VR2
   ```

   A text file with only serial numbers might look like this:

   ```
   82040903F01AB1
   82043604G18VR2
   ```

Software or System Option Keys

To perform a major or minor software update or activate options, obtain a key before you run the software update. A *key* is the number that activates software or options on a specific RealPresence Centro system. A key is valid only on the system for which it is generated.

There are two types of keys:

- **Software keys** are valid for the software updates you are installing as well as for any point, maintenance, or patch releases that may later become available.
- **Option keys** activate software options and are valid across all software releases.

To obtain these keys, log in to Polycom Support and request them using the Activation/Upgrade link. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.

Update System Software from a USB Storage Device

You can use a USB storage device to update one or multiple RealPresence Centro systems. A setup wizard guides you through the simple process. The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the factory restore button.

If the system is paired with a Polycom touch device, you cannot use the touch device USB port to update the system software. If you use your system within a DoD environment, be sure to contact your Information Assurance Office (IAO) for approval before using a USB device with your system.

Procedure

1. If you are updating to a major or minor release (x.y), obtain keys (.txt) for each system that you want to update from the Polycom website.

   Save the text file as `sw_keys.txt` and place it in the root directory of the USB storage device.
2. Open a browser and navigate to Polycom Support.
3. Under **Documents and Downloads**, select **Telepresence and Video**.
4. Navigate to the page that has the desired update for your system.
5. Save a software package (.tar) file from the Polycom website to the root directory of a USB storage device.
6. Connect the USB storage device to the USB port on the back of the system.

   The system detects the USB storage device and prompts you to confirm that you want to update the software.
7. Click **OK**.

   Follow the setup wizard instructions to complete the update.

Update System Software from a .tar File

You can manually install RealPresence Centro system software from a .tar file.

Procedure

1. Open a supported browser.
2. Configure the browser to allow cookies.
3. In the browser address line, enter the IP address of the system using the format http://IPaddress (for example, http://10.11.12.13).
4. In the system web interface, select **Admin Settings**.

   If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password, if one is set.

   The first time you open the system web interface each day, you might need to enter a user name and password after you select any of the interface options.
5. Go to **General Settings** > **Software Updates** > **Manual Software Updates** > **Browse**.
6. Select a .tar software file to upload and click **Open**.
7. Select **Start Transfer**.
8. After the .tar file transfers to the system, select **Start Update.**
9. Follow the on-screen instructions to complete the update.

Installing an Older Software Version

When your RealPresence Centro system is provisioned with a provisioning server, such as Polycom RealPresence Resource Manager, the system automatically detects software on the provisioning sever and downgrades to the software version on the provisioning server.

If your system is not provisioned, you can put the software package on a USB device to downgrade the system to an earlier version.

Determine the Software Version

Before you downgrade RealPresence Centro system software, Polycom recommends that you check the current system software version you are running.

Procedure

» In the local interface, go to **Settings** > **System Information** > **Information** > **System Detail** or click the **System** link in the system web interface.

Delete System Settings

When you want to reinstall an older version of software with a USB device after upgrading to a later version, Polycom recommends first deleting your RealPresence Centro system settings.

Procedure

» In the local interface, go to **Settings** > **System Information** > **Diagnostics** > **Reset System** and select **Delete System Settings**.

Downgrading Tips

Polycom recommends you review the following tips before downgrading your RealPresence Centro system software:

- When you use your system within a DoD environment, be sure to contact your Information Assurance Office (IAO) for approval before using a USB device with your system.
- Before downgrading, use the release notes to verify the interoperability of the camera, peripheral, hardware, and software versions you plan to install.
-
- When you downgrade the system software, the Polycom RealPresence Touch software is automatically downloaded to a compatible version after being paired. However, the RealPresence Touch platform version 2.0 might not automatically downgrade to version 1.0. In this case, to manually downgrade from version 2.0 to 1.0, you must use a USB storage device or initiate a downgrade from a server repository that includes version 1.0.
-
- Because of changes in software functionality and the user interface, some settings might be lost when you upgrade or downgrade. Polycom recommends that you store your system settings using profiles and download your system directory before updating your system software. Do not manually edit locally saved profile and directory files.

Troubleshooting

Topics:

To learn more about troubleshooting your system or device, refer to the following topics.

General Troubleshooting

The following table provides general troubleshooting information, including symptoms, problems and possible solutions for your RealPresence Centro system.

Symptom	Problem	Solution
The system does not respond to the remote control.	The remote control battery is not charged.	Charge the remote control battery.
	The room lights operate in the 38 Kz range and interfere with the remote control signals.	Turn off the room lights and try the remote control again.
	A touch control device, such as the RealPresence Touch, might be paired to the room system.	Only one device can be paired at a time. To use the remote control, unpair the touch control device.
Picture is blank on the main monitor.	The room system is sleeping. This is normal after a period of inactivity.	Pick up the remote control to wake up the system.

Symptom	Problem	Solution
The monitor remains blank after you pick up the remote control.	The monitor is powered off.	Power on the monitor.
	The monitor's power cord is not plugged in.	Connect the monitor's power cord and the power on the monitor.
	The monitor is not correctly connected to the room system.	Verify that the monitor is connected correctly according to the set up sheet that you received with the system.
You lost the administration password for your system or device.	You cannot access the administration settings without a valid password.	Refer to the factory restore topics to learn how to reset your system.
The system is experiencing video issues during calls, such as packet loss.	You have not configured the Network Quality settings in the system web interface.	Refer to the following Lost Packet Recovery topic link.

View Remote Sessions on the System

You can view a list of remote sessions that are connected to the RealPresence Centro system.

Procedure

1. In the system web interface, go to **Diagnostics** > **System** > **Sessions**.
2. In the system web interface, go to **Admin Settings** > **General Settings** > **Date and Time** > **Time in Call**.
3. Configure these settings.

Placing a Test Call

Polycom support is available to assist you when you encounter difficulties. First though, If you are having problems making a call, try the troubleshooting tips and then call our test numbers. When you finish configuring the RealPresence Centro system, you can call a Polycom video site to test your setup.

You can find a list of worldwide numbers that you can use to test your system at www.polycom.com/videotest.

When placing test calls, try these ideas:

- Make sure the number you dialed is correct, then try the call again. For example, you might need to dial 9 for an outside line or include a long distance access or country code.
- To find out if the problem exists in your system, ask the person you were trying to reach to call you instead.
- Find out if the system you are calling is powered on and is functioning properly.
- If you can make calls but not receive them, make sure that your system is configured with the correct number.

Top LED Light Ring on the RealPresence Centro System

The top light ring indicates where the active speaker has been detected. It gives a visual notification to participants in the room, telling them which speaker is active.

Indicator Light	System Status
LED off	No video is being sent to the far-end site in a call
Amber	Sleep
Blue	On Not in a call
Green	In an audio or a video call
Red	Microphones muted
Blinking blue	System starting
Blinking blue and amber	Software update

RealPresence Centro System Status and LED Indicators

The RealPresence Centro system has LED indicators at the bottom of the system to let you know whether the system is in standby mode, active, or in a call. The following table lists the LED indicators that display on the system and the status associated with each indicator.

LED Indicator	Status
No LED	The system is off.
Amber	The system is sleep or in standby mode.
Blue	The system is on, but not in a call.
Red	The system is on or in an audio or video call with the microphones muted.
Green	The system is in an audio or a video call.
Blinking green	The system is in a call with the video muted.
Blinking blue	The software on the system is updating.

EagleEye Producer Indicator Lights

An LED is integrated into the front of the EagleEye Producer unit. Different LED lights refer to different system states. These allow you to identify the current system state for the EagleEye Producer system. Detailed LED and system states mappings are shown in the following table.

LED Indicator Lights System State

LED	System State
Blue	Power On, EagleEye Producer Normal State
Blinking Blue	On, Not in a Call, Receive IR EagleEye Producer Boot Up
Fast Blinking Blue	Calibrate Webcam Room View
Amber	Standby - Asleep
Alternate Amber and Blue	Software update, Factory restore, USB image update
Blinking Amber	USB disk plugged in
Green	On, In a call
Blinking Green	On, In a call, Receive IR in a call
Fast Blinking Red	System error
Blink	Needs attention, Receive IR

Audio and Video Tests

You can perform the following audio and video diagnostic tests on your RealPresence Centro system.

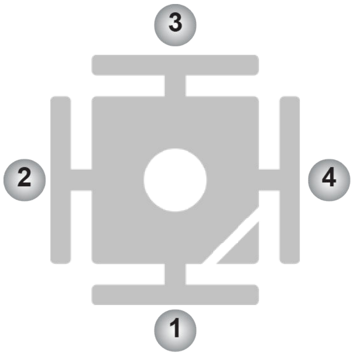
Diagnostic Screen	Description
Speaker Test	Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct. If you run the test from the system during a call, the far site will also hear the tone. If you run the test from the system web interface during a call, the people at the site you are testing will hear the tone, but you will not.
Audio Meters	Measures the strength of audio signals from microphones, far-site audio, and any device connected to the audio line in. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system.

Diagnostic Screen	Description
Camera Tracking	Provides diagnostics specific to the EagleEye Director. **Audio** Verifies microphone functionality. To use this feature, speak aloud and verify that you can see dynamic signal indications for two vertical microphones and five horizontal microphones. If no signal indication appears for a specific microphone, manually power off the EagleEye Director and then power it back on. Also verifies the reference audio signal: Set up a video call. Let the far side speak aloud and verify that you can see dynamic signal indications for the two reference audio meters. If no signal indication appears for a specific microphone, make sure the reference cable is connected firmly. After you verify microphone functionality, calibrate the camera again. **Video** • Left Camera shows video from the left camera. • **Right Camera** shows video from the right camera. • **Color Bars** displays the color bar test screen. **Note:** If the EagleEye Director is connected but is not selected as the current camera source, this choice is not visible on the screen.

Audio Meters on the RealPresence Centro System

Audio meters indicate the strength of the audio input and output of your microphones, far-site audio, and any device connected to the audio ports. To avoid or fix audio distortion, you can configure the Audio Meter setting in the local or web RealPresence Centro system interface.

The meters allow you to identify front, back, left, and right audio channels. To determine which side of the RealPresence Centro system is the front, refer to the following figure. Note that when you face the front of the system, the removable corner is on the lower right side of the base.



Reference Number	Description
1	Front audio channel
2	Left audio channel
3	Back audio channel
4	Right audio channel

Set Audio Meter Levels

You can set audio meter levels for your RealPresence Centro system so that normal and loud audio peaks are within an acceptable audio range.

Procedure

1. Do one of the following:
   - In the system web interface, go to **Diagnostics** > **Audio and Video Tests** > **Audio Meter**.
   - In the local interface, go to **Settings** > **System Information** > **Diagnostics** > **Audio Meter**.
2. To test the audio, do one of the following:
   - To check the microphones for the near-site, speak into the microphones.
   - To check far-site audio, ask a participant at the far site to speak, or call a phone in the far-site room to hear it ring.
3. For normal speech and program material, set the audio signal levels so that you see peaks between +3 dB and +7 dB.

   Occasional peaks of +12 dB to +16 dB with loud transient noises are acceptable. If you see +20 on the audio meter, the audio signal is 0 dBFS and the audio might be distorted. A meter reading of +20dB corresponds to 0dBFS in the room system audio. A signal at this level is likely clipping the audio system.

System Diagnostics

To assist in troubleshooting, you can view RealPresence Centro system diagnostics in either the system web interface or the local interface.

Access Diagnostic Screens in the Web Interface

You can access RealPresence Centro system diagnostics in the system web interface.

Procedure

1. In the system web interface, go to **Diagnostics** > **System** > **System Status**.
2. For details, click **More Info**.

Access Diagnostic Screens in the Local Interface

You can access RealPresence Centro system diagnostics in the local interface.

Procedure

» In the system local interface, select **Settings** > **System Information** > **Diagnostics.**

This screen includes the following system diagnostic details:

Diagnostic Screen	Description
Near End Loop	Tests the internal audio encoders and decoders, the external microphones and speakers, the internal video encoders and decoders, audio hardware, and the external microphones, speakers, cameras, and monitors. Monitor 1 displays the video and plays the audio that would be sent to the far site in a call. This test is not available when you are in a call.
Ping	Tests whether the system can establish contact with a far-site IP address that you specify. PING returns abbreviated Internet Control Message Protocol results. It returns H.323 information only if the far site is configured for H.323. It returns SIP information only if the far site is configured for SIP. If the test is successful, the system displays a message.
Trace Route	Tests the routing path between the local system and the IP address entered. If the test is successful, the system lists the hops between the system and the IP address you entered.
Color Bars	Tests the color settings of your monitor for optimum picture quality. If the color bars generated during the test are not clear, or the colors do not look correct, the monitor needs to be adjusted.

Diagnostic Screen	Description
Speaker Test	Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct. If you run the test from the system during a call, the far site will also hear the tone.
Audio Meter	Measures the strength of audio signals from the microphone or microphones, far-site audio, and any device connected to the audio line in. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the system.
Camera Tracking	Provides diagnostics specific to the EagleEye Director, if this camera is connected to the system. **Audio** • Verifies microphone functionality. To use this feature, speak aloud and verify that you can see dynamic signal indications for two vertical microphones and five horizontal microphones. If no signal indication appears for a specific microphone, manually power off the EagleEye Director and then power it back on. • Also verifies the reference audio signal: Set up a video call. Let the far side speak aloud and verify that you can see dynamic signal indications for the two reference audio meters. If no signal indication appears for a specific microphone, make sure the reference cable is connected firmly. After you verify microphone functionality, calibrate the camera again. **Video** • **Left Camera** shows video from the left camera. • **Right Camera** shows video from the right camera. • **Color Bars** displays the color bar test screen.

Diagnostic Screen	Description
Sessions	Displays the following information about each session connected to the system: • Type of connection, such as web or local interface • ID associated with the session, typically Admin or User • Remote IP address (the addresses of people logged in to the system from their computers)
Reset System	**Note**: Do not use this setting unless your administrator tells you to do so. If a password is set, you must enter it to reset the system. Returns the system to its default settings. When you select this setting using the remote control, you can do the following: • Keep your system settings (such as system name and network configuration) or restore system settings. • Keep or delete the directory stored on the system. System reset does not affect the global directory. • Keep or delete all PKI certificates and certificate revocation lists (CRLs). Before you reset the system, you might ask your administrator to download the Call Detail Report (CDR) and CDR archive. For more information about these reports, contact your administrator.

Viewing System Details on the Local Interface

You might need to view certain RealPresence Centro system details on the local interface to do video conferencing tasks, such as pairing, or to perform troubleshooting tests to provide information for your own testing or for technical support. You can also review information about calls, network usage, and performance on the various system screens in the local interface.

Available system menus vary based on how your administrator configured the system. Therefore, this section might describe settings that you cannot access on your system. To find out more about these settings, please talk to your administrator.

The System Information screen has the following choices:

- Information
- Status
- Diagnostics

- Call Statistics (in a call only)

Access the Information Screen

You can access RealPresence Centro system status screen in the local interface.

Procedure

» Go to ⚙ > **System Information** > **Information** to view the following system details**.**

Diagnostic Screen	Description
System Detail	Displays the following system information: • System Name • Model • Hardware Version • System Software • Serial Number • MAC Address • IP Address
Network	Displays the following network information: • IP Address • Host Name • 323 Name • 323 Extension (E.164) • SIP Address • Link-Local • Site-Local • Global Address
Usage	Displays the following usage information: • Time in Last Call • Total Time in Calls • Total Number of Calls • System Up Time

Access the Status Screen

You can access RealPresence Centro system status screen in the local interface.

Procedure

» Go to ⚙ > **System Information** > **Status.**

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for the out of a call status:

Status Screen	Description
Active Alerts	Displays the status of any device or service listed within the Status screens that has a current status indicator of red. Alerts are listed in the order they occurred. When a system device or service encounters a problem, you see an alert next to the **Settings** button on the menu.
Call Control	Displays the status of the **Auto-Answer Point-to-Point Video** and **Meeting Password** settings.
Audio	Displays the connection status of audio devices such as the microphones and SoundStation IP.
VisualBoard	Displays the connection status of the VisualBoard, if one is connected. If VisualBoard is not connected, this choice is not visible on the screen.
LAN	Displays the connection status of the IP Network.
Servers	• Always displays the Gatekeeper and SIP Registrar Server. • Displays the active Global Directory Server, LDAP Server, or Microsoft Server. • If enabled, displays the Provisioning Service, Calendaring Service, or Presence Service.
Log Management	Displays the status of the Log Threshold setting. You can download system logs, call detail reports, and configuration profiles using the system web interface.

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for in a call status:

- When a change occurs in the system status or a potential problem exists, you see an alert next to the **System** button on the menu.

Status Screen	Description
Call Statistics	Displays information about the call in progress. In multipoint calls, the Call Statistics screens show most of this information for all systems in the call.

View Call Statistics for an Active Point-to-Point Call With the Remote Control

You might need to view call statistics on the RealPresence Centro system local interface to do some troubleshooting for users. You can only view call statistics during a call. During a point-to-point call, you can view call statistics about a call participant or about an active stream. As a shortcut during a call, press the **Back** button on your remote control for two or more seconds to display the Call Statistics screen.

Procedure

» Go to ⚙ **System Information** > **Call Statistics**.

Streams associated with the participant are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and select **More Information**.

View Call Statistics for an Active Multipoint Call with the Remote Control

During a RealPresence Centro system multipoint call, you can view call statistics about any of the call participants or about an active stream.

Procedure

1. Go to 🛠 > **System Information** > **Call Statistics**.

   A list of participants in the call displays.
2. Do one of the following:
   - To view a participant's details, select **Participants**, navigate to the desired participant, and select **More Information**. The participants' active streams are displayed beneath the participant information.
   - To quickly access information about a particular stream or streams associated with a particular user, navigate to **Streams** for calls using Advanced Video Coding (AVC) or **Participant Streams** for calls using Scalable Video Coding (SVC)**.** Use the **Back** and **Next Participant** buttons to navigate to the participant with the stream or streams you want to view. Navigate to the desired stream and select **More Information**.
   - To quickly access a list of all active audio, video, and content streams within the call, navigate to **Active Streams** (available in SVC calls only). Select the desired stream, and select **More Information**.

View Call Statistics for an Active Multipoint Call on the Polycom Touch Control

During a multipoint call, you can view call statistics about any of the call participants or about an active stream.

Procedure

1. Touch **Participants**. A list of participants in the call displays.
2. Touch **View Call Statistics** and do one of the following:
   - To view a participant's details, navigate to the desired participant, and touch i.

- The participants' active streams are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and touch "I".
- From an individual stream view you can select **Next Stream** to view the next stream in the stream list. To quickly access a list of all active audio, video, and content streams within the call, navigate to **Active Streams**. This setting is available in SVC calls only. Select the desired stream and touch "I".

Provisioning Service Registration Failure

If automatic provisioning is enabled but the RealPresence Centro system does not register successfully with the provisioning service, you might need to change the Domain, User Name, Password, or Server Address used for registration. For example, users might be required to periodically reset passwords used to log into the network from a computer. If such a network password is also used as the provisioning service password, you must also update it on the system. To avoid unintentionally locking a user out of network access in this case, systems do not automatically retry registration until you update the settings and register manually on the Provisioning Service screen.

Call Detail Report (CDR)

When enabled by going to **Admin Settings** > **General Settings** > **System Settings** > **Recent Calls** in the RealPresence Centro system web interface, the Call Detail Report (CDR) provides the room system's call history. Within 5 minutes after ending a call, the CDR is written to memory and then you can download the data in CSV format for sorting and formatting.

Every call is added to the CDR, whether it is made or received. If a call does not connect, the report shows the reason. In multipoint calls, each far site is shown as a separate call, but all have the same conference number.

The size of a CDR can become unmanageable if you don't download the record periodically. If you consider that 150 calls result in a CDR of approximately 50 KB, you can set up a schedule to download and save the CDR after every 120 calls to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads. The CDR database is limited to the 150 most recent entries. If you are concerned about tracking all CDR records, ensure that you download the records at regular intervals so that the limit is not exceeded and records are not lost.

Note: The RealPresence Resource Manager system captures CDR information for the EagleEye Producer and the EagleEye Director II cameras and generates it to the RealPresence Resource Manager system CDR. The call details include **People Minutes** and **People Count (Call Begin)** at the beginning of a call and **People Count (Peak Value)** at the end of a call.

Data	Description
Row ID	Each call is logged on the first available row. A call is a connection to a single site, so there might be more than one call in a conference.
Start Date	The call start date, in the format dd-mm-yyyy.
Start Time	The call start time, in 24-hour format hh:mm:ss.

Data	Description
End Date	The call end date.
End Time	The call end time.
Call Duration	The length of the call.
Account Number	If **Require Account Number to Dial** is enabled on the system, the value entered by the user is displayed in this field.
Remote System Name	The far site's system name.
Call Number 1	The number dialed from the first call field, not necessarily the transport address. For incoming calls — The caller ID information from the first number received from a far site.
Call Number 2 (If applicable for call)	For outgoing calls — The number dialed from the second call field, not necessarily the transport address. For incoming calls — The caller ID information from the second number received from a far site.
Transport Type	The type of call — Either H.323 (IP) or SIP.
Call Rate	The bandwidth negotiated with the far site.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.
Call Direction	In—For calls received. Out—For calls placed from the system.
Conference ID	A number given to each conference. A conference can include more than one far site, so there might be more than one row with the same conference ID.
Call ID	Identifies individual calls within the same conference.
Total H.320 Channels Used	Number of narrow-band channels used in the call.
Endpoint Alias	The alias of the far site.
Reserved	Polycom use only.
View Name	Names the web or local interface used in the call.
User ID	Lists the ID of the user who made the call.
Endpoint Transport Address	The actual address of the far site (not necessarily the address dialed).

Data	Description
Audio Protocol (Tx)	The audio protocol transmitted to the far site, such as G.728 or G.722.1.
Audio Protocol (Rx)	The audio protocol received from the far site, such as G.728 or G.722.
Video Protocol (Tx)	The video protocol transmitted to the far site, such as H.263 or H.264.
Video Protocol (Rx)	The video protocol received from the far site, such as H.261 or H.263.
Video Format (Tx)	The video format transmitted to the far site, such as CIF or SIF.
Video Format (Rx)	The video format received from the far site, such as CIF or SIF.
Disconnect Local ID and Disconnect Reason	The identity of the user who initiated the call and the reason the call was disconnected.
Q.850 Cause Code	The Q.850 cause code showing how the call ended.
Total H.320 Errors	The number of H.320 errors experienced during the call.
Average Percent of Packet Loss (Tx)	The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire call. However, it does report an average of the sampled values.
Average Percent of Packet Loss (Rx)	The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire call. However, it does report an average of the sampled values.
Average Packets Lost (Tx)	The number of packets transmitted that were lost during a call.
Average Packets Lost (Rx)	The number of packets from the far site that were lost during a call.
Average Latency (Tx)	The average latency of packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.
Average Latency (Rx)	The average latency of packets received during a call based on round-trip delay, calculated from sample tests done once per minute.

Data	Description
Maximum Latency (Tx)	The maximum latency for packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.
Maximum Latency (Rx)	The maximum latency for packets received during a call based on round-trip delay, calculated from sample tests done once per minute.
Average Jitter (Tx)	The average jitter of packets transmitted during a call, calculated from sample tests done once per minute.
Average Jitter (Rx)	The average jitter of packets received during a call, calculated from sample tests done once per minute.
Maximum Jitter (Tx)	The maximum jitter of packets transmitted during a call, calculated from sample tests done once per minute.
Maximum Jitter (Rx)	The maximum jitter of packets received during a call, calculated from sample tests done once per minute.
Call Priority	The AS-SIP call precedence level assigned to the call (populated only when AS-SIP is enabled on the system).

Download a Call Detail Report (CDR)

You can download a CDR using the RealPresence Centro system web interface.

Procedure

1. In the system web interface, click **Utilities** > **Services** > **Call Detail Report (CDR)**.
2. Click **Most Recent Call Report** and then specify whether to open or save the file on your computer.

Knowledge Base

For more troubleshooting information for your RealPresence Centro system, you can search the Knowledge Base at Polycom Support.

Before You Contact Polycom Technical Support

If you are not able to make test calls successfully and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support at Polycom Support.

Enter the following information about your RealPresence Centro system, then ask a question or describe the problem. This information helps us to respond faster to your issue. In addition, please provide any diagnostic tests or troubleshooting steps that you have already tried.

Locate the System Serial Number

You can view the system serial number on the local interface of the RealPresence Centro system.

Procedure

» To locate the system serial number (14 digits), go to **Settings** > **System Information** > **Information** > **System Detail** or locate the number on the back of the system.

Locate the Software Version

You can view the software version on the local interface of the RealPresence Centro system.

Procedure

» To locate the software version, go to **Settings** > **System Information** > **Information** > **System Detail**.

Locate Active Alert Messages

You can view the active alert messages on the local interface of the RealPresence Centro system.

Procedure

» To locate the active alert messages, go to **Settings** > **System Information** > **Status** > **Active Alerts** for messages generated by your system.

Locate the IP Address and H.323 Extension Settings

You can view IP Address and H.323 extension settings on the local interface of the RealPresence Centro system.

Procedure

» To locate the IP Address and H.323 Extension settings, go to **Settings** > **System Information** > **Information** > **Network**.

Locate the LAN Status

You can view the LAN status on the local interface of the RealPresence Centro system.

Procedure

» In the system web interface, go to **Settings** > **System Information** >**Status** > **LAN**.

Locate Diagnostics

You can view diagnostics on the local interface of the RealPresence Centro system.

Procedure

» In the system web interface, go to **Settings** > **System Information** > **Diagnostics**.

Contacting Technical Support

If you are not able to make test calls successfully on your RealPresence Centro system and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support.

To contact Polycom Technical Support, go to Polycom Support.

Enter the following information, then ask a question or describe the problem. This information helps us to respond faster to your issue:

- The 14-digit serial number from the **System Detail** screen or the back of the system
- The software version from the **System Detail** screen
- Any active alerts generated by the system
- Information about your network
- Troubleshooting steps you have already tried

You can find the system detail information in the local interface by going to **Settings > System Information > Information** or in the system web interface by clicking **System** in the blue bar at the top of the system web interface screen.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components, such as RealPresence Centro systems, only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook, Skype for Business Server 2015 integrations. For additional information and details please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

System Panel Views

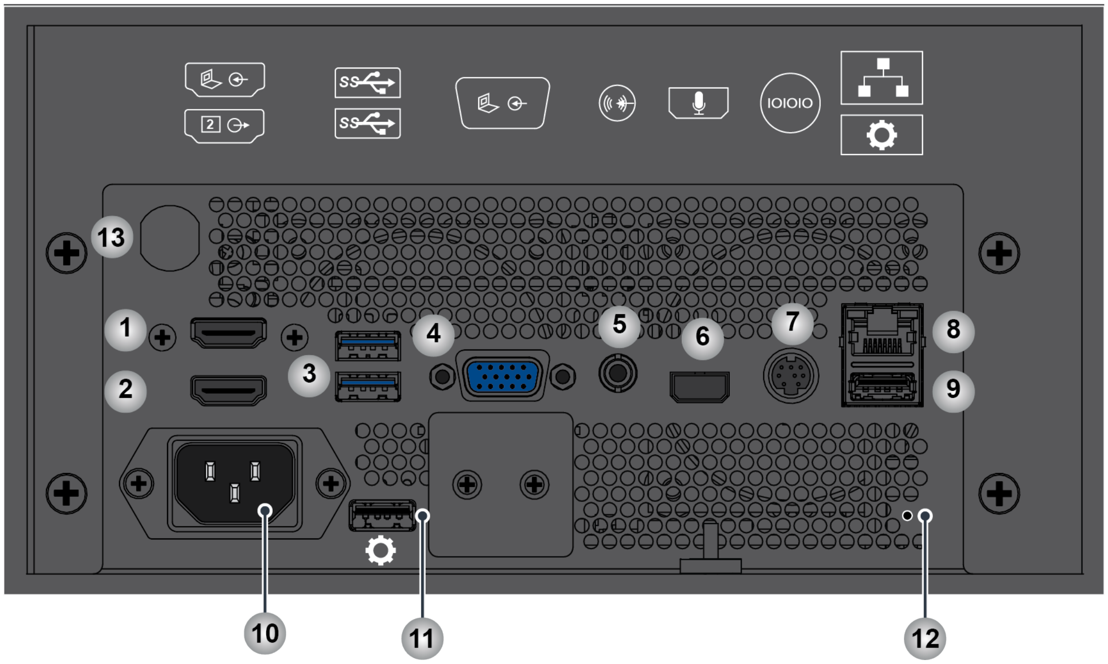
Topics:

- Polycom RealPresence Centro System

The following provides information on the RealPresence Centro system back panel views.

Polycom RealPresence Centro System

This following figure and table shows how the system web interface settings relate to hardware input and outputs for the RealPresence Centro system. Polycom recommends that you use either the HDMI or VGA video input, but not both.



Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
1	Audio/Video > Video Inputs > Input 2 Audio/Video > Audio > Audio Input > Type: HDMI	Video Input 2/Audio Input 1	HDMI version 1.3	Main video and audio input

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
2	Audio/Video > Monitors > Monitor 2	Video Output 2	• HDMI version 1.3 • DVI-D	Output for Monitor 2; does not include audio
3	N/A	USB connections	USB 3.0	Use these ports for the following tasks: • Connect secondary touch monitors • Perform software updates • Charge the remote control battery
4	Audio/Video > Video Inputs > Input 2	Video Input 2	VGA	Video input for Content
5	Audio/Video > Audio > Audio Input > Type: 3.5mm	Audio Input 2	3.5mm Stereo	Stereo line-level input 3.5mm audio is independent and not associated with any video input
6	N/A	Microphone Input	Polycom Microphone	Audio input for up to two Polycom microphone arrays or a SoundStructure mixer; supports up to 3 ceiling microphones for Acoustic Fence Technology
7	General Settings > Serial Ports	Serial Port	RS-232	Serial port
8	Network > LAN Properties	LAN Port	Ethernet	Connectivity for IP calls, People +Content IP, and the system web interface

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
9	N/A	USB connection	USB 2.0	Main service port. Use this port for the following tasks: • Perform a software update using a USB storage device • Perform a factory restore using a USB storage device **Note**: For a factory restore, insert one USB storage device into this port, and the other USB storage device into the port at Ref. number 11.
10	N/A	Power Input	12 0/240 VAC	Power input
11	N/A	USB connection	USB 2.0	Use this port only to perform a factory restore using a USB storage device. Insert one USB storage device into this port, and the other USB storage device into the port at Ref. number 9. **Note**: This port cannot be used to perform a software update using a USB storage device.
12	N/A	N/A	N/A	Factory restore button
13	N/A	Power button	N/A	Power the system on and off

Port Usage

Topics:

- Connections to Systems
- Connections from Systems

The following topics on port usage are useful when you configure your network equipment for video conferencing.

Connections to Systems

The following table shows IP port usage to RealPresence Centro systems.

				Configuration		
Inbound Port	**Type**	**Protocol**	**Function**	**On By Default?** **(Low Security Profile)**	**Enable/ Disable?**	**Configurable Port Number**
22	Static	TCP	Secure API	Yes	Admin Settings > Security> Global Security > Access Enable SSH Access: Enable to open port 22	No
23	Static	TCP	Telnet Diagnostics	No	Admin Settings > Security > Global Security > Access > Enable Telnet Access	No

				Configuration		
Inbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
24	Static	TCP	Polycom API	No	Admin Settings > Security > Global Security > Access > Enable Telnet Access	No
80	Static	TCP	Web UI over HTTP RealPresence Touch over HTTP	Yes	Admin Settings > Security > Global Security > Access > Enable Web Access - Disables HTTP and HTTPS port Admin Settings > Security > Global Security > Access > Restrict to HTTPS - Disables HTTP port	Admin Settings > Security > Global Security > Access > Web Access Port (http)

				Configuration		
Inbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
161	Static	UDP	SNMP	No	Admin Settings > Security > Global Security > Access > Enable SNMP Access Admin Settings > Servers > SNMP > Enable SNMP	Admin Settings > Servers > SNMP > Listening Port
443	Static	TLS	Web UI over HTTPS RealPresence Touch over HTTPS	Yes	Admin Settings > Security > Global Security > Access > Enable Web Access	No
1719	Static	UDP	H.225.0 RAS	No	Admin Settings > Network > IP Network > H.323 > Use Gatekeeper	No
1720	Static	TCP	H.225.0 Call Signaling	Yes	Admin Settings > Network > IP Network > H.323 > Enable IP H.323	No

				Configuration		
Inbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
5001	Static	TCP	People +Content™ IP client application for content sharing. Used by systems and the RealPresence Touch device	Yes	Admin Settings > Audio / Video > Video Input > General Camera Settings > Enable People +Content IP	No
5060	Static	TCP UDP	SIP (Protocol depends on Transport Protocol setting)	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP Admin Settings > Network > IP Network > SIP > Transport Protocol	No
5061	Static	TLS	SIP	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP Admin Settings > Network > IP Network > SIP > Transport Protocol	No

				Configuration		
Inbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
49152-65535	Dynamic	TCP	H.245	Yes	Admin Settings > Network > IP Network > H.323 > Enable IP H.323	Admin Settings > Network > IP Network > Firewall > Fixed Ports > TCP Ports (1024-65535)
16384-32764(Default)	Dynamic	UDP	RTP/RTCP Video and Audio	Yes	Admin Settings > Network > IP Network > H.323 > Enable IP H.323 Admin Settings > Network > IP Network > SIP > Enable SIP	Admin Settings > Network > IP Network > Firewall > Fixed Ports > UDP Ports (1024-65535)

Connections from Systems

The following table shows IP port usage from RealPresence Centro systems.

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
80	Static	TCP	Polycom Product Registration for RealPresence Centro system software installation and for the RealPresence Touch device	Yes	Uncheck "Register" checkbox during the setup wizard	No
123	Static	UDP	NTP	Yes	Admin Settings > General Settings > Date and Time > System Time > Time Server	No
162	Static	UDP	SNMP TRAP	No	Admin Settings > Servers > SNMP > Enable SNMP Admin Settings > Servers > SNMP > Destination Address <1,2,3>	Yes - Admin Settings > Servers > SNMP > Destination Address <1,2,3> > Port

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
389	Static	TLS	LDAP	No	Admin Settings > Servers > Directory Servers > Server Type	Yes - Admin Settings > Servers > Directory Servers > Server Type = LDAP - Admin Settings > Servers > Directory Servers > Server Port
389	Static	TLS	LDAP to ADS (External Authentication)	No	Admin Settings > Security > Global Security > Authentication > Enable Active Directory External Authentication	No
443	Static	TLS	RealPresence Resource Management (Provisioning, Monitoring, Softupdate)	No	Admin Settings > Servers > Provisioning Service > Enable Provisioning	No
443	Static	TLS	Microsoft Exchange Server (Calendaring)	No	Admin Settings > Servers > Calendaring Service > Enable Calendaring Service	No

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
443	Static	TLS	Microsoft Skype Address Book	No	Admin Settings > Servers > Directory Servers > Server Type	No
514	Static	UDP	SYSLOG	No	Diagnostics > System > System Log Settings > Enable Remote Logging Diagnostics > System > System Log Settings > Remote Log Server Transport Protocol = UDP	Yes - outgoing port can be specified in the **Remote Log Server Address** field.
601	Static	TCP	SYSLOG	No	Diagnostics > System > System Log Settings > Enable Remote Logging Diagnostics > System > System Log Settings > Remote Log Server Transport Protocol = TCP	Yes - outgoing port can be specified in the **Remote Log Server Address** field.

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
1718	Static	UDP	H.225.0 Gatekeeper Discovery	No	Admin Settings > Network > IP Network > H. 323 > Use Gatekeeper = Auto	No
1719	Static	UDP	H.225.0 RAS	No	Admin Settings > Network > IP Network > H. 323 > Use Gatekeeper	Yes - outgoing port can be specified in the **Primary Gatekeeper IP Address** field
1720	Static	TCP	H.225.0 Call Signaling	Yes	Admin Settings > Network > IP Network > H. 323 > Enable IP H.323	No
3601	Static	TCP	GDS	No	Admin Settings > Servers > Directory Servers > Server Type	No

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
5060	Static	UDP TCP	SIP	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP AND Admin Setting > Network > IP Network > SIP > Transport Protocol = Auto, TCP, or UDP	Yes - outgoing port can be specified in the dial string (user@domain:port) Note that the transport protocol used depends on Admin Settings > Network > IP Network > SIP > Transport Protocol
5061	Static	TLS	SIP	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP AND Admin Setting > Network > IP Network > SIP > Transport Protocol = Auto or TLS	Yes - outgoing port can be specified in the dial string (user@domain:port)
5222	Static	TCP	RealPresence Resource Manager: XMPP	No	Provisioned by RealPresence Resource Manager	No

				Configuration		
Outbound Port	Type	Protocol	Function	On By Default? (Low Security Profile)	Enable/ Disable?	Configurable Port Number
6514	Static	TLS	SYSLOG	No	Diagnostics > System > System Log Settings > Enable Remote Logging Diagnostics > System > System Log Settings > Remote Log Server Transport Protocol = TLS	Yes - outgoing port can be specified in the **Remote Log Server Address** field
49152-65535	Dynamic	TCP	H.245	Yes	Admin Settings > Network > IP Network > Enable IP H.323	Admin Settings > Network > IP Network > Firewall > Fixed Ports > TCP Ports (1024-65535)
16384-32764 (Default)	Dynamic	UDP	RTP/RTCP Video and Audio	Yes	Admin Settings > Network > IP Network > Enable IP H.323 Admin Settings > Network > IP Network > Enable SIP	Admin Settings > Network > IP Network > Firewall > Fixed Ports > UDP Ports (1024-65535)

Security Profile Default Settings

Topics:

- Maximum Security Profile Default Settings
- High Security Profile Default Settings
- Medium Security Profile Default Settings
- Low Security Profile Default Settings

The system security profiles provide varying levels of secure access to your system. Default settings for each security profile type vary. See the following topics for details.

Maximum Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **Maximum** security profile.

Admin Settings Area	**Maximum**		
	Range	**Default Value**	**Configurable?**
Place a Call			
Contacts	Search Box	No value	Yes
Speed Dial			
Edit	Search Box	No value	Yes
Manual Dial			
	Entry box	No value	Yes
	VideoAudio	Video	Yes
	Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144	Auto	Yes
	Auto, H.323, SIP	Auto	Yes
General Settings			
System Settings			
Call Settings			

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Auto Answer Point to Point Video	Yes, No, Do Not Disturb	No	Yes
Auto Answer Multipoint Video	Yes, No, Do Not Disturb	No	Yes
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Disabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	Yes
Background	Choose image file	No file selected	Yes
Startup Background	Choose image file	No file selected	Yes
Kiosk Mode	Checkbox	Disabled	Yes
Home Screen Icons	Checkbox	Disabled	Yes
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			
Enable Polycom Touch Device Note: Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes

Admin Settings Area	**Maximum**		
	Range	**Default Value**	**Configurable?**
SmartPairing	Disabled	Disabled	Read-only
Serial Ports			
Mode			
RS-232 Mode Note: Some systems support only a subset of listed modes.	Off Control Camera Control Closed Caption Pass Thru	Off	Yes
Login Mode	Range: None, Admin password only, Username/Password	Admin password only	Yes
Login prompt type	None, Admin password only, Username/ Password	Username/ Password	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto, TLS, TCP, UDP	TLS	Yes
Dialing Preference			
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP, H.323, SIP	IP H.323	Yes
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)	IP, H.323, SIP	SIP	Yes
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)	IP, H.323, SIP	H.323	Yes
Audio/Video			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Enabled	Read-only
Video Inputs			
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People +Content IP	Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	**Default Value**	**Configurable?**
Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Audio			
Polycom StereoSurround	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	Maximum	Yes
Authentication			
Enable Active Directory External Authenticat ion	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Allow Access to User Settings	Checkbox	Disabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
	Restrict to HTTPS	Checkbox	Enabled	Read-only
	Web access port (http) **Note:** You cannot select this setting if the **Restrict to HTTPS** setting is enabled.	16-bit integer	Grayed out (80)	Read-only
	Enable Telnet Access	Checkbox	Disabled	Read-only
	Enable SNMP Access	Checkbox	Disabled	Yes
	API Port			
	Enable SSH Access	Checkbox	Enabled	Yes
	Lock Port after Failed Logins	Off, 2-10	Off	Yes
	Port Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours	1 minute	Yes
	Reset Port Lock Counter After	Off, [1..24] hours	Off	Yes
	Enable Whitelist	Checkbox	Disabled	Yes

Admin Settings Area			Maximum		
			Range	**Default Value**	**Configurable?**
		Idle Session Timeout in Minutes	1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480	10	Yes
		Maximum Number of Active Sessions	10, 15, 20, 25, 30, 35, 40, 45, 50	25	Yes
	Encryption				
		Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Calls	Required for Video Calls Only	Yes
		Require FIPS 140 Cryptograp hy	Checkbox	Enabled	Yes
Local Accounts					
	Account Lockout				
		Lock Admin Account After Failed Logins	2-10	3	Yes
		Admin Account Lock Duration	1, 2, 3, 5 minutes	1	Yes
		Reset Admin Account Lock Counter After	Off, [1..24] hours	1	Yes
		Lock User Account After Failed Logins	2-10	3	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
User Account Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours	1 minute	Yes
Reset User Account Lock Counter After	Off, [1..24] hours	1	Yes
Login Credentials			
Use Room Password for Remote Access	Checkbox	Enabled	Read-only
Require User Login for System Access	Checkbox	Enabled	Yes
Password Requirements			
Admin (Room, Remote), User (Room, Remote)			
Reject Previous Passwords	8-16	10	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180	60	Yes
Minimum Changed Characters	1-4	4	Yes
Password Expiration Warning	1-7	7	Yes
Remote Access (Admin Remote, User Remote)			

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Minimum Length	8-16, 32	15	Yes
Require Lowercase Letters	Off, 1, 2, All	2	Yes
Require Uppercase Letters	Off, 1, 2, All	2	Yes
Require Numbers	Off, 1, 2, All	2	Yes
Require Special Characters	Off, 1, 2, All	2	Yes
Maximum Consecutiv e Repeated Characters	1-4	2	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
User (Room), Admin (Room)			
Minimum Length	8-16, 32	9	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Maximum Consecutive Repeated Characters	1-4	2	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
Meeting			
Minimum Length	Off, 1-20, 32	Off	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Reject Previous Passwords	8-16	10	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Consecutive Repeated Characters	1-4	2	Yes
SNMP Note: SNMP passwords are applicable only when the system uses SNMP v3.			
Minimum Length	8-16, 32	12	Yes

Admin Settings Area		Maximum		
		Range	**Default Value**	**Configurable?**
	Require Lowercase Letters	Off, 1, 2, All	1	Yes
	Require Uppercase Letters	Off, 1, 2, All	1	Yes
	Require Numbers	Off, 1, 2, All	1	Yes
	Require Special Characters	Off, 1, 2, All	1	Yes
	Reject Previous Passwords	8-16	10	Yes
	Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
	Maximum Consecutive Repeated Characters	1-4	2	Yes
	Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
Security Banner				
	Enable Security Banner	Checkbox	Enabled	Yes
	Banner Text	DoDCustom	DoD	Yes
	Local System Banner Text	Unicode characters, 2048 bytes max	DoD Banner Text	Yes
	Remote System Banner Text	Unicode characters, 2048 bytes max	DoD Banner Text	Yes
Certificates				
	Certificate Options			

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Always Validate Peer Certificates from Browser	Checkbox	Enabled	Yes
Always Validate Peer Certificates from Server	Checkbox	Enabled	Yes
Revocation			
Revocation Method	OCSPCRL	OCSP	Yes
Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Servers			
Directory Servers			
Server Type	Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status	N/A	Disabled	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Provisioning Service	Checkbox	Disabled	Yes
Calendaring Service			

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service	Checkbox	Disabled	Yes
	Domain Name User Name Password Server Address		

Diagnostics Area	Maximum		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	TLS	Read only

Changing Maximum Security Profile Default Values

When you configure the system to use the Maximum Security Profile, the system forces you to change the following settings from their default values:

- Admin account User Id
- User account User Id
- Admin room password
- Admin remote access password
- User room password
- User remote access password

Other Restrictions When Using the Maximum Security Profile

The following settings are not available in the “User Settings” menu (they are configurable only in their respective sections of the **Admin Settings**):

- **Camera** > **Allow Other Participants in a Call to Control Your Camera**
- **Meetings** > **Mute Auto Answer Calls**
- **Meetings** > **Auto Answer Point-to-Point Video**
- **Meetings** > **Auto Answer Multipoint Video**
- **Meetings** > **Allow Video Display on Web**

Configure Security Profiles

High Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **High** security profile.

Admin Settings Area	**High**		
	Range	**Default Value**	**Configurable?**
Place a Call			
Contacts	Search Box	No value	Yes
Speed Dial			
Edit	Search Box	No value	Yes
Manual Dial			
	Entry box	No value	Yes
	Video Audio	Video	Yes
	Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144	Auto	Yes
	Auto H.323 SIP	Auto	Yes
General Settings			
System Settings			

Admin Settings Area	High		
	Range	**Default Value**	**Configurable?**
Call Settings			
Auto Answer Point to Point Video	Yes No Do Not Disturb	No	Yes
Auto Answer Multipoint Video	Yes No Do Not Disturb	No	Yes
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Disabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	Yes
Background	Choose image file	No file selected	Yes
Startup Background	Choose image file	No file selected	Yes
Kiosk Mode	Checkbox	Disabled	Yes
Home Screen Icons	Checkbox	Disabled	Yes
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			

Admin Settings Area	High		
	Range	Default Value	Configurable?
Enable Polycom Touch Device **Note:** Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Disabled	Yes
Serial Ports			
Mode			
RS-232 Mode Note: Some systems support only a subset of listed modes.	Off Control Camera Control Closed Caption Pass Thru	Off	Yes
Login Mode	None, Admin password only, Username/Password	Admin password only	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto TLS TCP UDP	TLS	Yes
Dialing Preference			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	AVC Only	Yes
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes

Admin Settings Area	High		
	Range	Default Value	Configurable?
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP H.323 SIP	IP H.323	Yes
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	SIP	Yes
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	H.323	Yes
Audio/Video			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Disabled	Yes
Video Inputs			
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People +Content IP	Checkbox	Disabled	Yes

Admin Settings Area	High		
	Range	**Default Value**	**Configurable?**
Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Audio			
Polycom StereoSurround	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	High	Yes
Authentication			
Enable Active Directory External Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Allow Access to User Settings	Checkbox	Disabled	Yes
Restrict to HTTPS	Checkbox	Enabled	Read-only
Web access port (http) **Note:** You cannot select this setting if the **Restrict to HTTPS** setting is enabled.	16-bit integer	Grayed out (80)	Read-only

Admin Settings Area			High		
			Range	Default Value	Configurable?
		Enable Telnet Access	Checkbox	Disabled	Read-only
		Enable SSH Access	Checkbox	Enabled	Yes
		Enable SNMP Access	Checkbox	Disabled	Yes
		Lock Port after Failed Logins	Off, 2-10	Off	Yes
		Port Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours	1 minute	Yes
		Reset Port Lock Counter After	Off, [1..24] hours	Off	Yes
		Enable Whitelist	Checkbox	Disabled	Yes
		Idle Session Timeout in Minutes	1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480	10	Yes
		Maximum Number of Active Sessions	10, 15, 20, 25, 30, 35, 40, 45, 50	25	Yes
	Encryption				
		Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	Required for Video Calls Only	Yes
		Require FIPS 140 Cryptography	Checkbox	Enabled	Yes
Local Accounts					
	Account Lockout				
		Lock Admin Account After Failed Logins	Off 2-10	3	Yes

Admin Settings Area	High		
	Range	Default Value	Configurable?
Admin Account Lock Duration	1, 2, 3, 5 minutes	1	Yes
Reset Admin Account Lock Counter After Failed Logins	Off, [1..24] hours	Off	Yes
Lock User Account After Failed Logins	2-10	3	Yes
User Account Lock Duration	1, 3, 5, 10, 15, 20, 30 minutes 1, 2, 4, 8 hours	1 minute	Yes
Reset User Account Lock Counter After Failed Logins	Off, [1..24] hours	Off	Yes
Login Credentials			
Use Room Password for Remote Access	Checkbox	Enabled	Yes
Require User Login for System Access	Checkbox	Enabled	Yes
Password Requirements			
Admin (Room, Remote), User (Room, Remote)			
Reject Previous Passwords	Off, 1-16	10	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180	90	Yes
Minimum Changed Characters	1-4	4	Yes

Admin Settings Area	High		
	Range	Default Value	Configurable?
Password Expiration Warning	1-7	4	Yes
Remote Access (Admin Remote, User Remote)			
Minimum Length	1-16, 32	6	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
User (Room), Admin (Room)			
Minimum Length	8-16, 32	6	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes

Admin Settings Area		**High**		
		Range	**Default Value**	**Configurable?**
	Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
	Meeting			
	Minimum Length	Off, 1-20, 32	Off	Yes
	Require Lowercase Letters	Off, 1, 2, All	Off	Yes
	Require Uppercase Letters	Off, 1, 2, All	Off	Yes
	Require Numbers	Off, 1, 2, All	Off	Yes
	Require Special Characters	Off, 1, 2, All	Off	Yes
	Reject Previous Passwords	Off, 1-16	10	Yes
	Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
	Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
	SNMP **Note:** SNMP passwords are applicable only when the system uses SNMP v3.			
	Minimum Length	8-16, 32	8	Yes
	Require Lowercase Letters	Off, 1, 2, All	1	Yes
	Require Uppercase Letters	Off, 1, 2, All	1	Yes
	Require Numbers	Off, 1, 2, All	1	Yes
	Require Special Characters	Off, 1, 2, All	1	Yes

Admin Settings Area	High		
	Range	Default Value	Configurable?
Reject Previous Passwords	Off, 1-16	5	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
Certificates			
Certificate Options			
Always Validate Peer Certificates from Browser	Checkbox	Enabled	Yes
Always Validate Peer Certificates from Server	Checkbox	Enabled	Yes
Revocation			
Revocation Method	OCSPCRL	OCSP	Yes
Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner			
Enable Security Banner	Checkbox	Disabled	Yes
Banner Text	DoDCustom	Custom	Yes
Local System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Remote System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Servers			
Directory Servers			

Admin Settings Area	High		
	Range	**Default Value**	**Configurable?**
Server Type	Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status	N/A	Disabled	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Provisioning Service	Checkbox	Disabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service	Checkbox	DIsabled	Yes
	Domain Name User Name Password Server Address		

Diagnostics Area	High		
	Range	**Default Value**	**Configurable?**
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Yes

Changing High Security Profile Default Values

When you configure the system to use the High Security Profile, the system forces you to change the following settings from their default values:

- Admin account room password
- User account room password
- Admin account remote access password

Configure Security Profiles

Medium Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **Medium** security profile.

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
Place a Call			
Contacts	Search Box	No value	Yes
Speed Dial			
Edit	Search Box	No value	Yes
Manual Dial			
	Entry box	No value	Yes
	VideoAudio	Video	Yes
	Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144	Auto	Yes
	Auto H.323 SIP	Auto	Yes
General Settings			
System Settings			
Call Settings			

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
Auto Answer Point to Point Video	Yes No Do Not Disturb	No	Yes
Auto Answer Multipoint Video	Yes No Do Not Disturb	No	Yes
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Enabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	Yes
Background	Choose image file	No file selected	Yes
Startup Background	Choose image file	No file selected	Yes
Kiosk Mode	Checkbox	Disabled	Yes
Home Screen Icons	Checkbox	Disabled	Yes
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			

Admin Settings Area	**Medium**		
	Range	**Default Value**	**Configurable?**
Enable Polycom Touch Device **Note:** Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Disabled	Yes
Serial Ports			
Mode			
RS-232 Mode Note: Some systems support only a subset of listed modes.	Off Control Camera Control Closed Caption Pass Thru	Off	Yes
Login Mode	Range: None, Admin password only, Username/Password	Admin password only	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto, TLS, TCP, UDP	TLS	Yes
Dialing Preference			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes

Admin Settings Area	Medium		
	Range	**Default Value**	**Configurable?**
TIP	Checkbox	Disabled	Yes
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP H.323 SIP	IP H.323	Yes
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	SIP	Yes
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	H.323	Yes
Audio/Video			
Video Inputs			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Disabled	Yes
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People +Content IP	Checkbox	Enabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Enabled	Yes

Admin Settings Area	**Medium**		
	Range	**Default Value**	**Configurable?**
Audio			
Polycom StereoSurround	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	Medium	Yes
Authentication			
Enable Active Directory External Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Allow Access to User Settings	Checkbox	Disabled	Yes
Restrict to HTTPS	Checkbox	Enabled	Yes
Web access port (http) **Note:** You cannot select this setting if the **Restrict to HTTPS** setting is enabled.	16-bit integer	Grayed out (80)	Read only
Enable Telnet Access	Checkbox	Disabled	Yes
Enable SSH Access	Checkbox	Enabled	Yes

Admin Settings Area	Medium		
	Range	**Default Value**	**Configurable?**
Enable SNMP Access	Checkbox	Disabled	Yes
Lock Port after Failed Logins	Off, 2-10	Off	Yes
Port Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours	1 minute	Yes
Reset Port Lock Counter After	Off, [1..24] hours	Off	Yes
Enable Whitelist	Checkbox	Disabled	Yes
Idle Session Timeout in Minutes	1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480	10,15,20,25, 30,35,40,45, 50	Yes
Maximum Number of Active Sessions	10, 15, 20, 25, 30, 35, 40, 45, 50	25	Yes
Encryption			
Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	When Available	Yes
Require FIPS 140 Cryptography	Checkbox	Enabled	Yes
Local Accounts			
Account Lockout			
Lock Admin Account After Failed Logins	Off, 2-10	3	Yes
Admin Account Lock Duration	1, 2, 3, 5 minutes	1	Yes
Reset Admin Account Lock Counter After	Off, [1..24] hours	Off	Yes
Lock User Account After Failed Logins	Off, 2-10	3	Yes

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
User Account Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes 1, 2, 4, 8 hours	1 minute	Yes
Reset User Account Lock Counter After	Off, [1..24] hours	Off	Yes
Login Credentials			
Use Room Password for Remote Access	Checkbox	Disabled	Yes
Require User Login for System Access	Checkbox	Disabled	Yes
Password Requirements			
Admin (Room, Remote), User (Room, Remote)			
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180	Off	Yes
Minimum Changed Characters	Off, 1-4, All	Off	Yes
Password Expiration Warning	Off, 1-7	Off	Yes
Remote Access (Admin Remote, User Remote)			
Minimum Length	1-16, 32	3	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes

Admin Settings Area	**Medium**		
	Range	**Default Value**	**Configurable?**
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
User (Room), Admin (Room)			
Minimum Length	8-16, 32	8	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
Meeting			
Minimum Length	Off, 1-20, 32	Off	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes

Admin Settings Area	**Medium**		
	Range	**Default Value**	**Configurable?**
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
SNMP **Note:** SNMP passwords are applicable only when the system uses SNMP v3.			
Minimum Length	8-16, 32	3	Yes
Require Lowercase Letters	Off, 1, 2, All	Off	Yes
Require Uppercase Letters	Off, 1, 2, All	Off	Yes
Require Numbers	Off, 1, 2, All	Off	Yes
Require Special Characters	Off, 1, 2, All	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
Certificates			
Certificate Options			
Always Validate Peer Certificates from Browser	Checkbox	Disabled	Yes
Always Validate Peer Certificates from Server	Checkbox	Disabled	Yes

Admin Settings Area	Medium		
	Range	**Default Value**	**Configurable?**
Revocation			
Revocation Method	OCSPCRL	OCSP	Yes
Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner			
Enable Security Banner	Checkbox	Disabled	Yes
Banner Text	DoDCustom	Custom	Yes
Local System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Remote System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Servers			
Directory Servers			
Server Type	Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status	N/A	Disabled	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
Enable Recording Service	Checkbox	DIsabled	Yes
	Recording Service Domain Name User Name Password Server Address		

Diagnostics Area	Medium		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Read only

Changing Medium Security Profile Default Values

When you configure the system to use the Medium Security Profile, it forces you to change the following settings from their default values:

- Admin account room password
- User account room password

Low Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **Low** security profile.

Admin Setting	Low		
	Range	Default	Configurable?
Place a Call			

Admin Setting	Low		
	Range	**Default**	**Configurable?**
Contacts	Search box	No value	Yes
Speed Dial	Search box	No value	Yes
Recent Calls			
Manual Dial	Entry box	No value	Yes
	Video Audio	Video	
	Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144	Auto	
	Auto H.323 SIP	Auto	
Admin Settings > **General Settings** > **My Information**			
Contact Information	Entry boxes	No value	Yes
Location			
Admin Settings > **General Settings** > **System Settings**			
System Name			
System Name	Entry box	No value	
Call Settings			
Maximum Time in Call	Off, 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hours, 7 hours, 8 hours, 9 hours, 10 hours, 11 hours, 12 hours, 24 hours, 48 hours	8 hours	Yes
Auto Answer Point to Point Video	Yes No Do Not Disturb	No	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Auto Answer Multipoint Video	Yes No Do Not Disturb	No	Yes
Mulitpoint Mode	Auto, Full Screen, Discussion, Presentation	Discussion	Yes
Display Icons in a Call	Checkbox	Enabled	Yes
Enable Flashing Incoming Call Notification	Checkbox	Disabled	Yes
Preferred 'Place a Call' Navigation	Keypad Contacts Recent Calls	Keypad	Yes
Automatic Self View Control	Checkbox	Enabled	Yes
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Enabled	Yes
Maximum Number to Display	25, 50, 75, 100	100	Yes
Admin Settings > **General Settings** > **Home Screen Settings**			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	
Background	Choose Image File	No file selected	
Startup Background	Choose Image File	No file selected	
Kiosk Mode	Checkbox	Disabled	
Home Screen Icons	Checkbox	Disabled	
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes

Admin Setting	Low		
	Range	Default	Configurable?
RealPresence Touch Background	Choose image file	Image file not selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing > Enable Polycom Touch Device			
Note: Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Disabled	Yes
Serial Ports > Mode	RS-232 Mode Note: Some RealPresence Centro systems support only a subset of listed modes.		
	Off Control Camera Control Closed Caption Pass Thru	Off	Yes
Login Mode	None Admin Password only Username/Password	Admin Password Only	Yes
Network > IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto TLS TCP UDP	TLS	Yes
Dialing Preference			

Admin Setting	Low		
	Range	**Default**	**Configurable?**
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes
Call Type Order	Video	Video	No
Video Dialing Order	IP H.323 SIP	IP H.323	Yes
Auto Dialing Order Preference 1 (only displays if **Enable Audio-Only Calls** checkbox is selected)	SIP H.323	SIP	Yes
Auto Dialing Order Preference 2 (only displays if **Enable Audio-Only Calls** checkbox is selected)	H.323 SIP	H.323	Yes
Audio/Video > Video Inputs > Sleep			
Display	No Signal Black	No Signal	Yes
Time Before System Goes to Sleep	Off 1 minute 3 minutes 15 minutes 30 minutes 60 minutes 2 hours 4 hours 8 hours	15 minutes	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Enable Mic Mute in Sleep Mode	Checkbox	Disabled	Yes
General Camera Settings			
Allow Other Participants in a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People+Content IP	Checkbox	Enabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Enabled	Yes
Audio			
Polycom StereoSurround	Checkbox	Disabled	Yes
Security > Global Security > Security Profile			
Security Profile	Maximum High Medium Low	Low	Yes
Authentication			
Enable Active Directory External Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Allow Access to User Settings	Checkbox	Disabled	Yes
Restrict to HTTPS	Checkbox	Enabled	Yes
Web access port (http) Note:You cannot select this setting if the **Restrict to HTTPS** setting is enabled.	16-bit integer	Grayed out (80)	Read only
Enable Telnet Access	Checkbox	Disabled	Yes
Enable SSH Access	Checkbox	Enabled	Yes
Enable SNMP Access	Checkbox	Disabled	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Lock Port after Failed Logins	Off, 2-10	Off	Yes
Port Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes 1, 2, 4, 8 hours	1 minute	Yes
Reset Port Lock Counter After	Off, [1..24] hours	Off	Yes
Enable Whitelist	Checkbox	Disabled	Yes
Idle Session Timeout in Minutes	1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480	10,15,20,25,30,35,40 ,45,50	Yes
Maximum Number of Active Sessions	10, 15, 20, 25, 30, 35, 40, 45, 50	25	Yes
Encryption			Yes
Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	When Available	Yes
Require FIPS 140 Cryptography	Checkbox	Enabled	Yes
Local Accounts > Account Lockout			Yes
Lock Admin Account After Failed Logins	Off, 2-10	3	Yes
Admin Account Lock Duration	1, 2, 3, 5 minutes	1	Yes
Reset Admin Account Lock Counter After	Off, [1..24] hours	Off	Yes
Lock User Account After Failed Logins	Off, 2-10	3	Yes
User Account Lock Duration	1, 2, 3, 5, 10, 20, 30 minutes 1, 2, 4, 8 hours	1 minute	Yes
Reset User Account Lock Counter After	Off, [1..24] hours	Off	Yes
Login Credentials			Yes
Use Room Password for Remote Access	Checkbox	Disabled	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Require User Login for System Access	Checkbox	Disabled	Yes
Password Requirements			
Admin			
Minimum Length	Off, 1-32	Off	Yes
Require Lowercase Letters	Off, 1, 2, all	Off	Yes
Require Uppercase Letters	Off, 1, 2, all	Off	Yes
Require Numbers	Off, 1, 2, all	Off	Yes
Require Special Characters	Off, 1, 2, all	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200	Off	Yes
Minimum Changed Characters	Off, 1, 2, 3, 4, all	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1, 2, 3, 4	Off	Yes
Password Expiration Warning	Off, 1-7	Off	Yes
Can Contain ID or Its Reverse Form	Checkbox	Selected	Yes
User Room			
Minimum Length	Off, 1-32	Off	Yes
Require Lowercase Letters	Off, 1, 2, all	Off	Yes
Require Uppercase Letters	Off, 1, 2, all	Off	Yes
Require Numbers	Off, 1, 2, all	Off	Yes
Require Special Characters	Off, 1, 2, all	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Maximum Password Age in Days	30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200	Off	Yes
Minimum Changed Characters	Off, 1, 2, 3, 4, all	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1, 2, 3, 4	Off	Yes
Password Expiration Warning	Off, 1-7	Off	Yes
Can Contain ID or Its Reverse Form	Checkbox	Selected	Yes
Meeting			
Minimum Length	Off, 1-32	Off	Yes
Require Lowercase Letters	Off, 1, 2, all	Off	Yes
Require Uppercase Letters	Off, 1, 2, all	Off	Yes
Require Numbers	Off, 1, 2, all	Off	Yes
Require Special Characters	Off, 1, 2, all	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	none	Off	Yes
Minimum Changed Characters	none	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1, 2, 3, 4	Off	Yes
Password Expiration Warning	none	Off	Yes
Can Contain ID or Its Reverse Form	Checkbox	Selected	Yes
Remote Access			
Minimum Length	Off, 1-32	Off	Yes
Require Lowercase Letters	Off, 1, 2, all	Off	Yes
Require Uppercase Letters	Off, 1, 2, all	Off	Yes
Require Numbers	Off, 1, 2, all	Off	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Require Special Characters	Off, 1, 2, all	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200	Off	Yes
Minimum Changed Characters	Off, 1, 2, 3, 4, all	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1, 2, 3, 4	Off	Yes
Password Expiration Warning	Off, 1-7	Off	Yes
Can Contain ID or Its Reverse Form	Checkbox	Selected	Yes
SNMP			
Minimum Length	Off, 1-32	Off	Yes
Require Lowercase Letters	Off, 1, 2, all	Off	Yes
Require Uppercase Letters	Off, 1, 2, all	Off	Yes
Require Numbers	Off, 1, 2, all	Off	Yes
Require Special Characters	Off, 1, 2, all	Off	Yes
Reject Previous Passwords	Off, 1-16	Off	Yes
Minimum Password Age in Days	Off, 1, 5, 10, 15, 20, 30	Off	Yes
Maximum Password Age in Days	none	Off	Yes
Minimum Changed Characters	none	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1, 2, 3, 4	Off	Yes
Password Expiration Warning	none	Off	Yes
Can Contain ID or Its Reverse Form	Checkbox	Not Selected	Yes
Certificates > Certificate Options			
Always Validate Peer Certificates from Browser	Checkbox	Disabled	Yes

Admin Setting	Low		
	Range	Default	Configurable?
Always Validate Peer Certificates from Server	Checkbox	Disabled	Yes
Revocation			
Revocation Method	OCSPCRL	OCSP	Yes
Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner			
Enable Security Banner	Checkbox	Disabled	Yes
Banner Text	DodCustom	Custom	Yes
Local System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Remote System Banner Text	Unicode characters, 2048 bytes max	Null (no text)	Yes
Servers > Directory Servers			
Server Type	Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status	N/A	Disabled	Read only
SNMP			
Version 1	Checkbox	Disabled	Yes
Version 2c	Checkbox	Disabled	Yes
Version 3	Checkbox	Disabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable RealPresence Recording Suite	Checkbox	Disabled	Yes
Registration Status	Checkbox	Status text	Read Only

Admin Setting	**Low**		
	Range	**Default**	**Configurable?**
	Domain Name User Name Password Server Address	Enabled	Yes
Diagnostics > System > System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Read only

Call Speeds and Resolutions

Topics:

See the following topics to learn about maximum call speeds and resolutions for different call types.

Point-to-Point Call Speeds

The maximum allowable H.323/SIP point-to-point call speed for the RealPresence Centro system is 6144 kbps.

Multipoint Call Speeds for RealPresence Centro Systems

The following table shows the maximum allowable H.323/SIP call speeds for the number of sites in a call. Maximum speeds can be further limited by the communications equipment. Multipoint option keys are required for some of the capabilities shown in the table.

Number of Sites in Call	Max Speed for Each Site	Max Speed for Each Site (ICE Enabled, Skype for Business 2015	Max Speed for Each Site (CCCP Skype for Business 2015 with A/V MCU)
3	3072 kbps	1024 kbps	664 kbps
4	2048 kbps	512 kbps	664 kbps
5	1536 kbps	384 kbps	664 kbps
6	1152 kbps	256 kbps	664 kbps

These values do not apply when the Microsoft Skype Interoperability option is enabled, whether it is in a Skype for Business 2015 environment. When this option key is enabled, all calls are CCCP calls and are capped at 1920 kbps due to ICE restrictions.

The values in the Max Speed for Each Site (ICE Enabled, Skype for Business 2015) column are applicable only when both of the following criteria are met:

- The Skype Interoperability option key is disabled, so that calls are negotiated with H.263 using Skype for Business 2015 clients.

- The ICE calls go across the firewall boundary.

High-Profile Call Speeds and Resolutions

This section includes the H.264 high-profile resolutions and frame rates sent in calls between two RealPresence Centro systems. Resolutions and frame rates are based on both the call speed and the **Optimized for** setting of your Camera input.

Due to the complexities of the systems and their capabilities, it is not possible to include tables of the resolutions and frame rates for calls between a system and a different type of endpoint or a multipoint resource. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

The values for sharpness and motion are the same from 2 MB to 6 MB for systems that support higher call speeds. The difference between NTSC and PAL cameras is how frame rates are calculated:

- NTSC 60 fps equals PAL 50 fps
- NTSC 30 fps equals PAL 25 fps

The following table shows the resolutions for People video on systems with NTSC cameras in H.264 high-profile calls. The actual resolutions and frame rates might vary and depend upon the call types and call scenarios in your environment.

Call Speeds and Resolutions in High-Profile Calls

		Camera Source			
		HD (1280x720x60)		HD (1920x1080x60)	
Call Speed (kbps)	Motion/ Sharpness	Resolution	Max Frame Rate (fps)	Resolution	Max Frame Rate (fps)
<160	Motion	512x288	60	512x288	60
160-511	Motion	640x368	60	640x368	60
512-831	Motion	848x480	60	848x480	60
832-895	Motion	1024x576	60	720x832	60
896-1727	Motion	1280x720	60	1280x720	60
>=1728	Motion	1280x720	60	1920x1080	60
<128	Sharpness	640x368	30	640x368	30
128-511	Sharpness	1024x576	30	1024x576	30
512-1023	Sharpness	1280x720	30	1280x720	30
>=1024	Sharpness	1280x720	30	1920x1080	30

The following table shows the resolutions for People video on systems with NTSC EagleEye Acoustic cameras in H.264 high-profile calls.

Call Speeds and Resolutions in High-Profile Calls for EagleEye Acoustic

		Camera Source	
		HD (1920x1080x30)	
Call Speed (kbps)	**Motion/Sharpness**	**Resolution**	**Max Frame Rate (fps)**
<128	Motion/Sharpness	640x368	30
128-511	Motion/Sharpness	1024x576	30
512-1023	Motion/Sharpness	1280x720	30
>=1024	Motion/Sharpness	1920x1080	30

Multipoint Resolutions for High Definition Video for RealPresence Centro Systems

Polycom offers enhanced high definition (HD) multipoint resolutions, maximizing video quality in multipoint conferences for RealPresence Centro systems. This feature increases the maximum transmitting and receiving video resolutions in multipoint video conferences. During a multipoint video conference, if any endpoints in the video conference do not support high resolution video and transmit lower resolution video, all endpoints receive lower resolution video.

The maximum Multipoint Control Unit (MCU) transmitting and receiving resolutions are specified in the following table. Note that changing from discussion to speaker does not alter the transmit of 960x540 from an endpoint and the receive of 1080p from the endpoints.

RealPresence Centro systems support one endpoint as a host system and up to 5 other endpoints in a 6-way multipoint conference.

Number of Endpoints in the Video Conference	Maximum Transmitting Resolutions	Maximum Receiving Resolutions
2-4 endpoints	1080p, 30fps	960x540p, 30fps
5-8 endpoints	720p, 30fps	640x368p, 30fps

Resolution and Frame Rates for Content Video

The high frame rates with high resolution apply only to point-to-point calls above 832 kbps on RealPresence Centro systems. In addition, you must set **Optimized for** value of your Camera input to **Sharpness**. Low frame rates apply if your call does not meet these requirements.

For multipoint calls, the maximum resolution and frame rate for content is 720p @ 30 fps.

Resolution	Encode Resolution	Sharpness	Motion
800 x 600	800 x 600	30	60
1024 x 768	1024 x 768	30	60
1280 x 720	1280 x 720	30	60
1280 x 768	1280 x 720	30	60
1280 x 1024	1280 x 1024	30	60
1600 x 1200	1280 x 1024	30	60
1680 x 1050	1280 x 720	30	60
1920 x 1080	1920 x 1080	30	60*

*Available only when the **Quality Preference** setting on your system is set to **Content** in **Admin Settings** > **Network** > **IP Network** > **Network Quality**.