ADMINISTRATOR GUIDE

5.0.0 | September 2015 | 3725-63706-007B

Polycom® RealPresence® Group Series

6001 America Center Drive
San Jose, CA 95002
USA

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

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 OpenSourceVideo@polycom.com.

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 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

Conventions Used in Polycom Guides

Polycom guides contain terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions will help you successfully perform tasks.

Information Elements

Polycom guides may include any of the following icons to alert you to important information.

Icons Used in Polycom Guide

Name	Icon	Description
Note		The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone, video, or network performance.
Web Info		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.

Typographic Conventions

A few typographic conventions, listed next, are used in Polycom guides to distinguish types of in-text information.

Typographic Conventions

Convention	Description
Bold	Highlights interface items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. Also used to highlight text to be entered or typed.
Italics	Used to emphasize text, to show example values or inputs (in this form: <*example*>), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Blue Text	Used for cross references to other sections within this document and for hyperlinks to external sites and documents.
`Courier`	Used for code fragments and parameter names.

Before You Begin

The *Polycom RealPresence Group Series Administrator Guide* is for administrators who need to configure, customize, manage, and troubleshoot Polycom® RealPresence® Group systems. This guide covers the RealPresence Group 300, RealPresence Group 310, RealPresence Group 500, and RealPresence Group 700 systems.

Please read the Polycom RealPresence Group system documentation before you install or operate the system. The following related documents for RealPresence Group systems are available from www.polycom.com/videodocumentationsupport.polycom.com/PolycomService/support/cn/support/video/group_series/:

- *Polycom RealPresence Group Series Software, Options*, *and Accessories Installation Guide,* which describes how to install Polycom RealPresence Group software, options, and accessories
- *Polycom RealPresence Group Series User Guide*, and the *Polycom RealPresence Group Series and Polycom Touch Control User Guide*, which describe how to perform video conferencing tasks
- Setup sheets for your hardware
- Release notes
- *Polycom RealPresence Group Series Integrator Reference Guide*, which provides cable information and API command descriptions
- *Polycom RealPresence Group Series Regulatory Notices*, which describes safety and legal considerations for using Polycom RealPresence Group systems

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

System Serial Number: _____

Option Key: _____

Audience, Purpose, and Required Skills

The primary audience for this guide is administrators who need to configure, customize, manage, and troubleshoot Polycom RealPresence Group 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.

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 support.polycom.com.

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.

Introducing the Polycom RealPresence Group Series Systems

The following topics provide an overview of the Polycom® RealPresence® Group systems, including information on setting up, positioning, and starting the system and cameras:

Polycom RealPresence Group Systems

Your Polycom® RealPresence® Group system is a state-of-the-art visual collaboration tool. With crisp, clean video and crystal-clear sound, Polycom RealPresence Group systems provide natural video conferencing interaction using the most robust video communications technology. To fit your space and functional requirements, there are several RealPresence Group systems available.

For technical specifications and detailed descriptions of features available for RealPresence Group systems, please refer to the product literature available at www.polycom.com.

Polycom RealPresence Group 300 Systems

For smaller meeting rooms, huddle rooms, and offices, the RealPresence Group 300 system delivers high-quality and easy-to-use video collaboration at an affordable price.

Polycom RealPresence Group 300 system

Single-cable connections to the camera and display simplify setup, and sharing content is easy with the Polycom People+Content™ IP application. Its sleek design allows it to be easily hidden away, or taken outside the room or building for mobile applications.

Polycom RealPresence Group 310 Systems

For conference rooms and other meeting environments, the RealPresence Group 310 system delivers powerful video collaboration performance in a sleek design that is easy to configure and use.

Polycom RealPresence Group 310 system

You can share content using the Polycom People+Content application and a wired HDMI or VGA connection. Its sleek design allows it to be hidden away, or taken outside the room or building for mobile applications. This system supports single monitor output; an option key is required to connect a second monitor. Multipipoint conference calls are not supported.

Polycom RealPresence Group 500 Systems

For conference rooms and other meeting environments, the RealPresence Group 500 system delivers powerful video collaboration performance in a sleek design that is easy to configure and use.

Support for dual monitors and multiple options for sharing content make it an ideal fit for most standard-sized meeting rooms.

Polycom RealPresence Group 500 system

Single-cable connections for video and audio simplify setup, while the efficient design enables discreet placement of the device. Plus, the small design makes it ideal for mobile applications, whether moved to different locations within a building, or used as part of a mobile video kit.

Polycom RealPresence Group 700 Systems

For boardrooms, lecture halls, and other environments where only the best will do, the RealPresence Group 700 system offers extreme video collaboration performance and flexibility.

Polycom RealPresence Group 700 system

Powerful video processing and several input and output options make it ideal for rooms with complex requirements, such as multiple displays, cameras, and content sources. The intuitive interface that comes standard on all RealPresence Group products makes it easy for even novice users to control the system and get the most out of their video collaboration experience with no hassles.

Set Up Your System Hardware

This manual provides information to supplement the setup sheets provided with your system and its optional components. A printed copy of the system setup sheet is provided with each RealPresence Group system. PDF versions of the system setup sheets are available at support.polycom.com.

Recharge the Remote Control Battery

Your system setup sheet shows how to charge the battery in the remote control the first time. When the remote control battery power is at 10% or less, a notification is displayed on the home screen. The low battery notification returns after you dismiss other notifications, and is not displayed while the system is in a call.

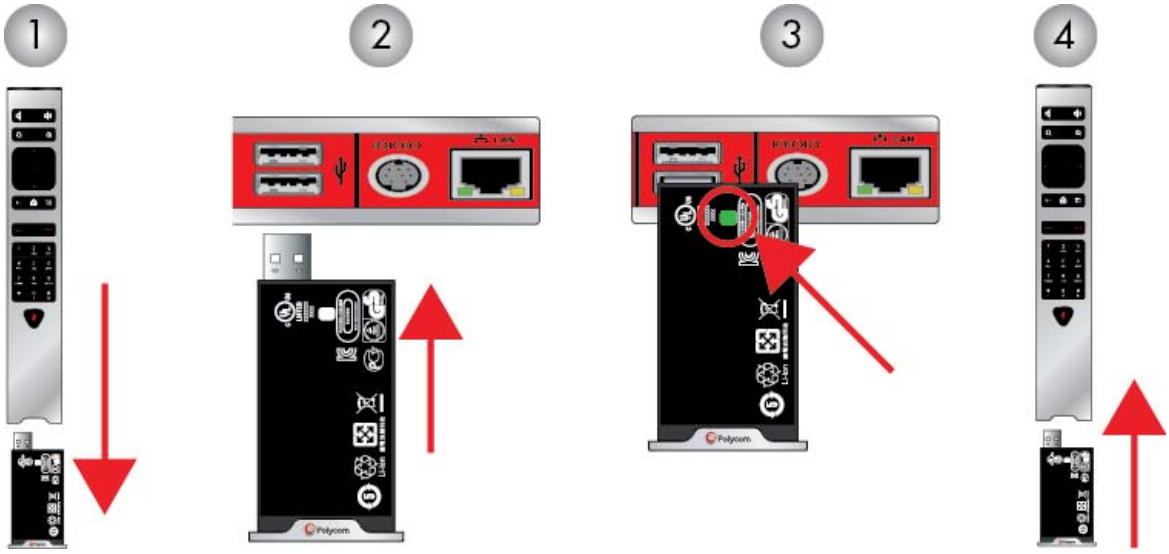
To recharge the remote control battery:

1. Pull the battery out of the end of the remote control.
2. Insert the USB plug into any USB 2.0 port, such as the one on your system. The RealPresence Group 300, RealPresence Group 310, and RealPresence Group 500 systems have two USB 2.0 ports on the back of the systems, while the RealPresence Group 700 system has one USB 2.0 port on the front.
3. While the battery is charging, the status light is orange. After the status light on the battery turns green, remove it from the port.
4. Insert the charged battery into the remote control.

Note: Recharging time

Recharging the battery might take anywhere from 20 minutes to several hours.

Charge the remote control battery



Ref. Number	Description
1	Pull the battery out of the end of the remote control.
2	Insert the USB plug of the battery into a USB 2.0 port.
3	Wait until the status light on the battery turns green.
4	Insert the charged battery into the remote control.

Position the System

Polycom RealPresence Group systems can accommodate being set up in a variety of ways. This section describes placement for your RealPresence Group system, RealPresence Touch, Polycom Touch Control, EagleEye™ Acoustic camera, and EagleEye Director automatic camera positioning system.

Position Polycom RealPresence Group Systems

RealPresence Group systems are designed to be placed on tabletops or in equipment racks. If the system or any accessories are installed in an enclosed space, such as a cabinet, ensure that the air temperature in the enclosure does not exceed 40°C (104° F). You might need to provide forced cooling to keep the equipment within the operating temperature range.

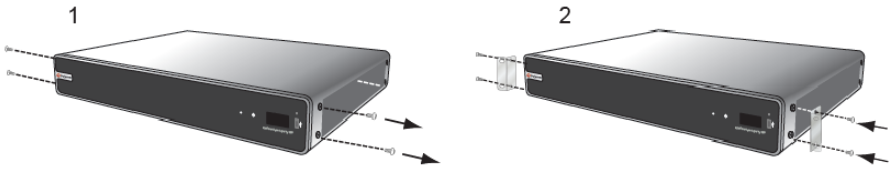
Caution: Allow ventilation
Keep ventilation openings free of any obstructions.

To position the system:

1 Do one of the following:

- If you plan to place the system on a table or open shelf, attach the self-adhesive feet to the bottom of the system.
- If you plan to mount a RealPresence Group 700 system in an equipment rack, install the mounting brackets, as shown in the following figure.

Mount the RealPresence Group 700 system



Note: Mounting bracket differences
Polycom RealPresence Group 300, 310, and 500 systems use a different type of mounting bracket. For more information, refer to support.polycom.com or contact your Polycom distributor.

2 Place the system in the desired location, keeping in mind the following pointers:

- Position the system so that the camera does not face toward a window or other source of bright light.
- Leave enough space to connect the cables easily.
- Place the camera and display together so that people at your site face the camera when they are looking at the display.

Position the RealPresence Touch Device

Polycom RealPresence Group systems can be controlled by the Polycom RealPresence Touch device. Ensure that the RealPresence Touch is conveniently located for use during a meeting, such as on a conference table. Place the device in a location where you can easily touch the screen and see the room system monitor displays. The RealPresence Touch device can be positioned horizontally at either a 30 degree or 65 degree viewing angle.

Position the Polycom Touch Control Device

Polycom RealPresence Group systems can be controlled by the Polycom Touch Control. When the Polycom Touch Control is not paired with a RealPresence Group system, the device can be used as a virtual remote control. To use the Polycom Touch Control as a virtual remote control, ensure that the infrared (IR) transmitter on the front of the device is facing the RealPresence Group system you want to control. Also, make sure that the Touch Control is conveniently located for use during a meeting.

Position the EagleEye Acoustic Camera

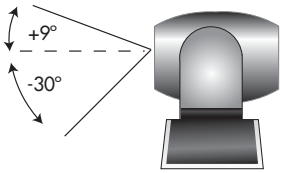
The Polycom EagleEye™ Acoustic camera is designed to be placed on top of your monitor, as shown next.

Position the Polycom EagleEye Director

The Polycom EagleEye Director is an automatic HD tracking system that works with RealPresence Group systems. Refer to Polycom EagleEye Director for more information about the automatic camera positioning system.

Follow these guidelines when you use the EagleEye Director with your RealPresence Group system:

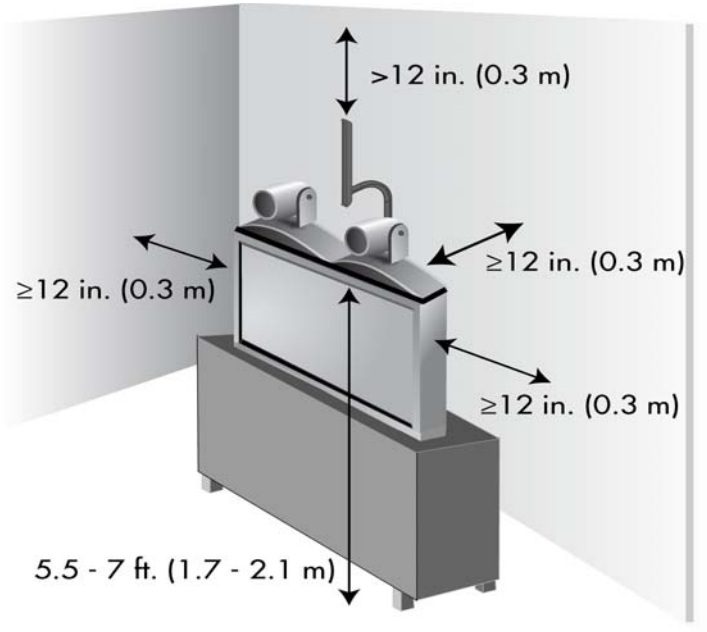
- Avoid setting the Polycom EagleEye Director in the corner of a room. The EagleEye Director should be at least 12 inches away from all of the walls.
- Make sure the EagleEye Director is on a level surface or mounting bracket.
- The camera's viewing angle is approximately 9 degrees above and 30 degrees below its direct line of sight, as shown next.



- To ensure optimal performance of the Polycom EagleEye Director facial recognition feature, follow these suggestions:
  - Provide ample lighting on faces of participants. This allows the system to correctly frame faces, using the eyes, noses, and mouths as guidelines.
  - Allow only minimal backlighting.
- To ensure the best view from the Polycom EagleEye Director voice-tracking feature, follow these suggestions:
  - Make sure ambient room noise is quiet enough to allow the system to locate the participant who is speaking.

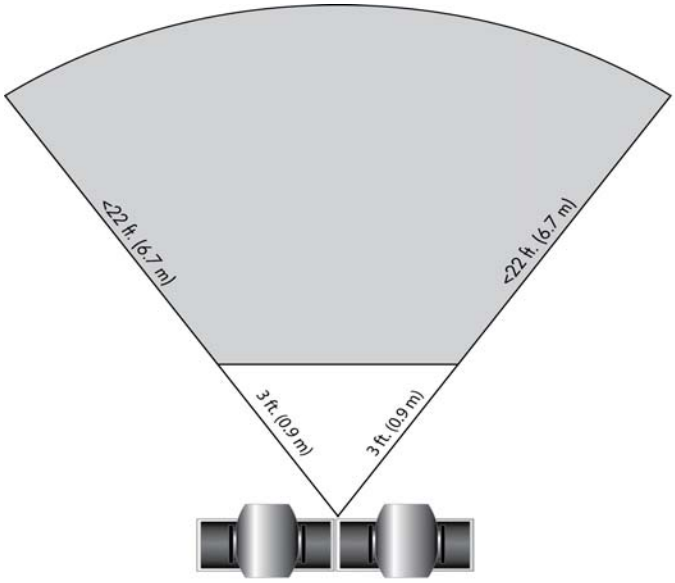
- Be sure to set up the audio connection from the RealPresence Group system to the EagleEye Director, whether you connect it directly to the audio output of the RealPresence Group system or to an audio processor managing the room audio.
- Set the EagleEye Director on top of a monitor. Ideally, place the camera between 5.5 and 7 feet from the ground.

EagleEye Director placement



- Ensure that people are sitting within the viewing range of between 3 and 22 feet from the device.

EagleEye Director viewing range



Power On and Off

After you have connected all of the equipment that you will use with the RealPresence Group system, connect the power and power on the system. Make sure that the system is powered off before you connect devices to it. Note that Polycom RealPresence Group 300, 310, 500, and 700 systems do not have what you might think of as a power *button*—they have a power *proximity sensor*. Instead of pressing an actual button that moves, you touch the sensor (or near the sensor) that indicates power  on the front of the system.

Polycom Touch Devices

For instructions on how to power on and off the RealPresence Touch, refer to Connect and Power On the Polycom® RealPresence Touch™.

For instructions on how to power on and off the Polycom Touch Control, refer to Connect the Polycom Touch Control.

Power-On Self Test (POST)

After being powered on, the RealPresence Group systems automatically perform system health checks before the system is initialized. This process is known as a power-on self test, or POST. The status of the POST sequence is displayed with the LED indicator light on the front of the device, or in the case of the RealPresence Group 700 system, in the text field display on the front of the device. For more information about what the colors of the indicator lights mean, refer to RealPresence Group System Indicator Lights. When the POST sequence completes with no severe errors, the RealPresence Group system starts normally.

Test results for the RealPresence Group 300, 310, 500, and 700 systems are logged in the system memory. If any warnings occur during POST on RealPresence Group 300, 310, 500, and 700 systems, you can view them after the system starts by going to **Settings > System Information > Status > Active Alerts** in the local interface, or **Diagnostics > System > Active Alerts** in the web interface. If a severe error occurs during startup, the system does not start up. Contact Polycom technical support.

Power On and Off Polycom RealPresence Group 300, 310, and 500 Systems

The RealPresence Group 300, 310, and 500 systems are powered off and on using the same steps.

- If the system is asleep, press any button on the remote control or pick up the remote control to wake the system up.
- Press  on the remote control.
- Touch the power sensor on the front of the system.

The Polycom screen is displayed within about 10 seconds.

To power off the RealPresence Group system, do one of the following:

- Press and hold  on the remote control.

  Refer to Configure Remote Control Behavior for more information about programming the remote control.

- Touch and hold the power sensor on the front of the system. The indicator light changes color and blinks, indicating that the system is shutting down. Release the power sensor when the indicator light changes color.

Power On and Off Polycom RealPresence Group 700 Systems

The RealPresence Group 700 system can be powered on and off with the remote using the same buttons as shown for the RealPresence Group 300, 310, and 500 systems; however, the Group 700 system supports a low-power standard that limits the power supplied to the camera when the system is powered off. So, if the EagleEye IV or EagleEye III camera is receiving its power only from the HDCI connector attached to the system, it will not have an active IR receiver capable of powering on the system using the handheld remote when in the Power Off state.

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

- Provide direct power to the EagleEye III or EagleEye IV camera with the optional EagleEye camera power supply, 1465-52748-040. This allows the IR sensor to remain in a Power On state, so that the camera is capable of receiving IR commands from the remote control.
- Position the RealPresence Group 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 RealPresence Group system.

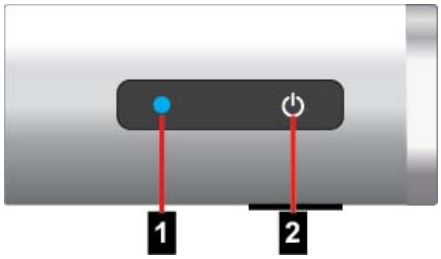
Sleep and Wake States

The RealPresence Group systems support Sleep and Wake states in which the system provides power to the EagleEye IV or EagleEye III camera. This allows the EagleEye IV or EagleEye III camera 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.

Indicator Lights

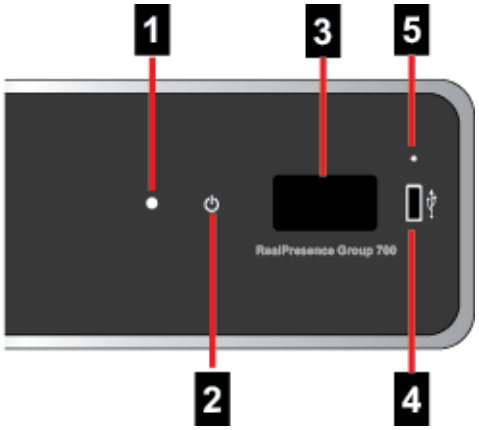
RealPresence Group System Indicator Lights

The following figure shows the location of the power sensor and indicator light on the front of the Polycom RealPresence Group 300, 310, and 500 system.



Ref. Number	Description
1	LED indicator light
2	Power sensor

The following figure identifies the features on the front of the RealPresence Group 700 system.



Ref. Number	Description
1	LED indicator light
2	Power sensor
3	Status display area
4	USB 2.0 port
5	Restore button

Use the USB port for any USB 2.0 device.

Note: Maximum Security Profile status display area
If your RealPresence Group 700 systems operates with the Maximum Security Profile, the status display area does not display the software version or IP address.

Brief status and diagnostic messages are displayed in the status display area of the RealPresence Group 700 system. The LED on the front of all RealPresence Group systems provides the following information.

Indicator Light	System Status
Off	System is powered off.
Blinking blue light	In a POST sequence, no errors are occurring and tests are successful. The system continues to blink blue and initializes after the sequence is complete if no severe errors occur.

Indicator Light	System Status
Blinking amber light	In a POST sequence, at least one test has resulted in a warning error. The system continues to blink amber but initializes after the sequence is complete if no severe errors occur.
Blinking red light	In a POST sequence, at least one test has resulted in a severe error. The system continues to blink red and will not start up.
Steady blue light	System is initializing. System is awake.
Blinking blue light	System received an IR (infrared) signal. System is receiving a call.
Steady amber light	System is asleep.
Alternating blue and amber lights	System is in software update mode. System is in factory restore mode.
Fast blinking amber light	System is shutting down.
Steady green light	System is in a call.

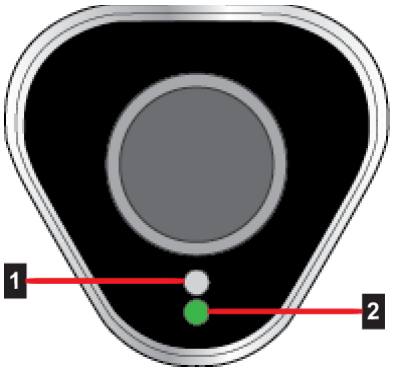
Polycom Touch Control Indicator Light

When the Polycom Touch Control is on, the **Home** button is lit.

Polycom EagleEye Acoustic Camera Indicator Lights

The following figure shows the location of the LED on the front of the EagleEye Acoustic camera.

EagleEye Acoustic indicator lights



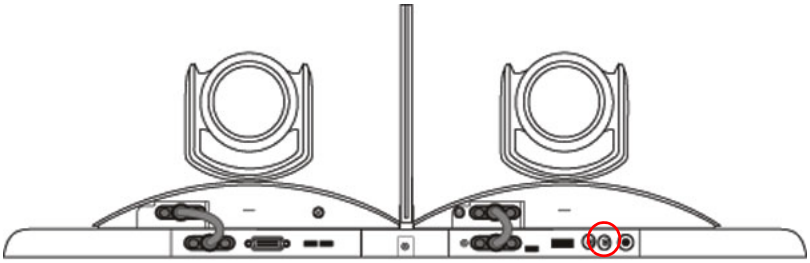
Ref. Number	Description
1	IR Sensor
2	System Status

The system status light provides the following information.

Indicator Light	System Status
Steady blue light	System is on and awake.
Blinking blue light	Camera firmware is being updated.
Steady amber light	System is asleep.
Steady green light	System is in a call.

Polycom EagleEye Director Indicator Light

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



This indicator light provides the following information.

Indicator Light	Status
Steady green light	Cameras are ready; camera tracking is off
Steady red light	Cameras are powering on
Blinking red light	Factory restore on the cameras is starting
Blinking blue light	Camera tracking is on

EagleEye Producer Indicator Lights

A light-emitting diode (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	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

LED	System State
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

Connect and Power On the Polycom® RealPresence Touch™

This section describes how you can make connections so that you can power on, power off, and wake up the Polycom® RealPresence Touch™. For information about enabling and setting the RealPresence Touch, refer to Enable and Set Up the RealPresence Touch.

Connect and Power On the RealPresence Touch

Before you can power on the RealPresence Touch, you must connect the Ethernet cable to the device.

To connect and power on the RealPresence Touch:

1. Connect the Ethernet cable to the back of the RealPresence Touch device.
2. Plug the Ethernet cable into the wall outlet. Do one of the following:
   - 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 optional power supply adapter. Then connect the power supply adapter to a LAN outlet and power outlet. The power supply adapter is sold separately.

   The RealPresence Touch powers on and displays the language selection screen in the setup wizard.

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.

To power off the RealPresence Touch:

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 Up the RealPresence Touch

After inactivity, you must wake the RealPresence Touch by touching the screen.

Wake Up the RealPresence Touch

After two minutes of inactivity, the RealPresence Touch goes to sleep.

To wake up the RealPresence Touch:

» Touch the screen to wake it up.

The last screen that was displayed before the sleep state is displayed.

Connect the Polycom Touch Control

This section describes how you can make connections so that you can power on, power off, and wake up the Touch Control. For information about setting up and using the Touch Control, refer to Set Up the Polycom Touch Control.

Power On the Polycom Touch Control

Before you can power on the Polycom Touch Control, you must connect the Ethernet cable to the device and to a wall outlet.

To power on the Polycom Touch Control:

1. Connect the Ethernet cable to the underside of the Polycom Touch Control.
2. Plug the Ethernet cable into the wall outlet. Do one of the following:
   - 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 optional power supply adapter. Then connect the power supply adapter to a LAN outlet and power outlet. The power supply adapter is sold separately.

   The Polycom Touch Control powers on and displays the language selection screen.

Power Off the Polycom Touch Control

To power off the Polycom Touch Control:

1. From the Touch Control Home screen, touch  **User Settings**.
2. Scroll to the Power section.
3. Select **Touch Control Power**.
4. In the menu that appears, select **Power Off the Touch Control**. If you choose to power off the Polycom Touch Control, you must disconnect and reconnect the LAN cable to power it on again.

Wake Up the Polycom Touch Control

The Touch Control goes to sleep after two minutes of inactivity.

To wake up the Polycom Touch Control:

» Touch anywhere on the screen to wake it up.

Configure the RealPresence Group System

This section describes how to configure your RealPresence Group system by using the setup wizard. It also explains how to access administrative settings in the local and web interfaces.

Setup Wizard

When you power on your system for the first time, the setup wizard leads you through the minimum configuration steps required to place a call. The setup wizard is also called the out-of-box (OOB) state.

The setup wizard allows you to set an Admin ID and password, which allows you to 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. Admin and User IDs are not case sensitive.

Note: Remember admin password

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 in order to access the Admin Settings and reset the password.

You can run the setup wizard or view the configuration screens in either of the following two ways.

- **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 web interface.

- **From a remote location**—If you know the IP address of the system, you can access and configure it using the web interface. For more information about using the web interface, refer to Use the Polycom RealPresence Group System Web Interface.

The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the restore button.

Note: Web Interface Start Up After Setup Wizard is Complete

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

Admin Settings

After you run the setup wizard, you can view or change the system's configuration by going to **Settings > Administration** in the system's local interface or to **Admin Settings** in the web interface. The local interface has a subset of the administration settings that are available in the web interface.

Note: Configuration and security when paired

When a RealPresence Group System is paired with a Polycom Touch Control, the following statements are true:

- You can change the system's configuration using the web interface only.
- During pairing, when prompted to enter the Admin ID and Admin Password, but no Admin password has been configured, you must submit a blank password.

If you enable a provisioning service, any settings provisioned by the Polycom RealPresence® Resource Manager system might be displayed as read-only settings in the Admin Settings. For more information about automatic provisioning, refer to the RealPresence Resource Manager system documentation on the Polycom web site.

The Polycom Touch Control has separate admin settings that allow you to update Touch Control software and configure LAN, regional, and security properties for the device. Refer to the following sections for more information:

- Configure the Polycom Touch Control LAN Properties
- Configure Polycom Touch Control Regional Settings
- Configure Admin ID and Password for the Polycom Touch Control

An Admin ID and password might be configured for the Touch Control Administration settings. The default ID is `admin` and the default password is `456`.

Note: PKI certificates

If your RealPresence Group system will be provisioned by the RealPresence Resource Manager system and you plan to use PKI certificates, make sure you configure the **Host Name** setting on the web interface in **Admin Settings > Network > LAN Properties > LAN Options**. Use the same name as the name that the RealPresence Resource Manager system will provision, so that certificate signing requests (CSRs) generated during certificate installation have the correct host name information in them. For more information about PKI certificates, refer to Manage Certificates and Revocation. For more information about provisioning, refer to Use a Provisioning Service.

Set Up the System Name

The system name appears on the screen of the far-end site when you make a call. The RealPresence Group system interface supports the language fonts listed in the following table. Other languages might not display correctly.

Supported language fonts

Afrikaans	German	Serbian
Albanian	Greek	Slovak
Arabic	Hungarian	Slovenian
Azerbaijani	Icelandic	Spanish
Basque	Indonesian	Swahili
Belarusian	Italian	Swedish
Bulgarian	Japanese	Tajik
Catalan	Kazakh	Thai

Supported language fonts

Afrikaans	German	Serbian
Chinese (Simplified)	Korean	Turkmen
Chinese (Traditional)	Kurdish	UK English
Croatian	Latvian	US English
Czech	Lithuanian	Uyghur
Danish	Macedonian	Ukrainian
Dutch	Norwegian	Urdu
Estonian	Persian	Uzbek
Faeroese	Polish	Vietnamese
Finnish	Portuguese	
French	Romanian	
Georgian	Russian	

Note: System Name limitations

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.

To configure a system name:

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

RealPresence Group System Software Options

Some of the features of a RealPresence Group system are optional. To activate some features, you must purchase and install a key code.

To view system options:

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

The following options are displayed. Activated options have checkmarks next to them.

- **Telepresence Interoperability Protocol (TIP)**: This option improves the interoperability of systems in environments with certain Cisco telepresence systems. For more information, refer to Configure SIP Settings for Integration with the Telepresence Interoperability Protocol (TIP).
- **Video 1080p**: This option makes 1080p video and content available to RealPresence Group systems.
- **Dual display**: This option enables a second monitor display. Available for RealPresence Group 300 and 310 systems. The other systems support dual monitors without a license key.
- **Skype for Business Interoperability License**: This option enhances the video experience by enabling the following Microsoft features for all RealPresence Group systems:
  - Real-time video (RTV) provides higher resolutions during video calls when integrated with Skype for Business Server 2015 or Microsoft Lync Server 2013.
  - The Microsoft version of H.264 SVC delivers a continuous presence style experience.
  - Simulcast H.264 streams are now supported, allowing RealPresence Group systems in SVC-enabled Lync calls to transmit multiple streams of the local video depending upon the capabilities of the far-end systems. For example, far-end systems displaying high resolution

images receive high resolution images from the RealPresence Group system, while simultaneously far-end systems displaying low resolution images receive low resolution images from the RealPresence Group system.

- Centralized Conferencing Control Protocol (CCCP) enables seamless participation in multipoint video conferences hosted on Lync's audio/video server.
- Microsoft Lync AVMCU Spotlight feature enables the system to display only the broadcaster's video when a participant is made the broadcaster in a call.
- RealPresence Group systems support Forward Error Correction (FEC) DV0 and DV1 in Lync 2013, Skype for Business Server 2015, and Skype for Business 2015 client environments for both H.264 SVC and RTV endpoints. The scheme introduces recovery packets on the transmitter which recover lost video packets on the receiver. Enabling or disabling the Lost Packet Recovery feature in the web interface does not affect the negotiation of FEC.
- IPv6 is supported in Lync 2013, Skype for Business Server 2015, and Skype for Business 2015 client environments with IPv6 networks.

To activate system options:

1. In the web interface, go to **Admin Settings > General Settings > Options**.
2. Click **Launch Polycom Support to Get a Key Code**.
3. Register for an account, or log in to Polycom Support with your email address and password.

   After you successfully log in, your request is sent to an account representative.
4. When you receive your new key code, enter it at **Key** and click **Save**.

For information about integrating with Skype for Business Server 2015 or Microsoft Lync Server 2013, refer to the *Polycom Unified Communications Deployment Guide for Microsoft Environments* at support.polycom.com.

Customize the Local Interface Home Screen

Use the Polycom RealPresence Group system web interface to configure how information is displayed on the Home screen of the local interface.

Note: Home screen when paired
Home screen customizations have no effect when the RealPresence Group system is paired with a Polycom Touch Control.

To configure the Home screen using the web interface:

1. In your web browser address line, enter the RealPresence Group system's IP address.
2. Go to **Admin Settings > General Settings > Home Screen Settings**.
3. Configure the settings on the Home Screen Settings page that are described in the following sections.

Display Speed Dial Entries

You use speed dialing to quickly call an IP address designated as a Favorite.

Notes: Speed dial entries when paired

Speed dial entries do not appear when the Polycom RealPresence Group system is paired with a Polycom Touch Control.

To enable speed dialing in the web interface:

1. Go to **Admin Settings > General Settings > Home Screen Settings > Speed Dial**.
2. Click the **Choose Favorites** link to create and select the favorites you want to designate as speed dial entries.
3. Select the **Enable Speed Dial** setting and click **Save**.

To place a call within your company's telephone system, enter the internal extension instead of the full number.

For more information about calling, adding, or removing speed dial entries, refer to Speed Dial.

Display a Calendar

If your RealPresence Group system is configured to connect to the Microsoft Exchange Server, you can view scheduled meetings on the Home screen. If no meetings appear, either the system is not connected to the Microsoft Exchange Server or no meetings are scheduled.

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

Change the Background Image

The RealPresence Group system local interface displays a default background image that's similar to the "wallpaper" of a computer. You cannot delete this image, but you can upload your own image to replace it.

The pixel size of the image you upload must be 1920 x 1080 and the image format must be JPEG.

To upload and use a background image:

1. In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > 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** to display the image as your background.

Kiosk Mode

Kiosk Mode simplifies the Home screen of the local interface by displaying only speed dial entries and calendar meetings (if enabled). For information on enabling Kiosk Mode, see Place Calls in Kiosk Mode.

Configure Home Screen Icons

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

Icon	Name
	Menu
	Content This icon appears only when a content source is detected.
	Settings This icon takes you to the Setting screen, where you find System Information, Administration, and, if enabled, User Settings.
	Place a Call

Enable Access to User Settings

User settings allow users to control some aspects of cameras and meetings, for example, allowing other people in a call to control your camera or whether to enable auto answer for point-to-point or multipoint calls.

To enable access to User settings:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Security > Settings**.
   - In the 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, making them available only through the web interface.

To prevent users from using User Settings or Administration Settings in the local interface:

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

Note: Showing icons locally

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.**

Display System Information on the Local Interface

The RealPresence Group system local interface displays an address bar at the bottom of the Home screen. In addition to displaying certain system information on the local interface Menu, you now have the ability to display the system's IP address, extension, and SIP address in the address bar.

To display system information in the address bar:

1. In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > Address Bar**.
2. Configure the following settings.

Setting	Description
Show IP address on the home screen	Displays the IP address from **Admin Settings > Network > LAN Properties > IP Address (IPv4)** on the left side of the address bar.
Show Extension on the home screen	Displays the H.323 Extension from **Admin Settings > Network > IP Network > H.323** in the center of the address bar.
Show SIP address on the home screen	Displays the SIP address from **Admin Settings > Network > IP Network > SIP** (the **Sign-in Address**) on the right side of the address bar. **Note:** The **Show SIP address** setting displays only if your system is configured with a SIP address.

Configure Menu Settings

The menu settings in the web interface determine some of the information that is displayed in the local interface main menu. The menu settings are pulled from the system's network settings. For more information about network settings, refer to Networks.

To configure local interface menu settings:

1. In the web interface, go to **Admin Settings > General Settings > Menu Settings**.
2. Configure these settings, then click **Save**.

Setting	Description
Show System Information	Specifies whether to show certain system information in the local interface menu.
Display	Specifies whether to display the following information: • The system's **SIP Address** • The system's **IP Address** • The **Extension** associated with the system **Note:** The **SIP Address** setting displays only if your system is configured with a SIP address.

Setting	Description
Show System Button	Specifies whether to show a **System** button in the menu. **Note:** The **System** button in the local interface main menu is not the same as the **System** link in the blue bar at the top of the web interface page.
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 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.

Networks

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

The topics in this section cover network types used worldwide, but note that not all network types are available in all countries. To get started configuring your network, see the following topics:

- Connect to the LAN
- Configure IP Settings
- Set SVC Call Preferences
- Set Preferred Speeds
- Configure Native Support for RealConnect

Connect to the LAN

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

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

LAN Status Lights

The LAN connector on the RealPresence Group 300, 310, 500, and 700 systems has two lights to indicate connection status and traffic.

Indicator Light	Connection Status
Left light off	No 1000Base-T connection.
Left light green	1000Base-T connection.
Right light off	No 10/100 Base-T connection and no network traffic with 1000 Base-T connection.
Right light on	10/100 Base-T connection and blinks with network traffic.
Right light blinking	Network traffic.

Configure LAN Properties

You can configure LAN properties for the RealPresence Group systems and for Polycom Touch Control devices. Refer to the following section and Configure the Polycom Touch Control LAN Properties.

To configure RealPresence Group System LAN properties:

» Do one of the following:

- In the local interface, go to **Settings > Administration > LAN Properties**.
- In the web interface, go to **Admin Settings > Network > LAN Properties**.

Configure IP Address (IPv4) Settings

Configure the following IP Address (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

Configure the following IP Address (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.
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.

Setting	Description
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 Servers Settings

Configure the following DNS Servers settings on the LAN Properties screen.

Setting	Description
DNS Servers (in the local interface **DNS** and 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.
Server 1 Address **Server 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.

Configure LAN Options Settings

Configure the following LAN Options settings on the LAN Properties screen. In the web interface, these settings are displayed within LAN Options, but in the local interface they are arranged differently.

Setting	Description
Host Name (web interface only)	Indicates the system's name. On IPv4 networks the system will send the host name to the DHCP server in order to enable it to register the hostname with the local DNS server and/or look up the domain where the endpoint is registered (if supported). This function is not supported on IPv6, so you can leave this field unconfigured if you're using an IPv6 network. However, configuring the field to contain the registered host name is recommended.
Domain Name (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.

Setting	Description
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 (web interface only)	Enables the RealPresence Group system to ignore ICMP redirect messages. You should enable this setting under most circumstances.
ICMP Transmission Rate Limit (millisec) (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 (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 (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 RealPresence Group system.
IPv6 DAD Transmit Count (web interface only)	Specifies the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The RealPresence Group 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	This setting appears only for RealPresence Group 700 systems. 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 local interface)	Specifies whether Link Layer Discovery Protocol (LLDP) is enabled.
Enable EAP/802.1X (under EAP 802.1X in local interface)	Specifies whether EAP/802.1X network access is enabled. RealPresence Group systems support the following authentication protocols: • EAP-MD5 • EAP-PEAPv0 (MSCHAPv2) • EAP-TTLS • EAP-TLS

Setting	Description
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.
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: • H.323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for RealPresence Group 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.

Configure the Polycom Touch Control LAN Properties

Before you can use the Polycom Touch Control with the RealPresence Group system, you must configure the LAN settings.

To configure Polycom Touch Control LAN settings:

1. From the Home screen, touch  **Administration.**
2. Touch the **LAN Properties** tab.
3. Configure the following **IP Address (IPv4)** settings.

Setting	Description
Set IP Address	Specifies how the Touch Control obtains an IP address. • **Obtain IP address automatically**—Select if the Touch Control gets an IP address from the DHCP server on the LAN. • **Enter IP address manually**—Select if the IP address is not automatically assigned.
IP Address	Displays the IP address currently assigned to the Touch Control, if the Touch Control obtains its IP address automatically. If you selected **Enter IP address manually**, enter the IP address here.
Subnet Mask	Displays the subnet mask currently assigned to the Touch Control. If you selected **Enter IP address manually**, enter the subnet mask here.
Default Gateway	Displays the gateway currently assigned to the Touch Control. If you selected **Enter IP address manually**, enter the gateway IP address here.

4 Configure the following **DNS** settings.

Setting	Description
Domain Name	Displays the domain name currently assigned to the Touch Control. If the Touch Control does not automatically obtain a domain name, enter one here.
DNS Servers	Displays the DNS servers currently assigned to the Touch Control. If the Touch Control does not automatically obtain a DNS server address, enter up to two DNS servers here. You can specify IPv4 DNS server addresses only when the IPv4 address is entered manually. When the IPv4 address is obtained automatically, the DNS Server addresses are also obtained automatically.

5 Optionally, view the general settings.

Setting	Description
Duplex Mode	Displays the duplex mode.
LAN Speed	Displays the LAN speed.

LLDP and LLDP-MED Support

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) are supported on RealPresence Group Series 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.

LLDP-MED Information Discovery

In this implementation, LLDP-MED enables the following information discovery:

- 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 Group system, it discovers VLANs advertised by the network switch and automatically configures the system for one of the VLANs. If the RealPresence Group 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 RealPresence Group Series 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 RealPresence Group Series system presence on the network.

Enable LLDP

To enable LLDP on your RealPresence Group system, you have the choice of enabling it before the setup wizard process, using a USB storage device, or after the setup wizard in the web or the local interface.

Enable LLDP Using a USB Storage Device

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

To use a USB storage device to enable LLDP:

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 RealPresence Group system is powered off.
4. Insert the USB storage device into the RealPresence Group system USB drive.
5. Power on the RealPresence Group system.

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

Enable LLDP in the Web Interface After the Setup Wizard Process

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

To enable LLDP in the web interface:

» In the web interface, go to **Admin Settings > Network > LAN Properties**. Select the check box at **Enable LLDP** and click **Save**.

Enable LLDP in the Local Interface After the Setup Wizard Process

If you have already gone through the setup wizard and do not want to reset your RealPresence Group system to run the setup wizard again, you can configure LLDP in the local interface.

To enable LLDP in the local interface:

In the local interface, go to **Settings > Administration > LAN Properties**. Select the **Enable LLDP** check box.

Configure IP Settings

You can configure IP network settings only through the web interface by going to **Admin Settings > Network > IP Network.**

Network Quality Settings

Use this group of settings to specify how your RealPresence Group system responds to quality issues.

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.
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.

H.323 Settings

If your network uses a gatekeeper, the 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.

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.

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 users to make calls using static aliases instead of IP addresses that can change each day.

To configure the system to use a gatekeeper:

1. In the 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 option 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.
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.

Setting	Description
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 RealPresence Group system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the RealPresence Group system unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper.

Note: No multipoint on Group 300 and 310 systems
Polycom RealPresence Group 300 and 310 systems cannot be enabled for multipoint calling.

SIP Settings

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

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 *Release Notes for Polycom RealPresence Group Systems*.

To specify SIP settings:

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

Setting	Description
Enable SIP	Allows the SIP settings to be displayed and configured.
Enable AS-SIP	Enables the RealPresence Group system to apply the settings configured for assured services SIP.

Setting	Description
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.
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure your RealPresence Group System operates within determines which protocol is required. **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 Real Presence Group Series system to use an ephemeral source port for all outgoing SIP messages. When enabled, it causes the Real Presence Group 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.
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 RealPresence Group 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**.

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

Configure SIP Settings for Integration with Microsoft Servers

Integration with Microsoft servers allows Skype for Business 2015, Lync 2013, and Polycom RealPresence Group system users to place audio and video calls to each other.

Note: Presence server limit

Because Polycom RealPresence Group systems run in dynamic management mode, they cannot be simultaneously registered with Skype for Business Server 2015/Microsoft Lync Server 2013 and the presence service provided by the Polycom RealPresence Resource Manager system. RealPresence Group systems can obtain presence services from only one source: Skype for Business Server 2015, Lync Server 2013, or the presence service provided by the RealPresence Resource Manager system.

Polycom supports the following features in Skype for Business 2015 and Microsoft Lync Server 2013:

- Interactive Connectivity Establishment (ICE)
- Centralized Conferencing Control Protocol (CCCP); this feature is available only with the optional Skype for Business Interoperability License key
- Federated presence
- The Microsoft real-time video (RTV) codec; this feature is available only with the optional Skype for Business Interoperability License key

For more information about this and other Microsoft interoperability considerations, refer to *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

If your organization deploys multiple Skype for Business Server 2015 or Microsoft Lync Server 2013 pools, a Polycom RealPresence Group system must be registered to the same pool to which the system's user account is assigned.

Note: Microsoft integration requires Professional Services

Assistance from Polycom Microsoft Integration Services is mandatory for Skype for Business 2015 or Microsoft Lync Server 2013 integrations. For additional information and details, please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Configure SIP Settings for Integration with the Telepresence Interoperability Protocol (TIP)

When SIP is enabled on a RealPresence Group system that has the TIP option, the system can interoperate with TIP endpoints. However, there are some limitations:

- Polycom RealPresence Group systems cannot host multipoint calls while in a SIP (TIP) call.
- SIP (TIP) calls must connect at a call speed of 1 Mbps or higher.
- Only TIP version 7 is supported.
- In a TIP call, only XGA content at 5 fps is supported.

For more information about Polycom support for the TIP protocol, refer to *Polycom Unified Communications Deployment Guide for Cisco Environments* at support.polycom.com.

Note: TIP option key code

You cannot configure TIP without purchasing and installing a Telepresence Interoperability Protocol (TIP) option key code.

RTV and Lync-Hosted Conference Support

To use RTV in a Lync-hosted conference, you must have the Skype for Business Interoperability License key enabled on your RealPresence Group system.

For more information about configuring your Skype for Business Server 2015 or Lync Server 2013 video settings for RTV, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

AS-SIP Settings

RealPresence Group systems support the Assured Services Session Initiation Protocol (AS-SIP), as defined by the Unified Capabilities Requirements (UCR) technical standards for telecommunication switching equipment developed by the DoD and Defense Information Systems Agency (DISA). AS-SIP is the term used to describe the DoD version of SIP used as part of its initiative to build a reliable and secure IP communications network. AS-SIP incorporates Multilevel Precedence and Preemption, Secure Signaling and Media, Quality of Service (QoS), and IPv6 support.

Configure AS-SIP Settings

The AS-SIP settings define service codes, network domains, and precedence levels for MLPP.

To enable AS-SIP on your system:

1. In the web interface, go to **Admin Settings > Network > IP Network > SIP**.
2. Select the **Enable AS-SIP** setting.

To configure your AS-SIP settings:

1. In the web interface, go to **Admin Settings > Network > IP Network > AS-SIP**.
2. Configure these settings.

Setting	Description
Service Code	Defines one or more of the US Federal Communications Commission (FCC) N11 special services dialing codes or worldwide special dialing codes.
Outbound Precedence Call Defaults	Defines the **Default Domain** (network domain) and the **Default Precedence** level used when dialing a call.
MLPP Network Domains	Defines the MLPP network domains your network uses.

To add a service code:

1. To add a **Service Code**, click  .
2. In the text field of the new line that appears, enter the numbers.
3. Click another line in the list to create the service code.

To delete any service code, click  .

To define outbound precedence call defaults:

1. Select the **Default Domain** to use for outbound calls, that is, the default network domain. RealPresence Group systems come preconfigured for use on the `uc` and `dsn` network domains, but you can add others. You can choose any defined network domain as the default domain to use for outbound calls. `uc` and `dsn` are the preconfigured network domains and `uc` is the default network domain for this setting.
2. Select the **Default Precedence** to use for outbound calls.
   This setting accepts one of the defined precedence levels from the configured default domain. The setting defaults to `ROUTINE`, which is the lowest precedence level defined in the default network domain `uc`.

Although `uc` and `dsn` are preconfigured on the system, you can edit their settings or create other network domains.

To define MLPP network domains:

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**.

To add a network domain, click and then configure the same settings defined above for the new network domain. Click **Save** when you are finished.

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. 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.

RealPresence Group 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

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.

Notes: AS-SIP restrictions

Consider the following restrictions when you enable AS-SIP on a RealPresence Group system:

- 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 Group endpoint by going to **Admin Settings > Network > Dialing Preferences > Dialing Options** and disabling the **TIP** setting. TIP signaling is incompatible with AS-SIP signaling.

Network Quality

Set the Network Quality options for the way your network handles IP packets during video calls.

To configure quality of service settings:

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

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 page of the 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: • **H.323**—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for RealPresence Group 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.

Setting	Description
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.
Enable Lost Packet Recovery	Allows the system to use LPR (Lost Packet Recovery) if packet loss occurs.
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. For more information on SVC, see Set SVC Call Preferences.
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).
Note: When a RealPresence Group 500 or RealPresence Group 700 system is hosting a multipoint call, the total call rate for all sites in the call is 6 Mbps.	

Lost Packet Recovery and Dynamic Bandwidth

You can handle video quality issues by selecting 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 % Packet Loss, Video Rate, and Video Rate Used on the Call Statistics screen.

Configure the System for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with H.323 video conferencing equipment, you must configure the system and the firewall to allow video conferencing traffic to pass in and out of the network.

Network Address Translation (NAT) network environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices on the LAN to communicate with other devices outside the LAN. If your system is connected to a LAN that uses a NAT, you will need to enter the **NAT Public (WAN) Address** so that your system can communicate outside the LAN.

To set up the system to work with a firewall or NAT:

1. In the web interface, go to **Admin Settings > Network > IP Network > Firewall.**
2. Configure these 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 RealPresence Group 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 RealPresence Group systems support ICE, the range of fixed UDP ports is 112. The RealPresence Group 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, 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. For more information, refer to H.460 NAT Firewall Traversal.
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**.

Setting	Description
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 RealPresence Group 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 administrators 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.

Caution: Firewalls are recommended

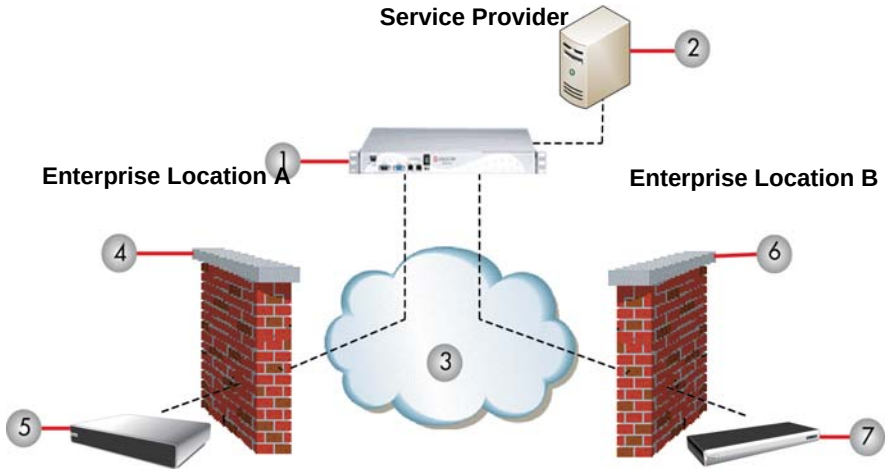
Systems deployed outside a firewall are potentially vulnerable to unauthorized access. Visit the Polycom Security section of the Knowledge Base at support.polycom.com for timely security information. You can also register to receive periodic email updates and advisories.

H.460 NAT Firewall Traversal

You can configure RealPresence Group 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 RealPresence Group systems behind different firewalls.

Example of Service Provider Firewall Traversal



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

To use this traversal, configure the RealPresence Group systems and firewalls as follows:

1. Enable firewall traversal on the RealPresence Group system.
   a. In the web interface, go to **Admin Settings > Network > IP Network > Firewall**.
   b. Select **Enable H.460 Firewall Traversal**.
2. Register the RealPresence Group system to an external Polycom VBP device that supports the H.460.18 and H.460.19 standards.
3. Make sure that firewalls being traversed allow RealPresence Group systems behind them to open outbound TCP and UDP connections.
   - Firewalls with a stricter rule set should allow RealPresence Group 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.

Basic Firewall/NAT Traversal Connectivity

Basic Firewall/NAT Traversal Connectivity allows RealPresence Group systems to connect to the SIP-based RealPresence solutions using the Acme Packet Net-Net family of Session Border Controllers (SBC). A RealPresence Group 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*.

RealPresence Group systems now 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.

Set SVC Call Preferences

Scalable Video Coding (SVC) conferencing provides several benefits, including fewer video resource requirements, better error resiliency, lower latency, and more flexibility with display layouts.

You can make and receive SVC multipoint calls when the Polycom RealPresence Group system is connected to an SVC-compatible bridge through the RealPresence 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 RealPresence Group system must be registered to a Lync 2013 or Skype for Business 2015 server. In a Microsoft Lync 2013 or Skype for Business 2015 hosted multipoint or point-to-point call, you can view multiple far-end sites in layouts. RealPresence Group 500 and 700 systems display up to five far-end sites on Lync 2013 or Skype for Business 2015 hosted (SVC), multipoint calls.

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 support.polycom.com.

For information on enabling encryption for SVC calls, refer to Configure Encryption Settings for SVC Calls.

Enable SVC Dialing Options

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

To configure dialing options:

1. In the 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 option disables SVC. This setting is not applicable to Lync-hosted calls, since SVC is negotiated automatically by Lync 2013, Skype for Business Server 2015, or Skype for Business 2015 client.
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far -end sites you call.
Enable Audio Add In	Specifies one additional outbound audio-only call from the RealPresence Group 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.

Enable Automatic Answering of SVC Point-to-Point Calls

A RealPresence Group system registered to a Lync 2013 or Skype for Business 2015 server and connected to an SVC-compatible bridge can automatically answer incoming SVC calls. To enable this feature, complete two tasks on a RealPresence Group system:

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

To enable Auto Answer Point-to-Point Video:

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

To enable Scalable Video Coding Preference (H.264):

1. In the 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**.

Set Preferred Speeds

To configure call speeds:

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

Setting	Description
Preferred Speed for Placed Calls IP Calls SIP (TIP) Calls	Determines the speeds to use for IP or SIP (TIP) 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. Users cannot specify a call speed when placing calls from the Polycom Touch Control. The **SIP (TIP) Calls** setting is available only when the **TIP** setting is enabled.
Maximum Speed for Received Calls IP Calls SIP (TIP) Calls	Allows you to restrict the bandwidth used when receiving IP or SIP (TIP) 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. The **SIP (TIP) Calls** setting is available only when the **TIP** setting is enabled.

Note: Point-to-point call bandwidth limits
For point-to-point calls, the Polycom RealPresence Group 300 and 310 systems use a maximum of 3 Mbps of bandwidth, and the RealPresence Group 500 systems use a maximum of 6 Mbps.

Configure Native Support for RealConnect

With the Native Support for RealConnect, Microsoft Lync and traditional video conference users do not have to change their workflow or learn a new process to join together in a video meeting.

Native Support for RealConnect eliminates end user frustration in trying to determine how to connect with people who might have varying devices. Integration between the RealPresence Group Series, Polycom DMA, Polycom RealPresence Collaboration Server (RMX), and Microsoft 2013 infrastructure automatically connects all of the environments together. This feature makes it easy for Lync and traditional videoconferencing system users to click to join calls from a Lync meeting invitation.

Set Up and Configuration

For Native Support for RealConnect to work with RealPresence Group Series systems, administrators must perform certain set up and configuration tasks.

Video Conference Administration

Perform the following tasks.

- IP H.323 must be enabled and registered to a gatekeeper. For information on enabling H.323 settings and registering to a gatekeeper, refer to H.323 Settings.
- The RealPresence Group Series system must be registered to a Lync SIP server so that a call can revert to Lync. For information on setting up a Skype for Business Server 2015 or Lync SIP server, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.
- The Polycom RealPresence Access Director must be set up to direct traffic to and from Polycom DMA. For configuration information, refer to the topic “Enable RealPresence DMA System for Lync 2013 or Skype for Business and Polycom RealConnect” in the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.
- The administrator must make a one-time change to the Lync meeting configuration policy so that RealPresence Group Series users can click **Join** on their system calendar and automatically join meetings. For details on editing the meeting configuration policy, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

Limitations

- In an ad hoc call, when a point-to-point call adds another endpoint, the conference might revert back to Skype for Business Server 2015 or Microsoft Lync Server 2013 and the ad hoc conference is not able to use SmartCascading functionality. However, it will still function like a Skype for Business Server 2015/Microsoft Lync Server 2013 call.
- Call participants cannot use their personal VMR ID. Instead, you must use an ID generated by the Skype/Lync meeting invite.
- The RealPresence Collaboration Server (RMX) sends the active speaker that has joined on the conference to the Skype for Business Server 2015 or Microsoft Lync Server 2013, so the Skype/Lync server displays only the active speaker.

Microsoft Lync

For Lync setup and configuration information, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

Polycom DMA

On Polycom DMA, the administrator must have set up the RealConnect policy for a single dialstring plan. In addition, RealPresence Access Director must be set up to direct traffic to and from Polycom DMA. For DMA setup and configuration information for this feature, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

Monitors and Cameras

These topics detail high-definition video conferencing, how to set up monitors and cameras with your system, and how to record calls:

Experience High-Definition Video Conferencing

Polycom RealPresence Group 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

Send Video in High Definition

Polycom RealPresence Group systems with HD capability can send video in wide-screen, HD format. For information about frame rates for content, refer to Content.

To send video in HD format, use any model of Polycom camera that supports HD video and a Polycom RealPresence Group system capable of sending 720p or better video.

Receive and Display Video in High Definition

When the far site sends HD video, Polycom RealPresence Group systems with HD capability and an HD monitor can display the video in wide-screen, HD format. The HD 720 format supported by these systems is 1280 x 720, progressive scan format (720p). Polycom RealPresence Group 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 RealPresence Group system or a conferencing platform that supports HD such as Polycom RealPresence Collaboration Server 1500 or 2000.
- The RealPresence Group system host must have the appropriate options 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, as shown in Multipoint Resolutions for High Definition Video.
- The call cannot be cascaded.

For more information about multipoint calls, refer to Multipoint Call Speeds.

Use Full-Motion HD

With RealPresence Group Series systems, Polycom sets a higher bar for video and audio performance. Seeing participants in full 1080p 60 fps, or full-motion HD, brings video to a new level of realism. Full-motion HD provides those clear, vibrant visuals and flawless audio that are critical to replicating an “in the same room” experience.

In group collaboration, the quality of content is as important as the quality of the people on video. Content that is grainy, pixelated, or slow to update makes it hard to get the most out of your meetings. With Polycom RealPresence Group systems, you share full-motion HD people and content at the same time, which helps eliminate compromises when sharing across distances.

Configure Monitor Settings

Note: Power off system before connecting devices

Make sure that the RealPresence Group system is powered off before you connect devices.

Configure Monitor Settings

The RealPresence Group system constantly detects any monitors connected to it. You choose which monitors with the **Enable** setting. You can also add a Monitor Profile to manage a group of monitor settings.

For more information about connecting monitors to RealPresence Group systems, refer to System Back Panel Views.

To configure monitors:

1. In the web interface, go to **Admin Settings > Audio/Video > Monitors.**
2. Configure these settings on the Monitors page. The settings for Monitor 1, Monitor 2, and Monitor 3 are the same, although the available options can be different.

Setting	Description
Enable	Specifies the monitor setting: • **Auto**–This is the default setting. Specifies that the **Video Format** and **Resolution** settings are automatically detected and disables those settings. • **Manual**–Enables you to select the **Video Format** and **Resolution** settings. **Resolution** settings are filtered based on the **Video Format** you selected. • **Off**–Disable this monitor.
Monitor Profile	Specifies which profile to use for this monitor. The choices depend on how many monitors the system uses and which monitor you are configuring.
Video Format	Specifies the monitor's format. Depending on which RealPresence Group System and monitor you configure, the choices are: • **HDMI** • **DVI** • **Component** • **VGA** **Note:** This setting is unavailable when you select **Auto** for the **Enable** setting.
Resolution	Specifies the resolution for the monitor. **Note:** This setting is unavailable when you select **Auto** for the **Enable** setting.

Monitor Profiles

Monitor Profiles set the preferences for what is shown on available monitors. Configuring this setting allows you to customize the monitor configuration to match your environment or your desired meeting experience.

The Monitor Profiles settings are just preferences. What you see can vary depending on layout views, whether content is being shown, the number of active monitors, and so on.

The following table describes the configuration of each monitor profile.

Setting	Description
Decide for Me	Default setting that sets monitors to show content and the current speakers based on a variety of factors. When you select **Decide for Me**, the settings for Monitor 2 and Monitor 3 are unavailable. If you later choose a different setting, the original values persist. **Note**: When Decide for Me is enabled, content is normally sent to Monitor 2.
Me Only (Monitor 2 or Monitor 3)	Sets the monitor to always show you.
Speaker Only	Sets the monitor to show current people speaking at the far-end on Monitor 1. Monitor 2 shows only one person.
Content Only (Monitor 2 or Monitor 3)	Sets the monitor to show available content. Otherwise, the monitor shows the room background.
Speaker and Content	Sets the monitor to show available content. Otherwise, the monitor shows the person speaking at the far-end. You can browse layouts with this setting.

Setting	Description
Recording Device with Speaker and Content (Monitor 3 only)	Sets the monitor to show available content or the person speaking to support recording with a DVR. The showing of content takes priority over the showing of a person speaking. This setting is available only with RealPresence Group 700 systems. Select this setting to record near, far, and content audio. If there is content, the video is recorded in full screen. If there is no content, the speaker is recorded in full screen.
Recording Device with Speaker Only (Monitor 3 only)	Sets the monitor to show the current person speaking, regardless of the speaker's location, to support recording with a DVR. This setting is available only with RealPresence Group 700 systems. Select this setting to record near, far, and content audio. Only the speaker is recorded in full screen.

The Automatic Self View setting can also affect what displays on the monitors. For more information, refer to Configure Menu Settings.

Record and Live Stream Calls

To record calls, you can either remotely log in to the Polycom® RealPresence® Media Suite or use the RealPresence Group 700 system on Monitor 3.

Polycom® RealPresence® Media Suite Recording

Polycom® RealPresence Media Suite is an enterprise recording, streaming and video content management solution that offers users, and administrators, self-service user portal features to record calls on Group Series, or turn any Group Series into a webcast studio. Using RealPresence® Media Suite, one or all of your Group Series systems, can be configured to perform as a webcasting studio for your organization.

From RealPresence Media Suite's User Portal, any user from your organization can click to start recording, click to create a live stream events, and share their video files. The Polycom® RealPresence Media Suite is also a streaming and recording system that participates in standards-based video and telepresence calls.

RealPresence Media Suite integrates with RealPresence Group systems to allow you to record, and/or live stream a call using the following methods:

- **Dial a RealPresence Group system from a RealPresence Media Suite portal**: If you have access to a RealPresence Media Suite portal, you can log in to the portal to dial in to a RealPresence Group system from which you want to record a call. This method is ideal for an administrator of a remote RealPresence Group 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 of the RealPresence Group systems local interface can also record in these ways:

- **Dial RealPresence Media Suite directly**: Use the default recording settings defined by a RealPresence Media Suite administrator. Before recoding 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.

For more information on recording with these two methods, refer to the *Polycom RealPresence Group Series User Guide*.

Note: Share a Recording With Others

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 *Polycom RealPresence Media Suite User Guide* at support.polycom.com.

RealPresence Media Suite Connection Methods

The following connection methods are supported for dialing a RealPresence Media Suite.

Media Suite Type	Connection Method	Example
Media Suite system	If the RealPresence Group system is not registered to the gatekeeper or to a SIP server, dial the RealPresence Media Suite IP address.	10.11.12.13
	If the RealPresence Group system is registered to the gatekeeper, dial the RealPresence Media Suite E.164 extension for H.323.	1234
	If the RealPresence Group system is registered to a SIP server, dial the RealPresence Media Suite SIP address.	CS123
VRR	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**.
	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 **4096@11.12.13.14**. If the SIP peer prefix of the RealPresence Media Suite is 8888 and the VRR number is 4096, dial **88884096**.

Enable Recording on a RealPresence Group 700 System

You can use a RealPresence Group 700 system to record the audio and video of a call on Monitor 3.

To enable and disable recording:

1. In the web interface, select **Admin Settings > Audio/Video > Monitors**.
2. Select one of the following settings for Monitor 3:
   - **Recording Device with Speaker and Content**. Select this setting to record what the speaker says, along with any content audio.
   - **Recording Device with Speaker Only**. Select this setting to record only what the speaker says.

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, you should 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 could have a better experience if you turn it on.

Finally, before attaching your Polycom RealPresence Group 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.

Use Sleep Settings to Prevent Monitor Burn-In

Monitors and Polycom RealPresence Group 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.

Set Up CEC Monitor Controls

Consumer Electronics Control (CEC) monitor controls enable the following features on RealPresence Group systems connected to any HDMI monitors that support the CEC protocol:

- **One Touch Play**–Use the RealPresence Group Series remote to wake up the monitors. All connected CEC-capable monitors are powered on, and their displays are switched to RealPresence Group Series input.
- **System Standby**–When the RealPresence Group 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 RealPresence Group system video.

Note the following points about using CEC controls with RealPresence Group 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 will power up but might not switch to the correct input when waking up.
- The RealPresence Group system does not respond to CEC commands issued by a television remote control.
- If a CEC-capable monitor is connected to a RealPresence Group system and another endpoint, the monitor displays the active endpoint when the RealPresence Group system is in standby mode.

Enable Monitors

All connected monitors must support CEC, so that the feature can operate with RealPresence Group systems. 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.

Note: Enable all CEC monitors connected

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

Enable or Disable CEC on the RealPresence Group System

CEC functionality is enabled by default on RealPresence Group systems.

To enable or disable the CEC controls:

1. In the web interface, go to **Admin Settings > Audio/Video > Monitors > Consumer Electronics Control**.
2. Select the **Enable Consumer Electronics Control** box to enable CEC. Clear the box to disable CEC.

Note: HDMI channel identification

On the HDMI channel, the RealPresence Group Series system is identified as **Polycom**.

Polycom Cameras

Polycom RealPresence Group 700 systems provide inputs for multiple PTZ cameras. RealPresence Group 310 and 500 systems can support a second non-PTZ camera, but do not support camera control for a second camera.

All Polycom cameras are capable of receiving IR signals.

Polycom RealPresence Group systems have built-in IR receivers to receive signals from the remote control. Be sure to point the remote control at the RealPresence Group system or your Polycom camera to control it.

Polycom EagleEye IV

The Polycom EagleEye IV cameras are completely digital with a 4k sensor that is specifically designed to work with the RealPresence Group Series. They support 1080p60 resolution and are available with either 12x or 4x zoom capabilities.

Polycom EagleEye IV

These cameras also have an available privacy cover, wide-angle lens, and digital extender. For more information, 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 support.polycom.com.

Polycom EagleEye III

The Polycom EagleEye™ III camera can provide 1080i 60/50 fps, 1080p 60 fps, and 720p 60/50 fps resolutions on all Polycom RealPresence Group systems.

Polycom EagleEye III

Polycom EagleEye Acoustic

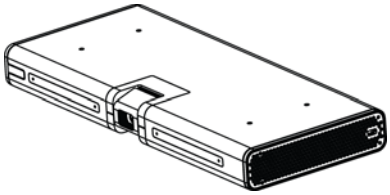
The Polycom EagleEye Acoustic camera can provide 1080p 25/30 fps resolution with embedded image sensor processing (ISP) technology and has an auto focus lens system, two microphones for stereo audio pickup, an IR detector, a status LED, and a captured HDCI cord for connection to the system.

Polycom EagleEye Acoustic

Polycom EagleEye Producer

Polycom EagleEye Producer is a camera peripheral technology that works with Polycom EagleEye III and EagleEye IV cameras to provide room framing and participant counting.

Polycom EagleEye Producer



Polycom EagleEye Director

The Polycom EagleEye Director is a high-end automatic camera positioning system that works in conjunction with a Polycom RealPresence Group system to provide accurate close-up views of the person who is speaking. The EagleEye Director also provides smooth transitions between the close-up view of the person who is speaking and the room view.

Note: EagleEye Director camera compatibility
The EagleEye Director is only compatible with EagleEye III cameras.

Polycom EagleEye Director

The EagleEye Director uses a dual-camera system. 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. By providing automatic and intelligent views in various speaking scenarios during a conference, the EagleEye Director delivers a user experience similar to a newscast video production.

Polycom EagleEye II

The Polycom EagleEye II camera can provide 1080i 60/50 fps for Polycom RealPresence Group systems.

Polycom EagleEye II

Polycom EagleEye HD

You can use the Polycom EagleEye HD camera with all Polycom RealPresence Group systems. Polycom EagleEye HD cameras provide 720p resolution.

Polycom EagleEye HD

Polycom EagleEye 1080

You can use the Polycom EagleEye 1080 camera for RealPresence Group systems with the 1080p Resolution option installed to send 1080p video. You can also use the Polycom EagleEye 1080 camera with systems that do not have the 1080p Resolution option, to see local video in 1080 format.

Polycom EagleEye 1080

Note: Use supplied cables to connect

When connecting a Polycom EagleEye 1080 camera to any input on a Polycom RealPresence Group system, use the cable and power supply that arrived with the camera. You must always use the power supply because the Polycom EagleEye 1080 camera does not receive power from the RealPresence Group system.

Polycom EagleEye View

The Polycom EagleEye View camera is a manual-focus, electronic pan, tilt, and zoom (EPTZ) camera that includes built-in stereo microphones and a privacy shutter. The Polycom EagleEye View camera is available with the Polycom RealPresence Group systems as the system camera and the main microphone. For more

information about the Polycom EagleEye View microphones, refer to Polycom EagleEye View and EagleEye Acoustic Microphones.

You can install the Polycom EagleEye View in a base-down orientation or inverted. To change the camera's orientation after installation, disconnect all cables attached to the camera. Then install the camera with the preferred orientation and reconnect the camera.

Polycom EagleEye View

Note: Cable for audio

When connecting a Polycom EagleEye View camera, use the cable with the brown connector that arrived with the camera if you want to use the camera's built-in microphones. Other cables do not carry the audio signals.

The Polycom EagleEye View camera can provide 1080i video to RealPresence Group systems.

Connect Cameras to RealPresence Group Systems

Refer to your system setup sheet and to the *Polycom RealPresence Group Series Integrator Reference Guide* for connection details. Refer to the release notes for a list of supported PTZ cameras. If you connect a supported PTZ camera, the system detects the camera type and sets the appropriate configuration. Make sure that the system is powered off before you connect devices to it.

Note: One EagleEye Director per system

Do not connect more than one Polycom EagleEye Director to a single RealPresence Group system.

Power Cameras with RealPresence Group Systems

The RealPresence Group systems 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. However, the RealPresence Group 700 system supports a low-power standard that limits the power supplied to the camera when the system is powered off. So, if the camera is receiving its power only from the HDCI connector attached to the system, it does not have an active IR receiver capable of powering on the RealPresence Group system using the handheld remote.

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

- Provide direct power to the EagleEye III or EagleEye IV camera with the optional 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 RealPresence Group 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 RealPresence Group system.

Note: Waking a sleeping camera
When you use a RealPresence Group system to provide power to an EagleEye III or EagleEye IV camera, you can wake a sleeping camera by sending a signal to the camera's IR sensor with the remote control

Configure Video Input Settings

Refer to System Back Panel Views for an illustrated view of the inputs and outputs available for each RealPresence Group 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 will be able to set up the camera the same as a supported camera.

To configure camera and video settings in the web interface:

» Go to **Admin Settings >Audio/Video > Video Inputs**.

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 option 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 which is 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.

Setting	Description
Enable People+Content™ IP	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 RealPresence Group 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 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.

Configure Video Input Settings

Configure the following settings for each video input connected to your RealPresence Group system.

Note: Only applicable settings display

Settings that don't apply to the selected video input are not displayed. For example, if an EagleEye Producer is not connected to your RealPresence Group system, the related settings are not displayed.

Setting	Description
Enable	Specifies the video input type. You can also choose to **Auto** select the video input type. For RealPresence Group 300, RealPresence Group 310, and RealPresence Group 500 systems, Input 1 is always HDCI, so you will not see an **Enable** setting here. **Note:** RealPresence Group 300 systems have only one video input. RealPresence Group 310 systems and RealPresence Group 500 systems have two video inputs, but only HDMI and VGA are allowed for the second input.
Model	Displays the type of device using the video input port.
Name	Displays the default name of the video input, but you can enter your own name for the device.
Display as	Specifies whether the video input is to be used for **People** or **Content**. The selection you make here 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.

Setting	Description
Orientation	Specifies the orientation of the camera. You can choose one of the following camera positions: • **Normal**— This default setting is a non-inverted camera orientation. • **Inverted**—This is an upside-down camera orientation. **Note**: This setting is available only when you have installed an EagleEye IV camera. To learn how to enable the setting, refer to EagleEye IV Camera Orientation.
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.
Tracking Mode (EagleEye Director)	Specifies the type of camera tracking: • **Voice**—Tracks the speaker. When another speaker starts talking, the view switches from the first speaker to the room, then to the next speaker. • **Direct Cut**—Tracks directly from speaker to speaker if silence intervals are less than 3 seconds. You must recalibrate the left camera when you select Direct Cut mode. If camera tracking has not been calibrated, Tracking Mode is unavailable. **Note:** This setting is available only when you have installed an EagleEye Director.
Tracking Speed (EagleEye Director)	Determines how quickly the system finds someone new and switches to that person. **Note:** This setting is available only when you have installed an EagleEye Director.
Backlight Compensation	Specifies whether to have the camera automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background. Enabling this setting helps to relieve a bright background, which can impact the tracking performance of the Polycom EagleEye Director.
White Balance	Specifies how the camera compensates for variations in room light sources. Select **Auto**, **Manual**, or a color temperature value. The color temperature values, measured in degrees Kelvin, correspond to the color of ambient light in a room. Because the available color temperature values vary by camera, this list is only a sampling of some of the values you might see in the interface: • **3200 K** (tungsten bulb) • **3680 K** (warm office fluorescent) • **4160 K** (cool office fluorescent) • **5120 K** (neutral daylight) • **5600 K** (cool daylight)
Brightness	Provides a slider to adjust how bright the image is.
Color Saturation	Provides a slider to adjust how colorful the image is.

Setting	Description
Tracking Mode (EagleEye Producer)	Specifies the tracking mode: • **Group Framing** - This is the default setting. Enables automatic tracking and framing of the group of participants in the room. • **Off** - Disables automatic tracking. All camera control must be handled manually. **Note:** This setting is available only when you have installed an EagleEye Producer.
Tracking Speed (EagleEye Producer)	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. • **Note:** This setting is available only when you have installed an EagleEye Producer.
Group Framing (EagleEye Producer)	Specifies the group 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. EagleEye Producer can detect the position of a person within six meters or less. **Note:** This setting is available only when you have installed an EagleEye Producer.
Automatic Image Calibration	Specifies the EagleEye Producer to automatically calibrate its integrated camera and an attached EagleEye camera. This is important when the cameras are projecting images that are not aligned.

Configure a Third-Party Camera

The RealPresence Group Series systems support some third-party cameras. For a list of supported third-party cameras and their connectors, see the *Polycom RealPresence Group Series Integrator Reference Guide*.

If your camera has a breakout cable that allows the video to be connected to the HDCI port, you can use either of the following two ways to get the serial data to and from the camera:

1. Use the HDCI port:
   a. On the system's back panel, connect the camera to the HDCI video input port.
   b. In the web interface, go to **Admin Settings > Audio/Video > Video Inputs** and configure the settings.
2. Use the external serial port:
   a. On the system's back panel, connect the camera to the serial port.
   b. In the web interface, select **Admin Settings > General Settings > Serial Ports**.
   c. For the **RS-232 Mode** setting, select **Camera Control** to enable the external serial port.
   d. Configure the **Serial Port Options**. Use the following settings:

Setting	Value
Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1
RS-232 Flow Control	None

You can use the external serial port with any one of the following video inputs:

RealPresence Group System	Video Input 1	Video Input 2	Video Input 3	Video Input 4
RealPresence Group 300 System	Yes	N/A	N/A	N/A
RealPresence Group 310 System	Yes	Yes	N/A	N/A
RealPresence Group 500 System	Yes	Yes	N/A	N/A
RealPresence Group 700 System	Yes	Yes	Yes	Yes

Note: Usage of serial ports

Some cameras come with a breakout cable that allows you to use the camera with the HDCI serial port. If you use the HDCI serial port, the cable has embedded serial capabilities, so you can use either method mentioned in this section to connect the camera. However, if you connect a camera to a Composite or HDMI port on the RealPresence Group system, you must control the camera through the external serial port.

Configure the EagleEye IV Camera

After you have connected your EagleEye IV camera, you might want to change certain settings in the web interface.

EagleEye IV Camera 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 Inverted Camera Position

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

To enable the inverted mount camera position:

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

Enable Normal Camera Position

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

To disable the inverted mount camera position:

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

For other EagleEye IV video input setting details, refer to Configure Video Input Settings.

Set Up the EagleEye Producer

Information on required cables and how to set up EagleEye Producer are included in *Set Up the Polycom EagleEye Producer.* Additional information is available in the *Polycom RealPresence Group Series Integrator Reference Manual*. Both documents are located at support.polycom.com.

Note: Connect only one EagleEye Producer to a RealPresence Group system

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

Update EagleEye Producer with RealPresence Group Series

Updates to Polycom EagleEye Producer software are included with the RealPresence Group system software updates. To update your EagleEye Producer, connect it to the RealPresence Group system before you run a software update. The software update program detects the EagleEye Producer and updates it if necessary. No license number or key code is needed to update the EagleEye Producer.

Note: EagleEye IV camera software automatic updates

The software for an EagleEye IV camera can now be updated when the camera is attached to a RealPresence Group system with an EagleEye Producer. This feature is automatic and does not require any configuration or intervention.

EagleEye Producer must run a software version that is compatible with the software version on the RealPresence Group system. For more information, go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html and click the **Current Interoperability Matrix** link.

Change Camera Tracking Settings

The Polycom EagleEye Producer detects the people in the room and provides room framing during a conference. Group framing, with a Normal tracking speed and Medium view, is enabled by default You can change the camera tracking settings, as described below.

Note: Calibrate EagleEye Producer before adjusting the camera

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 EagleEye Producer User Guide* at support.polycom.com.

To change camera tracking settings:

1. Do one of the following:
   - In the local interface of the RealPresence Group Series system, go to **Settings > Administration > Camera Tracking > Settings**.
   - In the web interface of the RealPresence Group Series system, go to **Admin Settings > Audio/Video > Video Inputs> Settings** and select the input used by the Polycom EagleEye Producer.
2. Configure the following settings.

Setting	Description
Tracking Mode	Specifies the tracking mode: • **Group Framing** - This is the default setting. Enables automatic tracking and framing of the group of participants in the room. • **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.
Group Framing	Specifies the group 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.

Stop and Start Camera Tracking

Camera tracking starts automatically when you start a call and enables group framing. You can also manually enable or disable camera tracking in the local interface.

To enable camera tracking:

» In the local interface of the RealPresence Group system, go to **Menu > Cameras** and select **Start Camera Tracking**.

To disable camera tracking:

» In the local interface of the RealPresence Group system, go to **Menu > Cameras** and select **Stop Camera Tracking**.

Note: Camera tracking and group framing stop when call ends

After a call ends, camera tracking stops automatically and group framing is disabled.

EagleEye Producer Auto Calibration

You can configure the EagleEye Producer to automatically calibrate its integrated camera and an attached EagleEye IV camera. This is important when the cameras are projecting images that are not aligned.

To enable auto calibration:

1. Attach the EagleEye camera to the EagleEye Producer, as shown in *Setting Up the Polycom EagleEye Producer*.
2. Ensure that camera tracking is enabled, as described in Stop and Start Camera Tracking.

   In the web interface, go to **Admin Settings > Audio/Video > Video Inputs > Input [`input number`]**, and select the **Automatic Image Calibration** checkbox.

View System Status

To view the system status of an EagleEye Producer, do one of the following:

- In the local interface of the RealPresence Group Series system, go to **Settings> System Information> Status**.
- In the web interface of the RealPresence Group Series system, go to **Diagnostics > System > System Status**.

If a Polycom EagleEye Producer is connected, the connection status displays. If the camera is not connected or is not selected as the current camera source, this choice is not visible on the screen.

To view more information about Polycom EagleEye Producer, select **More Info**.

For more information about using EagleEye Producer, refer to the *Polycom EagleEye Producer User Guide* on support.polycom.com.

Configure the Polycom EagleEye Director

Use the remote control or web interface to configure the Polycom EagleEye Director. You cannot configure the EagleEye Director using the Polycom Touch Control, but you can start and stop camera tracking.

For setup instructions, refer to *Setting up the Polycom EagleEye Director* on support.polycom.com.

After setting up the EagleEye Director, follow these steps to get started:

1. Power on the EagleEye Director.

   You can verify that the device is detected and compatible with the RealPresence Group system's software on the System Status page. Do one of the following:

   - In the local interface, go to **Settings > System Information > Status > EagleEye Director**.
   - In the web interface, go to **Diagnostics > System > System Status > EagleEye Director**.

   As long as you see **EagleEye Director** among the status settings, the device has been detected.
2. Calibrate the cameras. Refer to Calibrate the EagleEye Director Cameras for instructions. 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. Refer to Adjust the Room View for instructions.

Notes: Troubleshoot EagleEye Director 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.
- Restart the RealPresence Group system.
- Manually power off the EagleEye Director by unplugging its power supply and unplugging the HDCI cable from the RealPresence Group system. Then power on the EagleEye Director, plug the HDCI cable into the RealPresence Group system, and attempt camera detection again.

Calibrate the EagleEye Director Cameras

In Voice Tracking mode, you only need to calibrate the right camera. In Direct Cut mode, calibrate the right camera and then left one.

To calibrate the cameras:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Camera Tracking** > **Calibration**.
   - In the web interface, go to **Admin Settings** > **Audio/Video > Video Inputs** and select **Calibrate Voice Tracking**.
2. Follow the directions in the Auto Calibration page that appears. When you click **Start**, auto-calibration begins. When the automatic process ends, you have these choices:
   - **Yes, I see a green box around my mouth.** Selecting this choice means auto-calibration was successful and you can move forward with adjusting the room view, if you like.
   - **No, I see a green box, but it is not around my mouth.** Selecting this choice means you can try auto-calibration again or manually calibrate the camera.
   - **No, I do not see a box at all.** Selecting this choice means you must manually calibrate the camera.
3. If necessary, follow these steps to manually calibrate the camera:
   a. Use the arrow buttons and zoom controls on the remote control or web interface to zoom completely in, then aim the camera at your mouth.
   b. Select **Begin Calibration** or **Start** and follow the onscreen instructions until a message displays indicating successful calibration.

Note: Calibration tips

Ensure that only one person speaks while you are calibrating the cameras and keep the background quiet.

If you rearrange or move the Polycom EagleEye Director, recalibrate it.

If you cannot successfully calibrate the cameras, 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. For ways to test microphone functionality, refer to the **Camera Tracking** settings in Diagnostics, Status, and Utilities.

Adjust the Room View

1. Do one of the following:
   - From the local interface, go to **Settings > Administration** > **Camera Tracking** > **Calibration**, and then select **Begin Calibration**.
   - From the web interface, go to **Admin Settings** > **Audio/Video > Video Inputs**, and then select the **Input** used by the Polycom EagleEye Director.
2. Do one of the following:
   - In the local interface, select **Skip** to move to the Adjust Room View screen.
   - In the web interface, select **Adjust Room View**.
3. Use the arrow buttons and zoom controls on the remote control or 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 and Disable Camera Tracking with EagleEye Director

If EagleEye Director tracking is enabled, the camera follows the person or people who are speaking. This tracking action, also called automatic camera positioning, can be manually started or stopped.

To enable camera tracking:

» 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. For ways to test microphone functionality, refer to the **Camera Tracking** settings in Diagnostics, Status, and Utilities.
- In the web interface, go to **Admin Settings** > **Audio/Video > Video Inputs**, and then select the **Input** used by the Polycom EagleEye Director.
  - Enable the **Use Voices to Track People** setting.
- If the RealPresence Group system is paired with a Polycom Touch Control, follow these steps:
  1. 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.**

To disable camera tracking:

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

To 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**, as needed.

Camera tracking can also start or stop 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 Group 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.

Note: Room lighting and 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 web interface, go to **Admin Settings > Audio/Video > Video Inputs** and select the appropriate **Input**. For more hints on setting up the EagleEye Director, see Position the Polycom EagleEye Director.

Enable Camera Presets

Camera presets are stored camera positions that you can create in the 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 the Polycom Touch Control. Each preset stores the camera number, its zoom level, and the direction it points (if appropriate).

If far-end camera control (FECC, which, for RealPresence Group systems, is the **Allow Other Participants in a Call to Control Your Camera** setting under **Admin Settings > Audio/Video > Video Inputs > General Camera Settings**) is allowed, you can create 10 presets for the far-site camera. These presets are saved only for the duration of the call. You might also be able to use presets that were created at the far site to control the far-site camera.

If a Polycom Touch Control is paired with a Polycom RealPresence Group system, you must use the Polycom Touch Control to create presets. For more information about creating and using presets, refer to the *Polycom RealPresence Group Series User Guide* and the *Polycom RealPresence Group Series and the*

Polycom Touch Control User Guide. Once presets are in place, you can view them in the web interface by going to **Utilities > Tools > Remote Monitoring**.

Note: Voice tracking preset limitation
If you use a Polycom EagleEye Director with your RealPresence Group system, you cannot use presets for voice tracking.

Microphones and Speakers

To receive and send audio, you must connect and configure both microphones and speakers. This section contains placement information for various audio inputs and speakers. It also covers audio settings available from the web interface.

- Available Microphone Inputs by System
- Audio Input Tips by Microphone Type
- Audio Input Configuration Options
- Audio Output
- Configure Audio Settings
- Audio Meters
- Test StereoSurround

For specific details regarding how to connect audio inputs and speakers, refer to the appropriate RealPresence Group system setup sheet and System Back Panel Views. For information about required cables, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.

Available Microphone Inputs by System

The number of audio inputs varies based on the RealPresence Group system you are using.

As shown in the following figures, the RealPresence Group 300, RealPresence Group 310, and RealPresence Group 500 systems have one microphone input, while the RealPresence Group 700 system has two. You can freely configure the way you connect devices to a system, as long as you do not exceed the limits mentioned in the following sections. If you are using the RealPresence Group 700 system, you can connect devices to either or both inputs as long as you stay within the guidelines for the total number of devices allowed for the system.

RealPresence Group 300, 310, and 500 microphone inputs

RealPresence Group 700 microphone inputs

Audio Input Tips by Microphone Type

Make sure that the RealPresence Group system is powered off before you connect audio devices to it.

Polycom RealPresence Group System Table or Ceiling Microphone Arrays

Polycom microphone arrays contain three microphone elements for 360° coverage. You can connect multiple Polycom microphone arrays to a RealPresence Group system.

For the best audio experience, do the following:

- Place the microphone array on a hard, flat surface (table, wall, or ceiling) away from obstructions, so the sound will be directed into the microphone elements properly.
- Place the microphone array near the people closest to the monitor.
- In large conference rooms, consider using more than one microphone array. Each Polycom microphone array covers a 3-6 foot radius, depending on the noise level and acoustics in the room.

The following table describes the behavior of the microphone lights on a Polycom table microphone.

Microphone Light	Status
Off	Not in a call
Green	In a call, mute off
Red	Mute on
Blinking Red	Configuration error occurred, such as exceeding the number of supported conference link devices
Amber	Firmware upload

Polycom EagleEye View and EagleEye Acoustic Microphones

Polycom EagleEye™ View and EagleEye Acoustic cameras include built-in stereo microphones. The following tips can help you achieve the best audio when using these cameras:

- Enable Polycom StereoSurround.
- Place the camera at least 1 foot away from any walls to minimize boundary effects.
- Ensure that the people speaking are no more than 7 feet away from the EagleEye View or EagleEye Acoustic camera. The maximum distance covered depends on the noise level and acoustics in the room. If you connect a Polycom microphone, Polycom SoundStation® conference phone, or Polycom SoundStructure® to the RealPresence Group system microphone input while an EagleEye View or EagleEye Acoustic camera is connected to the system, the camera's built-in microphones are automatically disabled.
- Polycom recommends connecting other audio input devices in conference rooms larger than 12 feet by 15 feet.

Polycom SoundStation IP 7000 Conference Phone

When you connect a Polycom SoundStation IP 7000 conference phone to a Polycom RealPresence Group system, the conference phone becomes another way to dial audio or video calls. The conference phone also operates as a microphone, and as a speaker in audio-only calls. For more information, refer to the following documents at support.polycom.com:

- *Polycom SoundStation IP 7000 Conference Phone Connected to a Polycom RealPresence Group System in Unsupported VoIP Environments Integration Guide*
- *Polycom SoundStation IP 7000 Conference Phone Connected to a Polycom RealPresence Group System in Unsupported VoIP Environments User Guide*

Audio Input Configuration Options

You can use a variety of audio inputs with your RealPresence Group system. See the following sections to determine what audio inputs work with your system. For tips specific to the type of audio input you use, refer to Audio Input Settings.

Microphone Input Options for RealPresence Group 300/310

RealPresence Group 300 and RealPresence Group 310 systems can support any of the following devices:

- Two RealPresence Group microphone arrays or two Polycom HDX microphone arrays
- One SoundStation IP 7000 conference phone and one RealPresence Group or Polycom HDX microphone array
- One SoundStructure C-Series device and up to four RealPresence Group or Polycom HDX microphone arrays
- Polycom EagleEye View or EagleEye Acoustic with microphones enabled

Microphone Input Options for RealPresence Group 500/700

RealPresence Group 500 and RealPresence Group 700 systems can support any of the following devices:

- Four Polycom RealPresence Group microphone arrays or three Polycom HDX microphone arrays
- One SoundStation IP 7000 conference phone and two RealPresence Group or Polycom HDX microphone arrays
- One SoundStructure C-Series device and up to four RealPresence Group or Polycom HDX microphone arrays
- Polycom EagleEye View or EagleEye Acoustic with microphones enabled

Non-Polycom Microphones

You can connect non-Polycom microphones directly to audio input 1 on a Polycom RealPresence Group system, or through a line-level mixer to the AUX audio input on any Polycom RealPresence Group system. For more information about configuring these non-Polycom microphones, refer to Set Up Third-party Microphones.

SoundStructure Digital Mixer

You can connect several microphones to a Polycom RealPresence Group system through a Polycom audio mixer. Connecting a Polycom audio mixer to RealPresence Group systems provides flexibility in audio setup. The SoundStructure C-Series mixer connects to the digital microphone connector on a Polycom RealPresence Group system, and no configuration is necessary.

When incorporating a SoundStructure digital mixer, remember the following:

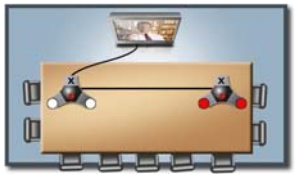
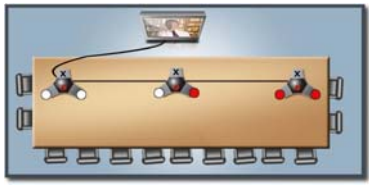
- Connect a SoundStructure digital mixer using the digital microphone input on the Polycom RealPresence Group system.

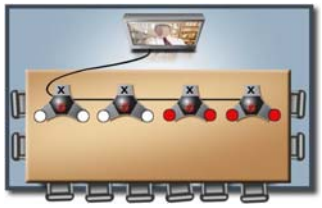
- Adjusting the volume on a Polycom RealPresence Group system changes the volume of the SoundStructure digital mixer that is connected.
- The following configuration settings are not available on a Polycom RealPresence Group system when a SoundStructure digital mixer is connected: Audio input 1 (Line In), Bass, Treble, Enable Polycom Microphones, Enable MusicMode™, and Enable Keyboard Noise Reduction.
- The Polycom RealPresence Group system Line Output is muted when a SoundStructure digital mixer is connected.
- All echo cancellation is performed by the SoundStructure digital mixer.

For example, it allows you to provide a microphone for each call participant in a boardroom. Refer to the *Polycom RealPresence Group Series Integrator Reference Guide* for connection details.

Polycom Microphone Placement to Send Stereo from Your Site

You can use up to 2 microphones with RealPresence Group 300 and 310 systems, and up to 4 microphones with the RealPresence 500 and 700 systems. The following illustrations show microphone placement examples for different room layouts.

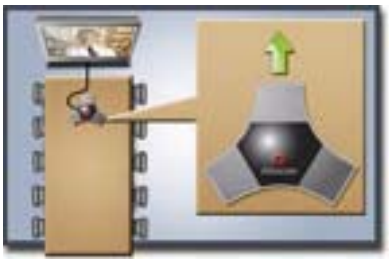
Number of Microphones with Stereo Enabled	Long Table	Wide Table
One	Mic 1 set to **Left+Right** 	Mic 1 set to **Left+Right** 
Two	Mic 1 set to **Left+Right** Mic 2 set to **Left+Right** 	Mic 1 set to **Left** Mic 2 set to **Right** 
Three	Mic 1 set to **Left+Right** Mic 2 set to **Left+Right** Mic 3 set to **Left+Right** 	Mic 1 set to **Left** Mic 2 set to **Left+Right** Mic 3 set to **Right** 

Number of Microphones with Stereo Enabled	Long Table	Wide Table
Four	Mic 1 set to Left+Right Mic 2 set to Left+Right Mic 3 set to Left+Right Mic 4 set to Left+Right 	Mic 1 set to Left Mic 2 set to Left Mic 3 set to Right Mic 4 set to Right 

× – Not Used
○ – Left Channel
● – Right

Left and right channel assignments depend on the settings that you select on the Stereo Settings screen. If Autorotation is enabled for a microphone, the system automatically assigns active channels for the microphone. Make sure that microphones with Autorotation disabled are oriented as shown in the following illustration.

Microphone placement



After you place the microphones, you will need to configure the system to send stereo as described in Stereo Settings.

Audio Output

You must connect at least one speaker to the Polycom RealPresence Group systems in order to hear audio. You can use the speakers built into the main monitor, or you can connect an external speaker system, such as the Polycom StereoSurround kit, to provide more volume and richer sound in large rooms.

When you connect a SoundStation IP 7000 conference phone to a Polycom RealPresence Group system, the conference phone becomes another way to dial audio or video calls. The conference phone also operates as a microphone, and as a speaker in audio-only calls.

Refer to your system setup sheet for connection details. Make sure that the system is powered off before you connect devices to it. For more information about connecting speakers to RealPresence Group systems, refer to System Back Panel Views.

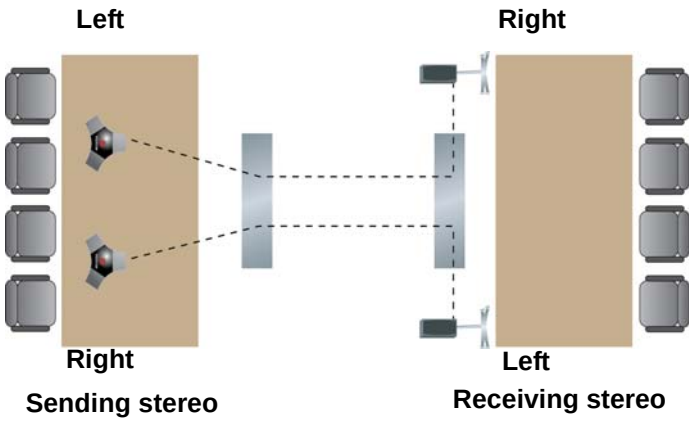
Speaker Placement to Receive Stereo from Far Sites

The Polycom StereoSurround kit is designed for use with Polycom RealPresence Group systems. It includes two speakers and a subwoofer.

When a RealPresence Group system is configured for Polycom StereoSurround, the audio inputs and outputs are all treated as stereo. Otherwise, all audio inputs and outputs are mono.

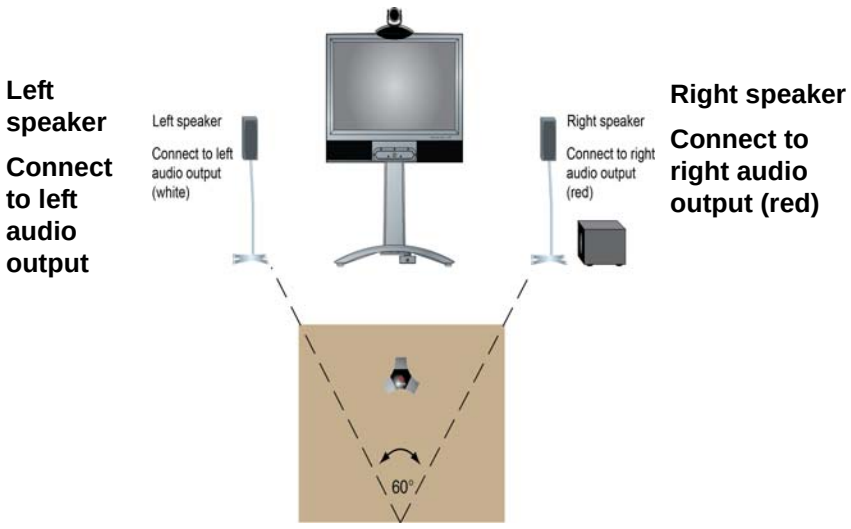
When you set up the system for StereoSurround, the left microphone and speaker should be on the left from the local room perspective. Place the speaker connected to the audio system's right channel on the right side of the system, and the other speaker on the left side. The system reverses the left and right channels for the far site, as shown in the following illustration. This ensures that the sound comes from the appropriate side of the room.

StereoSurround microphone and speaker placement



For best results, place the speakers about 60° apart as seen from the center of the conference table.

Speaker with subwoofer placement



Left speaker

Connect to left audio output

Right speaker

Connect to right audio output (red)

If you use the subwoofer in the Polycom StereoSurround kit, place it beside a wall or in a corner near the speakers.

Set the Speaker Volume

To set the volume of an external speaker system:

1. Do one of the following:
   - In the local interface, go to **Settings > System Information > Diagnostics > Speaker Test.**
   - In the web interface, go to **Diagnostics > Audio and Video Tests > Speaker Test**.
2. Click **Start** to start the speaker test.
3. Adjust the volume of the speaker system. From the center of the room the test tone should be as loud as a person speaking loudly, about 80-90 dBA on a sound pressure level meter.
4. Click **Stop** to stop the speaker test.

Configure Audio Settings

There are several types of audio settings to configure in the web interface. They include the following:

- General Audio Settings
- Audio Input Settings
- Audio Output Settings
- Stereo Settings

All of these setting types are located in the same area of the web interface.

To configure any audio settings:

1. In the web interface, go to **Admin Settings > Audio/Video > Audio.**
2. Configure the settings for each section of the Audio screen that are described in this section of the book.

Note: Audio settings with SoundStructure connected
Some audio settings are unavailable when a SoundStructure digital mixer is connected to the Polycom RealPresence Group system. For more information, refer to Audio Output.

General Audio Settings

The general audio settings allow you to specify various user tones, sound effect volume, and more.

General Audio Settings

Setting	Description
Polycom StereoSurround	Specifies that Polycom StereoSurround is used for all calls. To send or receive stereo audio, make sure your Polycom RealPresence Group system is set up as described in Available Microphone Inputs by System and Audio Output.
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.

Setting	Description
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**. For details on these settings, see Configure Call Settings.
Enable MusicMode	Specifies whether the system transmits audio using a configuration that best reproduces interactive and live performance music picked up by microphones. This mode provides the highest possible bandwidth for audio. When MusicMode is enabled, even the faintest musical notes come through clearly. **Note:** Automatic noise suppression and automatic gain control are disabled when MusicMode is enabled.
Enable Keyboard Noise Reduction and NoiseBlock™	Specifies whether the system mutes audio from the RealPresence Group Series 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:** MusicMode is disabled when this setting is enabled. If an external echo canceller is used, keyboard noise reduction is not available.
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 RealPresence Group system 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 is installed.
Enable Acoustic Fence	Specifies whether Acoustic Fence can be used or not. For details on Acoustic Fence, refer to Acoustic Fence Technology.
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.

Audio Input Settings

The RealPresence Group 300 system has no audio input settings, and the settings for the RealPresence Group 310, 500, and 700 systems are quite different. The following tables describe each.

RealPresence Group 310 and 500 Audio Input Settings

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.
Use Input for Microphone	Specifies use of the 3.5mm input. When enabled, this setting is used as an audio input for external equipment. The audio is only heard on the far-end sites. When the local mute is activated, this input is muted. When disabled, the port is used as an audio content port. The audio is heard by both the near and far-end sites and is not controlled by the local mute.
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.
Echo Canceller	Specifies whether to use the system's built-in echo canceller for that audio input. This setting is available only when the **Use Input for Microphone** setting is enabled.
Audio Meter (not labeled)	Displays the audio level for the 3.5 mm input port, left and right channels.
Type	Displays embedded audio from the HDMI connector.
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level for the HDMI input port, left and right channels.

RealPresence Group 700 Audio Input Settings

Setting	Description
Type	Displays **Line** (dual RCA, auxiliary audio input).
Audio Input Level	Sets the audio input level.
Echo Canceller	Specifies whether to use the system's built-in echo canceller for that audio input. This setting is available only when the **Use Input for Microphone** setting is enabled.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.
Type	Displays **3.5 mm** (line-level stereo audio input, associated with HD15/VGA video input 3).
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.

Setting	Description
Type	Displays **HDMI 1** (HDMI connector embedded audio input, associated with video input 1).
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.
Type	Displays **HDMI 2** (HDMI connector embedded audio input, associated with video input 2).
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.
Type	Displays **HDMI 3** (HDMI connector embedded audio input, associated with video input 3).
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.
Type	Displays **Component** (dual RCA, associated with component video input 4).
Audio Input Level	Sets the audio input level.
Audio Meter (not labeled)	Displays the audio level of the line input, left and right channels.

3.5mm Audio Input Selection

Administrators can now select in the RealPresence Group Series web interface how to enable 3.5mm audio input from the RealPresence Group Series 3.5mm audio port. On active calls, administrators can enable 3.5mm audio input on the near-end conference site.

When administrators enable audio 3.5mm input for use during active calls, 3.5mm audio input is heard during active calls from the RealPresence Group system speakers and from all far-end sites.

When administrators 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 when the RealPresence Group system is in an active call, 3.5mm audio input is heard from the RealPresence Group system speakers and from all far-end sites. When there is audio as part of active HDMI or VGA content, the 3.5mm audio input mixes in with the HDMI or VGA audio input.

Enable 3.5mm Audio Input

To enable 3.5mm audio input, you cannot use 3.5mm input as a microphone. Because of this, you must clear the **User Input for Microphone** checkbox, as shown in the tasks below.

To enable 3.5mm audio input:

1. In the web interface, go to **Admin Settings > Audio and Video > Audio Settings > Audio Input > 3.5mm Audio Input**.
2. Clear the **Use Input for Microphone** checkbox.

3 Clear the **Video Content Ports Association** checkbox.

3.5mm audio input is now enabled for use during active calls.

Enable 3.5mm Audio Input for Content Sharing

You can enable audio input for content sharing.

To enable 3.5mm audio input for content sharing:

1. In the web interface, go to **Admin Settings > Audio and Video > Audio Settings > Audio Input > 3.5mm Audio Input**.
2. Clear the **Use Input for Microphone** checkbox.
3. Select the **Video Content Ports Association** checkbox.
4. Click **Save**.

   3.5mm audio input is now enabled when content sharing is active in a call.

Audio Output Settings

After you configure the general audio and audio input settings, configure the audio output settings.

Audio Output Settings

Setting	Description
Master Audio Volume	Sets the main audio output volume level going to the speakers.
Bass	Sets the volume level for the low frequencies without changing the master audio volume.
Treble	Sets the volume level for the high frequencies without changing the master audio volume.
Type	Display the current audio output type.
Output Mode	Specifies whether volume for a device connected to the line out connectors is variable or fixed. • **Variable**—Allows users to set the volume with the remote control. • **Fixed**—Sets the volume to the Audio Level specified in the system interface.
Audio Output Level	Displays the output level meter for the current audio output type.

Stereo Settings

To send or receive stereo audio, make sure your Polycom RealPresence Group system equipment is set up as described in Available Microphone Inputs by System and Audio Output. Then configure the system to use Polycom StereoSurround, test the system configuration, and place a test call.

If you are in a call with a far site that is sending audio in stereo mode, you can receive in stereo. In multipoint calls where some sites can send and receive stereo and some sites cannot, any site that is set up to send or receive stereo will be able to do so.

Stereo Settings

Setting	Description
Polycom Microphone Type	Displays the type of Polycom microphone being used.
Stereo	Positions the audio input within the left and right channels. **Left** sends all of the audio to the left channel. **Right** sends all of the audio to the right channel. For Polycom digital microphone and ceiling microphone arrays, **Left+Right** sends audio from one microphone element to the left channel and audio from a second element to the right channel.
Autorotation	Specifies whether autorotation is used for Polycom microphones. If this feature is enabled, the system automatically assigns left and right channels for the microphone based on sound it senses from the left and right speakers. **Note:** This feature does not work when headphones are used.
Audio Meter (dB meter)	Lets you see the peak input signal level for Polycom microphones.

Audio Meters

The audio meters in the user interface allow you to identify left and right channels. The meters also indicate peak signal levels. Set signal levels so that you see peaks between +3 dB and +7 dB with normal speech and program material. 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.

Test StereoSurround

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

To test your stereo configuration:

1. Make sure the microphones are positioned correctly.

   Refer to Polycom Microphone Placement to Send Stereo from Your Site.
2. In the web interface, go to **Admin Settings > Audio/Video > Audio.**
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.

Set Up Third-party Microphones

You can configure a Polycom RealPresence Group system to use non-Polycom microphones.

To configure a Polycom RealPresence Group system to use devices connected directly to audio input 1:

1. In the web interface, go to **Admin Settings > Audio/Video > Audio > Audio Input.**
2. Do the following**:**
   a. Enable **Use Input for Microphone**.
   b. Enable **Echo Canceller**.
   c. Adjust the **Audio Input Level** if necessary.
   d. Speak into the microphones that are connected to the audio line inputs. The audio meter should peak at about 5 dB for normal speech.

Acoustic Fence Technology

RealPresence Group Series systems feature a technology that 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.

Note: Not Supported on RealPresence Group 300 or 310 systems
Acoustic Fence is not supported on RealPresence Group 300 or 310 systems.

In addition to the primary Polycom microphone array, one or more fence microphone arrays are required.You can use up to four microphones with RealPresence Group Series 500 and 700 systems. The boundary radius can be two feet to several feet around the following Polycom peripherals:

- Polycom microphone array
- Desktop microphones

- Ceiling microphones
- EagleEye View camera
- Polycom® EagleEye Acoustic camera

Note: Mono mode only is supported
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 web interface.

To configure the Acoustic Fence:

1. In the 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 sensitivity and 10 is the maximum sensitivity. Higher settings increase the radius of the fence area around the primary microphone.

For more details on the setup and the associated scenarios, refer to the Polycom Acoustic Fence white paper at www.polycom.com/videodocumentation.

Content

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 Polycom RealPresence Group system
- People+Content IP installed on a computer, with any Polycom RealPresence Group system
- A computer connected directly to a Polycom RealPresence Group system or a Polycom Touch Control
- A USB drive connected to a Polycom Touch Control

Polycom RealPresence Group 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.

To prepare for sharing content, see the following topics:

- Configure DVD Player Settings
- Connect Computers to Polycom RealPresence Group Systems
- Configure Content Sharing
- Microsoft Lync and Skype for Business Client 2015 Content Viewing
- Configure Content Display with People+Content IP
- Use the Polycom VisualBoard Application
- Configure the Polycom UC Board
- Configure Closed Captioning

For more information about sharing content during a call, refer to the *Polycom RealPresence Group Series User Guide*.

Configure DVD Player Settings

Whether you can play DVDs using your RealPresence Group system depends on the version you own:

- With a RealPresence Group 310 or a RealPresence Group 500 system, you can connect a DVD player to an HDMI or VGA input to play content.
- With a Polycom RealPresence Group 700 system, you can also connect a DVD player to the system's video input to play DVDs in calls.
- Using a DVD player with a RealPresence Group 300 system is not a viable option.

Play a Videotape or DVD

The 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.

To configure DVD audio settings for playing a DVD on a RealPresence Group 310, 500, and 700 system:

1. In the 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.

Connect Computers to Polycom RealPresence Group Systems

You can connect a computer directly to a RealPresence Group system. When you do this, other call participants can see everything that you see on your computer.

When you connect to video and audio from your computer, the audio is muted unless the computer is selected as a video source.

For more information about connecting computers as content video sources for RealPresence Group systems, refer to Configure Video Input Settings. Refer to your system setup sheet for connection details.

Configure Content Sharing

You can configure content sharing on the web interface.

Note: Recommended Monitor 2 output resolution settings

For content to display properly, the RealPresence Group system 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.

To configure the content display:

1. In the 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 showing content, refer to the *Polycom RealPresence Group Series User Guide*.

As long as the default values for other settings in the system have not changed, you are ready to share content on your RealPresence Group system. However, if you disabled the H.239 protocol for some reason, you must enable the program for content sharing by following these steps:

3 In the web interface, go to **Admin Settings > Network > Dialing Preference.**

4 Enable **H.239**.

If the audio level of the call using content sharing needs to be adjusted, follow these steps to change the level:

5 In the web interface, go to **Admin Settings > Audio/Video > Audio > Audio Input.**

6 Set the **Audio Input Level**.

Note: H.239 while in a call
You cannot enable or disable H.239 while in a call.

Microsoft Lync and Skype for Business Client 2015 Content Viewing

RealPresence Group systems can now view content from Microsoft Lync 2013 and Skype for Business 2015 remote desktop (RDP) clients in active calls. Microsoft clients must initiate the content sharing request.

For information on how to share content from Lync clients, refer to Microsoft documentation. RealPresence Group systems can view the following content types from Lync clients:

- **All Monitors** Displays content from all monitors connected to the system with the Lync client.
- **Primary Monitor** Displays content from the primary monitor connected to the system with the Lync client.
- **Secondary Monitor** Displays content from the secondary monitor connected to the system with the Lync client.
- **Program** Displays content from a particular program connected to the system with the Lync client.

There are a few limitations with Lync, as follows:

- RealPresence Group systems can view content from Lync clients, but are not able to share content with Lync clients.
- RealPresence Group systems cannot share content, including content shared though People+Content IP and through VisualBoard, while actively receiving content from Lync clients.
- RealPresence Group systems do not support viewing PowerPoint (Office Web App), Whiteboard, Poll, and Q & A content from Lync clients. In multipoint conferences with more than one Lync client, Lync clients can select these content sharing options, but RealPresence Group systems in the conference do not receive the content.

- For content to display properly, the RealPresence Group system Monitor 2 must support Progressive mode, and the output resolution should be set to a Progressive setting (for example, 1280x720p or 1920x1080p). Interlaced output for Monitor 2 is not supported (do not use Resolution setting -1920x1080i-).
- For Lync content viewing on RealPresence Group systems, Polycom recommends you deploy Lync Room System accounts instead of regular Lync user accounts for all room-based Group Series systems. By using these accounts, enterprises avoid sharing content within the same room which results in a audio echo. To deploy these accounts, refer to the *Microsoft Lync Room System Deployment Guide* on the Microsoft site.
- With this feature, users can scroll and zoom content on the RealPresence Group system monitor, and RealPresence Group systems can control content received from Lync clients. For details, see the *Polycom RealPresence Group Series User Guide*.

Note: Ending a Lync conference while RDP content is being shared ends all audio, video, and RDP content sessions

If a Lync client ends a call while sending RDP content, the video display appears frozen. Do one of the following:

- Ask the Lync client to stop presenting RDP content either before or after ending the call.
- Ask a Lync client in the AVMCU call to remove the Lync participant who is sending the RDP content from the call.

This issue can occur because RDP content is a separate session from the video call, so even when the video call has ended, the RDP content does not end until it is separately stopped or removed from the call.

Scroll and Zoom

After a Lync client shares content with a RealPresence Group system in an active call, and when a USB mouse is connected to the system, users can scroll and zoom on the RealPresence Group system monitor to see all the shared content.

To scroll and zoom:

1. Connect a USB mouse to the RealPresence Group system.
2. Move the mouse to scroll and zoom.

Control Lync Content

RealPresence Group systems can control content received from Lync clients, when Lync clients give control to a RealPresence Group system and when a USB mouse is connected to the system. Lync clients must select the specific RealPresence Group system they want to give control to. After a RealPresence Group system receives content from a Lync client in an active call and takes control of content received from the Lync client, the RealPresence Group system can open and use shared applications, programs, and files on the system with the Lync client using a connected USB mouse and keyboard.

Note: Normal Lync feature restrictions apply

Any normal Lync feature restrictions apply. For more information refer to Microsoft documentation. Password-enabled applications, programs, or files remain password enabled when using this feature.

To control content from a Lync endpoint:

1. Connect a USB mouse to the RealPresence Group system. If you want to use shared applications, programs, and files that require keyboard functions, connect a USB keyboard to the RealPresence Group system.
2. When a Lync user initiates sharing in an active call, the RealPresence Group system displays a notification. Select the **Control Remote** checkbox.

   The RealPresence Group system now controls the content received from the Lync client.

Return Control of Lync Content

You can return control of the Lync content at any time.

» To return control of the Lync content, use a USB mouse to clear the **Control Remote** checkbox.

- The Lync client now controls the shared content. The RealPresence Group system can still scroll and zoom to see all the shared content. To learn how to scroll and zoom, refer to Scroll and Zoom.

Note: Recommended Monitor 2 output resolution settings

For content to display properly, the RealPresence Group system 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.

For content to display properly, the RealPresence Group system Monitor 2 must support Progressive mode, and the output resolution should be set to a Progressive setting (for example, 1280x720p or 1920x1080p). Interlaced output for Monitor 2 is not supported (do not use Resolution setting -1920x1080i).

For details on configuring Lync Content Viewing, refer to *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

For details on how end users can control Lync content, and can scroll and zoom in Lync content, refer to the *Polycom RealPresence Group Series User Guide* at support.polycom.com.

Configure Content Display with People+Content IP

People+Content IP 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.

Before a presenter can use a computer to show content with People+Content IP, you need to 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 memory
    Recommended computer: 1 GHz Pentium III (or equivalent); 512 MB memory
- Connect the computer or computers to the IP network.

To install People+Content IP on a computer:

1. On a computer, open a web browser and go to the Polycom web site at www.polycom.com/ppcip.
2. Download and install the People+Content IP software.

Note: Touch Control installs People+Content IP

If the Polycom RealPresence Group system is paired with a Polycom Touch Control, People+Content IP does not need to be installed. If you connect the PC to the USB connection on the underside of the Polycom Touch Control, a version of People+Content IP launches automatically.

Use the Polycom VisualBoard Application

The Polycom VisualBoard™ application allows you to show and annotate content in real time from Polycom RealPresence Group systems by using an electronic annotation device such as a touch screen monitor. You can use the monitor as your only content monitor or you can use it in addition to your current content monitor.

When using a touch screen monitor, you can annotate the content using finger, a stylus, or a mouse. When using a standard monitor, you can use the UC Board device or a mouse to annotate. For flat, cold surfaces such as white boards with projectors, Polycom suggests using the Polycom UC Board with the VisualBoard application.

Requirements 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, UC Board hardware, or a supported touch monitor
- Connected at least one monitor for use with the RealPresence Group system (two monitors are also supported).
- Enabled the VisualBoard option on the RealPresence Group web interface

Note: USB storage devices cannot be daisy chained

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.

Enable the VisualBoard Application

To enable the VisualBoard application:

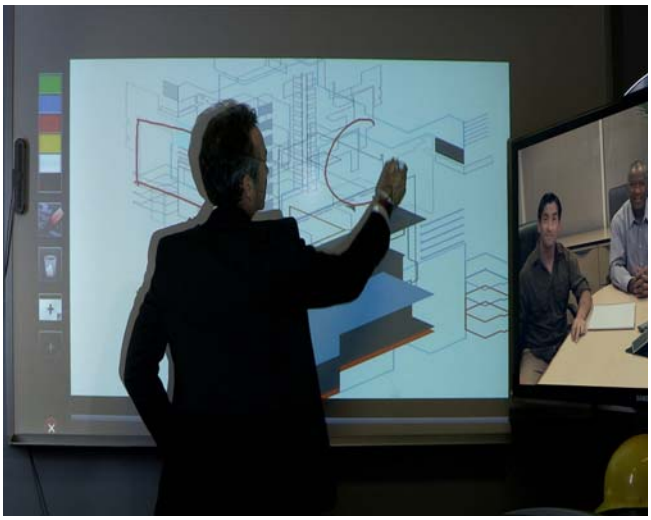
1. In the web interface, go to **Admin Settings > General Settings > System Settings > VisualBoard/RDP.**
2. Select **Enable** and click **Save**.

For more information about how to install and configure the VisualBoard application, as well as the list of supported touch screen monitors, refer to the *Polycom VisualBoard Technology Application with Polycom RealPresence Group Series User Guide* at support.polycom.com.

Configure the Polycom UC Board

With the Polycom UC Board, you can show and annotate content in real-time from Polycom RealPresence Group 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.

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.

To set up two monitors and configure to show content:

1. To configure monitor 1, go to **System > Admin Settings > Monitors**. On the monitor 1 screen, enable **Display Near Video** and **Display Far Video**.
2. To configure monitor 2:
   a. Advance to the Monitor 2 screen and set **Resolution** to either 720p or 1080p.
   b. Enable **Display Content** to show shared content and Polycom UC Board annotations.

To improve performance, configure your monitor or projector to use **Game Mode**, if that setting is available.

Here are a few installation tips:

- Polycom recommends LED backlit, LCD displays over 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 *Quick Start Guide for the Polycom UC Board*, available with the UC Board hardware and at support.polycom.com.

Configure Closed Captioning

You can provide real-time text transcriptions or language translations of the video conference by displaying closed captions on your 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 RealPresence Group systems with software version 4.1.3 or later, including a RealPresence Group 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.

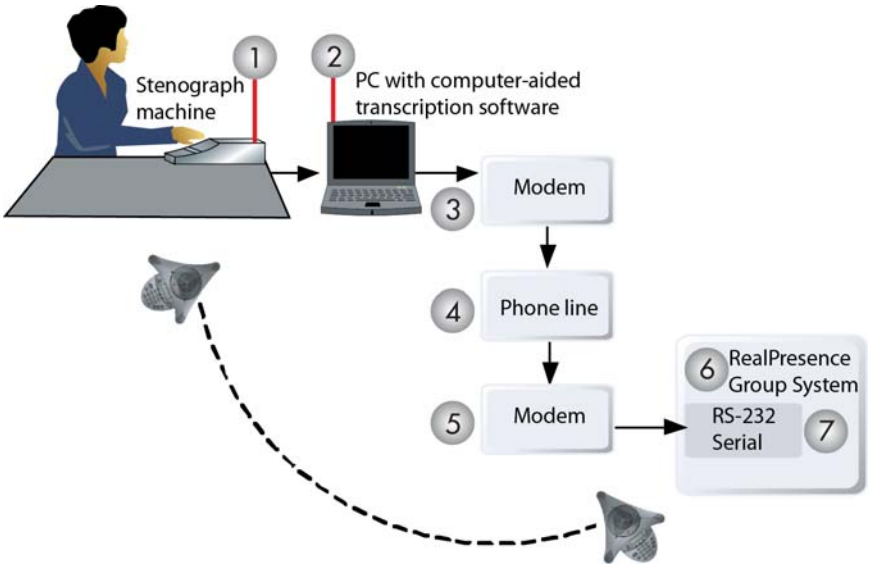
Depending on the capabilities of the system, the captioner may enter caption text using one of the following methods:

- 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 RealPresence Group system web interface

Through a 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 Polycom RealPresence Group system, as shown in the following diagram.

Closed captioning through a dial-up connection



Ref. Number	Description
1	Stenograph machine
2	PC with computer-aided transcription software

Ref. Number	Description
3	Modem
4	Phone line
5	Modem
6	RealPresence Group System
7	RS-232 serial port

To supply closed captions through a dial-up connection:

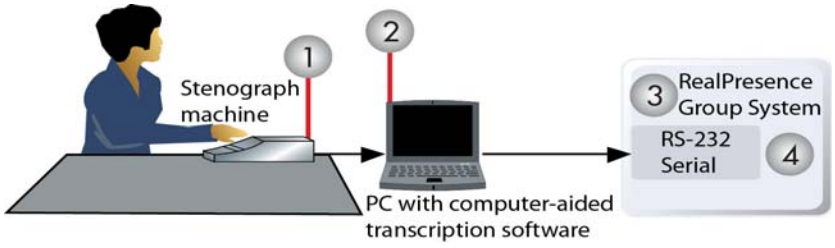
1. Ensure that the computer and the RealPresence Group system are configured to use the same baud rate and parity settings.
2. In the web interface, go to **Admin Settings > General Settings > Serial Ports.**
3. Set the RS-232 Mode to **Closed Caption**.
4. Establish a dial-up connection between the computer and the RealPresence Group 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.

Through the Serial RS-232 Port

Closed captioners can provide captions from inside the conference room, using equipment connected directly to the serial port of the Polycom RealPresence Group system, as shown in the following diagram.

Closed captioning through the system serial RS-232 port



Ref. Number	Description
1	Stenographer machine
2	PC with computer-aided transcription software
3	RealPresence Group System
4	RS-232 serial port

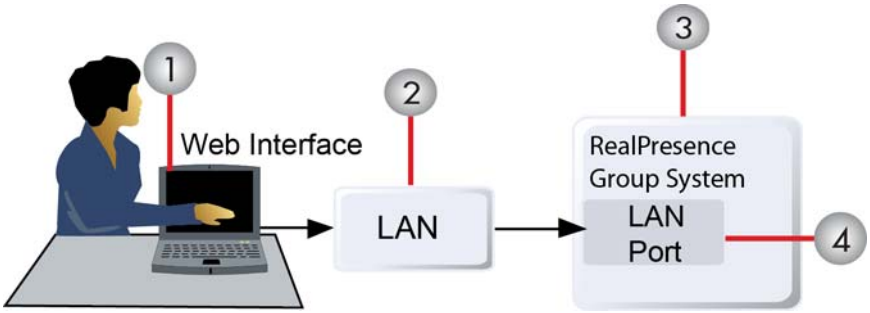
To supply closed captions using equipment connected directly to the serial port:

1. Ensure that the computer and the RealPresence Group system are configured to use the same baud rate and parity settings.
2. In the 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.

Through 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 Polycom RealPresence Group system web interface, as shown in the following diagram.

Closed captioning through the web interface



Ref. Number	Description
1	Web interface
2	LAN
3	RealPresence Group System
4	LAN port

To supply closed captions for a conference using the web interface:

1. In your web browser address line, enter the RealPresence Group system IP address.
2. Go to **Utilities > Tools > Closed Caption**.
3. Log in using this information if prompted:

   User Name: Your name.

   Password: Meeting password defined for your video conferencing system.
4. In the Closed Caption screen, type the caption text into the text field. Text wraps to the next line after 32 characters.
5. Press **Send** to send the text to the sites in the conference.

Place and Answer Calls

Before you start using the system, configure your system and call settings. System Settings screens provide access to high-level options for the entire system. For convenience, some of the User Settings options are repeated on these screens.

To get started with calling, see these topics:

- Configure Call Settings
- Multipoint Calling
- Manage Directories in the Web Interface
- Use the Web Interface Place a Call Page
- Stop and Start Camera Video in a Call
- Place Calls in Kiosk Mode

Configure Call Settings

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

To configure call settings:

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

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.
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 RealPresence Group system is the host of a multipoint call. The available settings are as follows: **Auto** **Full Screen** **Discussion** **Presentation** For detailed information on these settings, refer to Select a Multipoint Viewing Mode.
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.
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 RealPresence Group system.

Set the Call Answering Mode

You have several choices when it comes to how calls are answered.

To set the call answering mode:

1. In the 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 you to answer calls manually.
   - **Do Not Disturb**–Disables incoming calls from being processed.

Enable Flashing Incoming Call Alerts

For hearing-impaired users, an attention-getting message displays when an incoming call is received by a RealPresence Group 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.

If a RealPresence Group system is paired with a Polycom Touch Control and is configured with **Admin Settings > General Settings > System Settings > Call Settings > Auto Answer Point-to-Point** set to **Yes**, users do not see the flashing message on the RealPresence Group system or on the Touch Control screen. The call is answered automatically and users interact with the call on the Touch Control screen.

To turn on flashing alerts:

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

To turn off flashing alerts:

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

Multipoint Calling

You can use your Polycom RealPresence Group 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, Polycom RealPresence Group systems can host multipoint calls.

Note: Multipoint video conferencing option key code required
You cannot configure multipoint calls without purchasing and installing a Multipoint Video Conferencing option key code.

Enter a Multipoint Option Key

Depending on your Polycom RealPresence Group 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.

To enter the multipoint option key:

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

Note: RealPresence Group 300 and 310 do not support multipoint calling
The multipoint option key cannot be used with Polycom RealPresence Group 300 and 310 systems.

Select a Multipoint Viewing Mode

What the far-end site sees during a multipoint call can vary depending on how the RealPresence Group 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.

To select a multipoint viewing mode:

1. In the 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.

Multipoint Viewing Modes

Setting	Description
Video images from multiple sites can be automatically combined on one monitor in a display known as *continuous presence*.	
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.

Multipoint Viewing Modes

Setting	Description
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.

The RealPresence Group systems support several multipoint layouts, as well as dual-monitor compositing. When you use two monitors of equal size, you have the capability of up to eight-way multipoint calling, depending on your system configuration. When sharing content, one monitor is used for content and one for people, but the configuration varies, depending on whether you have enabled Self View and how many people are participating. When you do not share content, the configuration for both monitors is spread over both monitors, again depending on whether Self View is enabled and how many participants are in the call.

Note: Multipoint layouts and system type

When the host of a conference call is a RealPresence Group 500 system, the system displays all remote sites on a split screen with the speaker in a large window. On the RealPresence Group 700 system, up to 8 sites are displayed on the monitor based upon layout chosen. When the host has dual monitors, the layout can span both monitors. The far-end site sees 4 sites, with each quadrant displaying the last 4 speakers.

Include an Additional Audio Call

When your multipoint conference call hits the maximum number of calls allowed for your license type, you can initiate one additional outbound, audio-only call from your RealPresence Group system. However, incoming calls are rejected for as long as you are at the call limit for your system.

Keep in mind the following points:

- When the multipoint option is disabled, or if you are making a TIP-enabled call, the RealPresence Group system supports one video call and one audio-only call.
- Audio-only calls can be encrypted and unencrypted independently from video calls.

Note: Audio call limits

After you reach the call limit and make an audio-only call, if you hang up a video call and try to make another call, the call will still be an audio-only call.

Enable and Disable Audio Add In

Audio Add-In feature is the default behavior. You can disable and enable it in the web interface.

To disable Audio Add In:

» Go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options** and clear the **Enable Audio Add In** checkbox. Click **Save**.

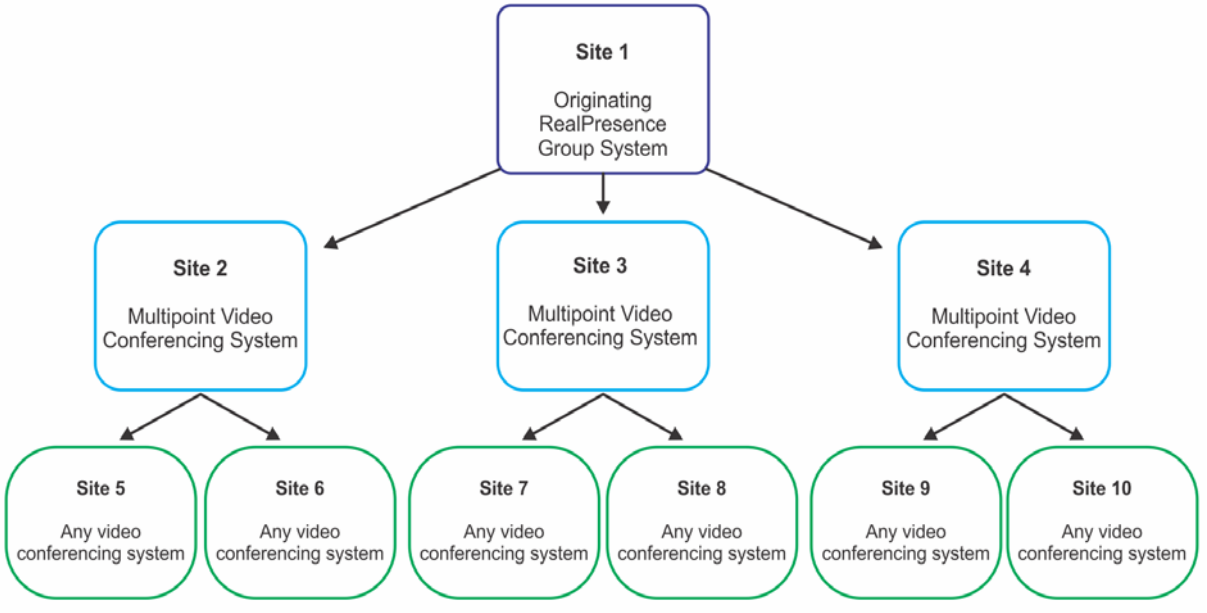
To enable Audio Add In:

» Go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options** > and select **Enable Audio Add In**. Click **Save**.

Include Multiple Sites in a Cascaded Call

You can include multiple sites in a cascaded call if the sites you call have internal multipoint capability. The following diagram shows how to do this.

Cascaded call with multiple sites



To place a cascaded call:

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.

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 Polycom RealPresence Group 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.

Note: Group calling not supported on RealPresence Group 300 and 310 systems
You cannot place group calls on RealPresence Group 300 or 310 systems.

Manage Directories in the Web Interface

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

Polycom RealPresence Group 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 or Microsoft Lync Server 2013
- Up to 4,000 contacts from a Polycom GDS server.
- An unlimited number of contacts when the RealPresence Group system is registered with Skype for Business 2015 or Microsoft Lync Server 2013.

Polycom RealPresence Group systems support up to 200 Favorites groups that users create within Favorites. 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 or Microsoft Lync Server 2013, which appear in the Favorites group.

Note: Microsoft integration requires Professional Services
Assistance from Polycom Microsoft Integration Services is mandatory for Skype for Business 2015 or Microsoft Lync Server 2013 integrations. For additional information and details, please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Browse Global Directory Entries

Global directory 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 scroll through the global directory to view a list of all global directory entries and 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), Microsoft Lync, or Lightweight Directory Access Protocol (LDAP) global directory.

The global directory browsing feature does not support directory servers that are unable to store contents locally on RealPresence Group systems, including Microsoft Lync in Web Query mode.

To browse the global directory using the web interface:

1. In the web interface, select **Place a Call > Global Entry**.
2. Scroll through the global directory entries and select **Call** to place a call or select an entry to view the contact's information.

Note: Browsing the LDAP directory
In order 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.

Manage Favorites

Local interface users can select **Contacts** from the menu to view favorites and the directory.

Web interface users can add favorites from the directory, create new favorite contacts, and create favorite groups. You perform the following tasks on the **Place a Call > Manage Favorites** screen.

To create a new Favorites contact:

1. To create a favorite contact not in the directory list, click **Create New Favorite**.
2. Enter the contact call information and click **Save**.

To create a Favorites group:

1. Click **Create New Group**.
2. Enter a **Name** for the group and click **Save**.

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

To edit a Favorites group:

1. Find the group name in the list of contacts.
2. Next to the group contact name, click **Edit Group**.

   Do one of the following:

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

To delete a Favorites contact or group:

1. In the search box, type a contact name and click **Search**.
2. In the contact name you want to delete, click **Delete**.

Import and Export Favorites

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

To access these features, you must be able to access a web browser on your device. Polycom recommends you use one of the following web browsers:

- Microsoft Internet Explorer
- Mozilla Firefox

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 on the RealPresence Group system.
- When the uploaded XML file includes favorites groups or entries already on your RealPresence Group system, the duplicate files are added as separate directory entries.

To export Favorites groups and contacts:

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

You can export Favorites groups and entries both when you are in a call and when you are not in a call on the RealPresence Group system.

To import Favorites groups and contacts:

1. In the 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 RealPresence Group system.

Types of Favorites Contacts

Favorites contains the types of Contacts shown in the following table.

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

Directory Server Registration	Types of Contacts	Presence State Displayed
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 and Microsoft Lync Server 2013 directory entries are saved as Contacts by the user and stored on the Skype/Lync Server. Users must create their contact lists using Microsoft Office Communicator on a computer. Users cannot edit or delete these entries from Favorites using the Polycom RealPresence Group system. Users can copy these entries to other Favorites and remove them from those groups.	Real-time presence

Connect to Microsoft Exchange Server Calendaring Service

RealPresence Group 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. A RealPresence Group 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.

Connecting to a calendaring service allows the system to:

- Display the day's scheduled meetings, along with details about each.
- 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.

If the meeting was created using the Polycom Conferencing Add-In for Microsoft Outlook or Lync Meeting Add-in for Microsoft Office 2013, the RealPresence Group system can do the following:

- Identify video-enabled meetings with a  icon displayed on the system calendar.
- Let users join the meeting without knowing the connection details.

Note: Microsoft integration requires Professional Services

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.

To configure the Calendaring Service:

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

Setting	Description
Enable Calendaring Service	Enables the system to connect to the Microsoft Exchange Server 2013 or and retrieve calendar information.
Email	Specifies the Outlook mailbox or 365 account this system should monitor for calendar information. This should match the Primary SMTP Address for the account on Microsoft Exchange Server 2013, which displays as the value of the mail attribute in the account properties.
Domain	Specifies the domain for registering to the Microsoft Exchange Server 2013, in either NETBIOS or DNS notation, for example, either `company.local` or `COMPANY`. If you are using the **Auto Discover Using** option, do not provide a value in this field.
User Name	Specifies the user name for registering to Microsoft Exchange Server 2013, 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 the Microsoft Exchange Server 2013. 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 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 RealPresence Group 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 RealPresence Group system to use for the Calendaring Service. The system may prompt you to confirm the password. If after configuring the Calendaring Service a message pops up informing you 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. You can also use an API command to automatically discover the Microsoft Exchange Server address. For more information, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.

Setting	Description
Microsoft Exchange Server	Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access Server. If your organization has multiple Client Access 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. Otherwise, use the **Auto Discover Using** option that allows the system to automatically determine the connection information for Microsoft Exchange Server 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.

Join Scheduled Meetings

If your RealPresence Group system is configured to connect to the Microsoft Exchange Server, and the Polycom Conferencing for Microsoft Outlook add-in is installed at your site, 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.

To join a scheduled meeting from the Home screen:

1. With your remote, select a meeting on the Home screen.
2. Select **Join** to call into the meeting. If **Join** is not displayed, you must get and install the Polycom Conferencing Add-In for Microsoft Outlook or Lync Meeting Add-in for Microsoft Office 2013.

For information about displaying the Calendar button on the Home screen, refer to Customize the Local Interface Home Screen. For more information about using Polycom Conferencing for Microsoft Outlook, refer to the *User Guide for the Polycom RealPresence Group Series*. 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 Deployment Guide* at support.polycom.com.

Use the Web Interface Place a Call Page

When you click the **Place a Call** link on the web interface, the default view shows you the following widgets:

- Search
- Place a Call
- Contacts

- Manual Dial
- Speed Dial
- Recent Calls
- Support Documents

For information on configuring Home screen settings for the local interface, refer to Customize the Local Interface Home Screen.

Search

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

Place a Call

In the **Place a Call** area, you can place a call by searching your contacts or manually:

To call a favorite contact:

1. In the **Contacts** section, enter a name and click **Search**.
2. Select a contact name and click **Call**.

For information about editing Favorites contacts, refer to Manage Favorites.

To place a call manually:

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.

To require a password, select **Meeting Password** and enter a password in the field that displays below the check box.

Speed Dial

On the web interface Place a Call page, you can call Speed Dial contacts and can edit the Speed Dial contact list.

To call speed dial contacts:

» In the Speed Dial section, select a contact from the list and click **Call**.

To add speed dial contacts:

1. In the **Speed Dial** section, click **Edit**.

2 Enter a contact name and click **Search**.
3 In the contact you want to add, click **Add**.
4 To save your changes, click **Done**.

To remove speed dial contacts:

1 In the **Speed Dial** section, click **Edit**.
2 In the contact you want to delete, click **Remove**.
3 To save your changes, click **Done**.

Recent Calls

On the web interface Place a Call page, you can place calls to Recent Call contacts.

You can also configure a Recent Calls list to display on the RealPresence Group system Place a Call screen on the web interface and Home screen on the local interface. The list includes the following information:

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

To dial a recent call from the web interface:

» On the web interface Place a Call page'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**.

To configure Recent Calls in the web interface:

1 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 Polycom RealPresence Group 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 web interfaces.
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 Polycom RealPresence Group system web interface. For more information about the CDR, refer to Call Detail Report (CDR).

Support Documents

You can easily access support documents from the web interface.

Stop and Start Camera Video in a Call

You can stop your near-end site camera video while in a call. Using the local interface, you can also stop your near-end site camera video before a call begins. You can then start your camera video again at any time.

Stopping your camera video allows you to stop sending your near-end, camera-encoded video while still remaining connected to the conference. When your video is stopped, the far-end site does not see near-end video transmission from you.

When your camera video is turned off in non-Lync environments, a video pause image is sent to the far-end site. In Lync environments, video transmission stops, and no Self View is displayed when your video is stopped. Turning off your video does not affect the sending or receiving of content.

To stop camera video from the web interface in a call:

» Select **Camera Off** from the call menu at the top of the screen.

When you stop the video, a video pause icon appears on the display.

To start camera video from the web interface in a call:

» Select **Camera On** from the call menu at the top of the screen.

When you start the video, the video pause icon disappears from the display.

For information on stopping and starting video from the local interface, refer to *Polycom RealPresence Group Series User Guide.*

Place Calls in Kiosk Mode

In the local interface, Kiosk Mode simplifies the Home screen by displaying only speed dial entries and calendar meetings (if enabled). In Kiosk Mode, therefore, you can call speed dial numbers, join calendar meetings, and answer calls.

You must create your speed dial numbers before you use Kiosk Mode.

Kiosk Mode is disabled by default. If Kiosk Mode is enabled, these conditions apply:

- The Home screen menu, Out of Call menu, and other icons are disabled.
- Alerts bring the local interface out of Kiosk Mode until you clear the alerts.
- You can still use the remote to adjust the volume, control the camera, and mute/unmute the microphone when in calls.
- You can bring up the In a Call menu by pressing Menu on the remote during the call.

To enable Kiosk Mode:

1 In the web interface, go to **Manage Favorites > Create Favorite** and create one or more Favorites.

2. On the web interface Place a Call screen, select **Edit** next to **Speed Dial**, then search for and add Favorites to Speed Dial.
3. Go to **Admin Settings > General Settings > Home Screen Settings > Speed Dial**.
4. Select **Enable Speed Dial** and then click **Save**.
5. Go to **Kiosk Mode**, then select **Enable Kiosk Mode** and click **Save**.

For information on using Kiosk Mode, refer to the *User Guide for the Polycom RealPresence Group Series and the Polycom Touch Control*.

Security

To configure your RealPresence Group system security settings using the system web interface, use one of the following browsers with cookies enabled:

- Microsoft Internet Explorer version 9 or 10
- Mozilla Firefox 22
- Apple Safari 6.0.5

For detailed security information, see the following topics:

- Configure Security Profiles
- Manage System Access
- Enable a Whitelist and Add IP Addresses
- Enable Visual Security Classification
- Manage Certificates and Revocation
- Set Up Security Banners
- Configure a Meeting Password

To go to the web interface:

» Open a web browser and enter the IP address of the RealPresence Group system using the `https://IPaddress` (for example, `https://10.11.12.13`).

For more information about using the web interface, refer to Access the Web Interface.

Caution: HTTP redirects to HTTPS
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 RealPresence Group Series web interface via HTTP are redirected to the HTTPS interface.

You can find security options and passwords in this part of the interface:

- In the local interface, go to **Settings > Administration > Security**.

  The local interface has general, password, and remote access settings.
- In the web interface, go to **Admin Settings > Security**.

  The web interface has global and local settings.

Settings are under different sections of the security interfaces. Not all systems show all of the options, and many settings in the web interface are unavailable in the local interface.

Note: Security options by country
In accordance with local laws and regulations not all security options are available in all countries.

Configure Security Profiles

RealPresence Group system security profiles provide varying levels of secure access to your RealPresence Group system. The security profile your RealPresence Group 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 the web interface Admin Settings. The default values and ability to change some RealPresence Group settings are affected by which security profile your system uses. Refer to the tables in Security Profile Default Settings to see how these settings are affected for each security profile.

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. For specific configuration information, refer to each profile's settings in Security Profile Default Settings.

To view or change a security profile:

1. In the 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.

Manage System Access

Managing access to the RealPresence Group system is essential for security. This section includes the following topics:

External Authentication

Polycom RealPresence Group systems support two roles 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.

Polycom RealPresence Group systems provide two local accounts, 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 RealPresence Group system itself.

An administrator can configure RealPresence Group 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 RealPresence Group system. The AD administrator assigns accounts to AD groups, one for RealPresence Group system admin access and one for user access. For this reason, external authentication is also referred to as Active Directory authentication.

The RealPresence Group system administrator configures the external authentication settings on the RealPresence Group 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 RealPresence Group system. The RealPresence Group 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)

Note: Active Directory Server with PKI

When External Authentication is enabled in PKI environments where **Always Validate Peer Certificates from Server** is enabled on the RealPresence Group 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 RealPresence Group 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 RealPresence Group system using the server's IP address results in certificate validation failure, and consequently authentication failure. The RealPresence Group system configuration would have to specify the server by DNS name, in this case, to successfully match the server certificate data.

RealPresence Group systems support Active Directory on Microsoft Windows Server version 2008 R2 and Microsoft Windows Server 2012.

Note: Local user account can be disabled
The RealPresence Group system local user account is disabled when **Enable Active Directory External Authentication** is enabled. The admin account is active and usable, however.

To enable external authentication:

1. In the web interface, go to **Admin Settings > Security > Global Security > Authentication**.
2. Configure these settings on the Authentication page, 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:** RealPresence Group 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 RealPresence Group system. This name must exactly match the name in the ADS for authentication to succeed.
Active Directory User Group	Specifies the Active Directory group whose members should have user access to the RealPresence Group system. This name must exactly match the name in the ADS for authentication to succeed.

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.

Note: Use local admin credentials to pair
You can only use the local Polycom RealPresence Group system admin credentials to pair the system with a Touch Control.

Login and Credentials

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

Local Access

Local access means using a RealPresence Group system through the local interface.

To configure local access to the system:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Security > Passwords**.
   - In the 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.
Admin Remote Access Password	Specifies the password for the local administrator account used when logging in to the system remotely using the 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. You can enable this setting at any time. **Note**: This setting is supported for the RealPresence Group systems only. It is not supported for the RealPresence Touch or Polycom Touch Control devices.
User ID	Specifies the ID for the user account. The default User ID is `user`. User IDs are not case sensitive.

Setting	Description
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.

Note: Enabling Maximum Security Profile requires new ID values

When you configure the RealPresence Group 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

Remote Access

Remote access means using a RealPresence Group 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 RealPresence Group system, such as the local interface, web interface, telnet, or serial API.

To configure remote access settings:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Security > Remote Access**.
   - In the 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) (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 web interface.
Allow Access to User Settings	Specifies whether the User Settings screen is accessible to users through the local interface. For more information about user access settings, refer to Manage User Access to Settings and Features.

Setting	Description
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 Polycom RealPresence Group 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 Polycom RealPresence Group 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. For more information about this setting, refer to Secure API 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**.
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 Polycom RealPresence Group 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	For information about this setting, refer to Port Lockout.
Enable Whitelist	Specifies whether to enable a whitelist. For more information about this setting, refer to Enable a Whitelist and Add IP Addresses.
Idle Session Timeout in Minutes (web interface only)	Specifies the number of minutes your web interface session can be idle before the session times out.
Maximum Number of Active Sessions (web interface only)	Specifies the maximum number of users who can be logged in to and using your system through telnet or the web interface at the same time.

Manage User Access to Settings and Features

You can allow users to change common user preferences by providing access to the User Settings screen.

To allow users to customize the workspace, select the **Allow Access to User Settings** option to make the **User Settings** choice on the Settings screen available to users on the local interface's Home screen.

If the Polycom RealPresence Group system is paired with a Polycom Touch Control, selecting **Allow Access to User Settings** makes the **RealPresence Group Series system** tab available on the Touch Control User Settings screen.

User Settings contains the following options, 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

Detect Intrusions

The Polycom RealPresence Group system logs an entry to the security log when it detects a possible network intrusion. This logging is controlled by the setting **Admin Settings > Security > Global Security > Access > Enable Network Intrusion Detection System (NIDS)**. 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
```

Secure API Access

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

Note: Empty passwords

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.

Enable and Disable Secure API Access

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

To enable SSH for secure API access, do one of the following:

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

To disable SSH for secure API access, do one of the following:

- In the web interface of the RealPresence Group Series system, select **Admin Settings > Security > Global Security > Access** and disable the **Enable SSH Access** setting.
- In a RealPresence Group Series 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 system on port 22.

Note: Maximum login attempts

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:

1. Enable remote access.
2. If necessary, enable external authentication.
3. Enable the SSH feature.
4. Start an SSH session using the Polycom RealPresence Group series system IP address and port 22.
5. When prompted, enter the remote access credentials.

For information on accessing the API, refer to the *Polycom RealPresence Group Series Integrator Reference Guide* at support.polycom.com.

Configure Admin ID and Password for the Polycom Touch Control

You can set an admin ID and password, which allows you to limit access to the Polycom Touch Control Administration settings.

To set a Polycom Touch Control admin ID and password:

1. From the Home screen touch  **Administration.**

   An admin ID and password might be configured for the Touch Control Administration settings. The default ID is `admin` and the default password is `456`.
2. Touch the **Security** tab.
3. Set the following security settings.

Setting	Description
Admin ID	Specifies the ID for the administrator account. The default Admin ID is `admin`.
Admin Password	Specifies the password for administrator access when logging in to the Touch Control. The default password is `456`. When this password is set, you must enter it to configure the Touch Control Admin Settings. The password must not contain spaces.

Local Accounts

For RealPresence Group system accounts, you need to set up password policies and account lockout settings.

Password Policies

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 system.

To configure password policies:

1. In the 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.

Setting	Description
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.
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.

Account Lockout

RealPresence Group systems provide access controls that prevent unauthorized use of the system. 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 RealPresence Group systems. 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. For more information about that mechanism, refer to Port Lockout.

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 RealPresence Group system’s Admin and User local accounts. When external authentication is used, the Active Directory Server protects Active Directory accounts.

RealPresence Group 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

To configure the account lockout feature:

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

The following are examples of how the account lockout feature works.

A RealPresence Group system web interface is configured with these settings:

- **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 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 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 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.

Enable a Whitelist and Add IP Addresses

When a whitelist is enabled, the Polycom RealPresence Group 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 web interface.

Note: Update whitelist if you have dynamic IP address

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.

To enable a whitelist:

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

To add addresses to an enabled whitelist:

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:

- `10.12.128.7`
- `172.26.16.0/24`

IPv6 Address Formats

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

- `::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

Note: Whitelist limit
The system can accept up to 30 IP address entries for the whitelist.

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. It is supported only on the web interface.

Note: Telnet port lockout
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.

To configure the port lockout feature:

1. In the 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 web interface from accepting logins. If set to **Off**, the system does not lock the web interface due to failed login attempts.
Port Lock Duration	Specifies the amount of time that a 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 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**). 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.

Port lockout is supported only on the web interface, and only Admin users are allowed to log in to the web interface. If external authentication *is not* in use, users can successfully log in to the 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 web interface.

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

A RealPresence Group 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 web interface, and another user fails to log in to the external Active Directory ‘SuperUser’ account in a separate 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 web interface port—two by one user and one by a second user. If the next attempt to log in to the web interface by either user or some other user is successful, the failed login counter for the web interface port is reset to zero, allowing 4 more failed attempts to occur on the 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 web interface, further attempts to access the 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 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 web interface, and another user fails to log in to the external Active Directory ‘SuperUser’ account in a separate 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 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 web interface is locked.

Encryption

AES encryption is a standard feature on all Polycom RealPresence Group 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 Polycom RealPresence Group systems with a maximum speed of 6 Mbps for unencrypted calls, the maximum speed for encrypted SIP calls is 4 Mbps.

RealPresence Group systems provide the following AES cryptographic algorithms to 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

RealPresence Group 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.

To enable encryption:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Security > Settings**.
   - In the 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 (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

Configure Encryption Settings for SVC Calls

You must complete two quick tasks to enable encryption for SVC calls:

- Set the transport protocol.
- Set AES encryption.

To set the transport protocol:

1. In the 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**.

To set AES encryption:

1. In the 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**.

For more information on SVC-based calling, refer to Set SVC Call Preferences.

Configure Encryption Settings for Skype for Business 2015 and Microsoft Lync 2013

Polycom RealPresence Group systems support media encryption in calls with Skype for Business 2015 and Microsoft Lync 2013. Skype for Business 2015, Microsoft Lync 2013 Server pool, and the Polycom RealPresence Group system must be configured to support encryption so that calls can connect with encryption. If components have encryption turned off, calls connect without encryption. If one component is set to require encryption and the other is not, calls fail to connect.

Before you use Microsoft Lync 2013 or Skype for Business 2015 in video conferences with RealPresence Group systems, you must enable AES encryption in the web interface.

To enable encryption for Microsoft Lync 2013 and Skype for Business 2015:

» Go to **Admin Settings > Security > Global Security > Encryption > Require AES Encryption for Calls** and ensure that **When Available** is selected.

For more information about encryption configuration in a Skype for Business 2015 or Microsoft Lync Server 2013 environment, refer to the *Polycom Unified Communications for Microsoft Environments Deployment Guide* at support.polycom.com.

H.323 Media Encryption

To provide extra security for encrypted H.323 calls, the RealPresence Group 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.

To verify the check codes match:

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 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.

List of Sessions

You can use the sessions list to see information about everyone logged in to a RealPresence Group system including:

- Type of connection, for example, Web

- ID associated with the session, typically Admin or User
- Remote IP address (that is, the addresses of people logged in to the RealPresence Group system from their computers)

To view the Sessions List:

» From the local interface, go to **Settings > System Information > Diagnostics > Sessions**.

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

Enable Visual Security Classification

This feature helps RealPresence Group system call participants remain conscious of the security classification when in a BroadWorks managed call. During and throughout a call, the Visual Security Classification (VSC) provides a visual indication to the RealPresence Group 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 web interface. Before enabling this feature, ensure the following:

- The RealPresence Group system must be registered to a BroadSoft R20 call server.
- The Multipoint Video Conferencing option key must be disabled.
- AS-SIP must be disabled.

To enable Visual Security Classification:

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

Manage Certificates and Revocation

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 RealPresence Group Series products before you integrate these products with the PKI.

RealPresence Group systems can use certificates to authenticate network connections to and from the Polycom RealPresence Group 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.

RealPresence Group systems can generate requests for certificates (CSRs) that can be 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 RealPresence Group system for use in all TLS connections used by the system.

RealPresence Group 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 RealPresence Group system's web server presents this certificate after receiving connection requests from browsers attempting to connect to the RealPresence Group system web interface.
2. A Client certificate—the RealPresence Group system presents this certificate to a remote server when challenged to provide a certificate as part of authenticating the identity of the RealPresence Group 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 RealPresence Group systems are deployed in an environment that does not have a fully deployed PKI, you do not need to install these certificates because all RealPresence Group 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 Polycom RealPresence Group system web interface.

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 Group 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 RealPresence Group system web interface, the RealPresence Group system is the server and the web browser is the client application. In other situations, such as when the RealPresence Group system connects to LDAP directory services, the RealPresence Group system is the client and the LDAP directory server is the server.

To configure certificate usage:

1. 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 RealPresence Group system when a network connection is being established between the two systems.
Always Validate Peer Certificates from Browser	Controls whether the RealPresence Group system requires a browser to present a valid certificate when it tries to connect to the web interface.
Always Validate Peer Certificates from Server	Controls whether the RealPresence Group system requires the remote server to present a valid certificate when connecting to it for services such as those listed for client-type CSRs in Create Certificate Signing Requests (CSRs) (provisioning, directory, SIP, and so forth).
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 Group system. The following section outlines how to do this, and the procedure is the same for installing the client certificate, the server certificate, and any required CA-type certificates.

To add a signed certificate on the Certificates page:

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 RealPresence Group 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 page.
5. Click **Save**.

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

Note: Add server certificate before using web interface

If you do not add the server certificate for the RealPresence Group system before using the 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.

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 Group system. The following section outlines how to do this, and the procedure is the same for installing the client certificate, the server certificate, and any required CA-type certificates.

To add a signed certificate on the Certificates page:

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 RealPresence Group 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 page.
5. Click **Save**.

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

Note: Add server certificate before using web interface

If you do not add the server certificate for the RealPresence Group system before using the 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.

Create Certificate Signing Requests (CSRs)

The RealPresence Group system allows you to install one client and one server certificate for identification of the RealPresence Group 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 RealPresence Group system. 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 example, if your RealPresence Group 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 RealPresence Group system web server uses the server-type CSR and resulting certificate whenever a user attempts to connect to the RealPresence Group 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 RealPresence Group 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 RealPresence Group system.

To create a CSR:

1. 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 page 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.
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
Organization (O)	Specifies your organization's name. Default is blank. Maximum Characters: 64

Setting	Description
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
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

Note: Adding more OU fields

The RealPresence Group 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.

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: One CSR allowed

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 RealPresence Group 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.

Configure Certificate Revocation Settings

When certificate validation is enabled (refer to Configure Certificate Validation Settings), the RealPresence Group 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 RealPresence Group 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 RealPresence Group system for each CA whose certificate has been installed on the system.
- The Online Certificate Status Protocol (OCSP). OCSP allows the RealPresence Group system to contact an *OCSP responder*, which is a network server that provides real-time certificate status through a query/response message exchange.

You must configure the RealPresence Group system to use the revocation method most appropriate for your environment.

Note: CRL download limitation

The RealPresence Group 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 RealPresence Group 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.

To use CRLs:

1. Go to **Admin Settings > Security > Certificates > Revocation.**
2. Configure these settings on the Revocation page and click **Save**.

Setting	Description
Revocation Method	Select the CRL method.
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. The RealPresence Group system assumes that the lack of a CRL means the certificate is not revoked. If a CRL is installed, the system performs a revocation check when validating the certificate.
Add CRL	1 Click **Browse** to search for and select a CRL. 2 Click **Open** to add the CRL to the list.

You can also view automatically and manually downloaded CRLs on this page. To remove a CRL from the list, click **Remove**.

Note: Expired CRL blocks web interface access

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 RealPresence Group system web interface because the revocation check always fails. In this case, unless the RealPresence Group 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. See the Delete Certificates and CRLs for more information.

To use OCSP:

1. Go to **Admin Settings > Security > Certificates > Revocation.**
2. Configure these settings on the Revocation page and click **Save**.

Setting	Description
Revocation Method	Select the OSCP method.
Allow Incomplete Revocation Checks	When this field is enabled, the RealPresence Group system treats the following response from the OCSP responder as a successful revocation checks that would otherwise be considered a failed 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 RealPresence Group system treats this as a revocation check failure and does not allow the connection. • If the OCSP responder indicates a known *good* status, the RealPresence Group 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 RealPresence Group system attempts to use the address in the certificate (when present) instead of the **Global Responder Address** specified in the previous field. **Note:** The Polycom RealPresence Group system supports only the use of HTTP URLs in the AIA field of a certificate when **Use Responder Specified in Certificate** is enabled.

Note: OCSP response message and CA certificates

For validation of the OCSP response message, if you use OCSP, you might need to install one or more additional CA certificates on the RealPresence Group systems.

Certificates and Security Profiles within a Provisioned System

When your RealPresence Group 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 RealPresence Group endpoint during installation using the setup wizard, or afterwards using the web interface.
  - You must use full PKI and observe the following procedures before you enable provisioning on the RealPresence Group endpoint:
    1. You must install a signed client certificate on the RealPresence Group 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 RealPresence Group endpoint during installation using the setup wizard, or afterwards using the 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.

Delete Certificates and CRLs

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

To delete all certificates and CRLs the RealPresence Group system is using:

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

The RealPresence Group system restarts after deleting all installed certificates and CRLs.

RealPresence Server Address Configuration in PKI-enabled Environments

When configuring the server addresses for the services listed in Create Certificate Signing Requests (CSRs) as potentially needing a client-type CSR (such as SIP, LDAP directory etc.), you might need to use a particular address format if the server address is contained in the server certificate that it presents when connecting to it. If this is the case, use the following guidance for configuring these server addresses on the RealPresence Group system:

- 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.

Set Up Security Banners

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

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.
```

Note: No security banner on the Polycom Touch Control

The security banner is not supported with the Polycom Touch Control.

To configure a security banner:

1. In the 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 web interface.
Local System Banner Text	If you enable the security banner on the 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 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.

Configure a Meeting Password

If you set up a meeting password, users must supply the password to join multipoint calls on the RealPresence Group system when the call uses the internal multipoint option, rather than 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.

To configure a meeting password:

1. Do one of the following:
   - In the local interface, go to **Settings > Administration > Security > Passwords**.
   - In the web interface, go to **Admin Settings > Security > Meeting Password**.
2. Enable and configure the **Meeting Password** setting.

Manage the System Remotely

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

- The Polycom RealPresence Group 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.
- For more information about the API commands, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.

Use the Polycom RealPresence Group System Web Interface

You can use the Polycom RealPresence Group system web interface to perform most of the calling and configuration tasks you can perform on the local system. The Polycom RealPresence Group system web interface is supported for Microsoft Internet Explorer version 9 or later or Mozilla Firefox 22 on Windows, and Apple Safari 6.0.5 on Mac OS X.

Access the Web Interface

To configure your browser to use the web interface:

- Be sure that you use Microsoft Internet Explorer 9.0 or later, or Apple Safari, as your web browser.
- Configure the browser to allow cookies.

To access the system using the web interface:

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`), and enter the Admin Remote Access Password, if one is set.

Monitor a Room or Call with the Web Interface

The monitoring feature within the web interface allows administrators of RealPresence Group systems to view a call or the room where the system is installed.

To enable room and call monitoring:

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

To monitor a room or call using the web interface:

1. In your web browser address line, enter the system's IP address.
2. Go to **Utilities > Tools > Remote Monitoring**.
3. Perform the following tasks, depending on whether you are in or out of a call:
   - Place or end a call
   - View near and far sites
   - Use Call Control to change moderators and broadcast participants
   - Show content from a laptop, PC, DVD player, or document camera
   - Change camera sources
   - Adjust camera position
   - Adjust system volume
   - View camera presets
   - Zoom cameras
   - Mute and unmute the microphones

Manage System Profiles with the Web Interface

Administrators managing systems that support multiple applications can change system settings using profiles. You can store a RealPresence Group system profile on a computer as a `.profile` file using the web interface. The number of profiles you can save is unlimited.

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.

Note: System profiles for backing up system

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.

To store a profile using the web interface:

1. In your web browser address line, enter the system's IP address.
2. Go to **Utilities > Services > Profile Center**.

3 Click **Download** next to **Current Settings Profile** to download the profile file from the system.
4 Save the file to a location on your computer.

To upload a profile using the web interface:

1 Reset the Polycom RealPresence Group system to restore default settings.
2 In your web browser address line, enter the system's IP address.
3 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.

Send a Message

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 site can see the message; it is not broadcast to all the sites in the call.

To send a message using the web interface:

1 Go to **Diagnostics > Send a Message**.
2 In the Send a Message page, 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 Servers

Set Up a Directory Server

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.

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

Directory Servers Supported	Authentication Protocols	Global Directory Groups	Entry Calling Information
Polycom GDS	Proprietary	Not Supported	Might include: • H.323 IP address (raw IPv4 address, DNS name, or H.323 extension) • ISDN number
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*
Skype for Business Server 2015/Microsoft Lync Server 2013	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

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

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
Skype for Business Server 2015/Microsoft Lync Server 2013	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

To configure the Polycom GDS directory server:

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

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.

To configure the LDAP directory server:

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

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.

To configure the Skype for Business Server 2015 or Microsoft Lync Server 2013 directory settings:

1. In the web interface, go to **Admin Settings > Network** > **IP Network** > **SIP.**
2. Configure the SIP settings as described in Configure SIP Settings for Integration with Microsoft Servers.
3. In the web interface, go to **Admin Settings > Servers > Directory Servers and select the Microsoft** Service Type.
4. Configure these settings on the Directory Servers page.

Setting	Description
Registration Status	Specifies whether the system is successfully registered with the Skype for Business Server 2015 or Microsoft Lync Server 2013.
Domain Name	Specifies the Domain Name entered on the SIP Settings screen.
Domain User Name	Specifies the Domain User Name entered on the SIP Settings screen.
User Name	Specifies the User Name entered on the SIP Settings screen.

Set Up SNMP

RealPresence Group systems support SNMP (Simple Network Management Protocol) versions 1, 2c, and 3. A RealPresence Group system sends SNMP reports to indicate conditions, including the following:

- All alert conditions found on the Polycom RealPresence Group system alert page
- 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

Download MIBs

In order 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 Polycom RealPresence Group system web interface.

To download a Polycom MIB using the Polycom RealPresence Group system web interface:

1. In your web browser address line, enter the RealPresence Group system's IP address.
2. Go to **Admin Settings > Servers > SNMP**.
3. Click the desired link:
   - Download Legacy MIB

- Download MIB

Set Up SNMP Management

To configure the RealPresence Group system for SNMP Management:

1. In the 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
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.

Setting	Description
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 checkbox next to the **Port** setting disables the corresponding Destination Address.

Use a Provisioning Service

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

- Polycom RealPresence Group systems are registered to a standards-based presence service, so presence states are shared with Contacts.
- Polycom RealPresence Group 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 RealPresence Group system.
  - The Polycom RealPresence Group 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 RealPresence Group system. When RealPresence Group systems request provisioning, the provisioned bundle and any automatic settings are downloaded. A RealPresence Group system user with administrative rights can change the settings on the RealPresence Group 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 a Polycom Touch Control is connected to a provisioned RealPresence Group system, a RealPresence Resource Manager system can receive status updates from the Polycom Touch Control and can provide software updates to the Polycom Touch Control. For supported RealPresence Resource Manager versions, go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html and click the **Current Interoperability Matrix** link.

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 or Disable the Provisioning Service

You can register the Polycom RealPresence Group system with the RealPresence Resource Manager system in several 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 RealPresence Group 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 RealPresence Group system web interface.

To enable and configure a provisioning service in the Admin Settings:

1. In the web interface, go to **Admin Settings > Servers > Provisioning Service.**
2. Select the **Enable Provisioning** setting.
3. Configure these settings for automatic provisioning. Multiple Polycom RealPresence Group systems can be registered to a single user.

   When available, the RealPresence Group system completes the fields mentioned in step 4. If the system does not complete the fields automatically, get this information from your network administrator.

Setting	Description
Server Type	Specifies the type of provisioning server. Select RPRM or DMS.
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.

Note: Troubleshoot provisioning registration

If automatic provisioning is enabled but the 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 update it on the Polycom RealPresence Group system, too. To avoid unintentionally locking a user out of network access in this case, RealPresence Group systems do not automatically retry registration until you update the settings and register manually on the Provisioning Service page.

To disable a provisioning service:

1 In the web interface, go to **Admin Settings > Servers > Provisioning Service**.

2 Disable the **Enable Provisioning** setting.

Set Up Multitiered Directory Navigation

You can use the RealPresence Resource Manager to navigate the RealPresence Group 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.
- You cannot use Polycom Touch Control to navigate the RealPresence Group system LDAP directories.
- This feature is supported on dynamically-managed RealPresence Group systems only.

To use multitiered directory navigation, you must configure the following web interface settings:

- Go to **Admin Settings > Servers > Directory Servers** and make selections for each setting. For more information about these settings, refer to the Set Up a Directory Server.
- Go to **Admin Settings > Servers > Provisioning Service** and enable provisioning. For more information about these settings, refer to Enable or Disable the Provisioning Service.

Keep your Software Current

You can update your Polycom RealPresence Group system by going to support.polycom.com, navigating to **Documents and Downloads > Telepresence and Video**, and then downloading and installing the appropriate software. You can download and install software for the Polycom Touch Control, with no software or options key codes. You can also download and install Polycom Touch Control software from a web server.

You can also have your system automatically check for and apply software updates.

To automatically check for and apply software updates:

1. In the web interface, go to **Admin Settings > General Settings > Software Updates**.
2. Select **Automatic Software Updates**.
3. Configure these settings.

Setting	Description
Automatically Check for and Apply Software Updates	Enables settings that allow you to set up a schedule for automatically checking for and applying software updates to your system.
Start Time	Specifies the **Hour**, **Minute**, and **AM/PM** setting to start checking for updates.
Duration	Specifies how long the system should wait to determine whether updates are available.

For information about the latest software version, including version dependencies, refer to the *Polycom RealPresence Group Series Release Notes*. For detailed information about obtaining software key codes and updating your software, refer to the*Software and Options for the Polycom RealPresence Group Series and Accessories Installation Guide*.

Note: Automatic software updates
If your organization uses a management system for provisioning endpoints, your Polycom RealPresence Group system might get software updates automatically.

Control and Navigation

You can customize how the remote control works, set up various controllers for the system, and set the date and time on your system. See the following topics for more information:

- Configure Remote Control Behavior
- Connect Control and Accessibility Equipment
- Enable and Set Up the RealPresence Touch
- Set Up the Polycom Touch Control
- Enable SmartPairing
- Configure Contact Information
- Configure Regional Settings
- Configure Sleep Settings

Configure Remote Control Behavior

You can customize the behavior of the remote control to support the user's environment. Keep in mind the following regarding remote control behavior:

- If the Polycom RealPresence Group system is paired and connected with either a RealPresence Touch or a Polycom Touch Control, the remote control is disabled.
- The Polycom RealPresence Group system remote control IR transmits a modulated frequency of 38 kHz.
- When a USB keyboard is connected to a RealPresence Group system, you can enter only numbers with the remote control on the local interface's **Place a Call > Keypad** or **Place a Call > Contacts** screens.

To configure remote control behavior:

1. In the 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. For more information about Polycom RealPresence Group system IR codes, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.
Channel ID	Specifies the IR identification channel to which the Polycom RealPresence Group 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 Polycom RealPresence Group system set to any Channel ID. For more information about changing this setting, refer to Configure the Remote Control Channel ID.
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 RealPresence Group 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.

Configure the Remote Control Channel ID

You can configure the Channel ID so that the remote control affects only one Polycom RealPresence Group system, even if other systems are in the same room.

Note: Polycom Touch Control set to channel 3

The Polycom Touch Control virtual remote control is always set to channel 3.

If the remote control is set to channel 3, it can control a Polycom RealPresence Group 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.

Note: Do not block IR signal from remote

While performing these 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.

To configure the channel ID on the remote control:

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.
4. If the channel ID is saved successfully, the LED flashes twice. Otherwise, the LED flashes six times and you must repeat steps 1 - 3.

To confirm the channel ID from the remote control:

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.

To configure the channel ID for a Polycom RealPresence Group system and remote control in the web interface:

1. Go to **Admin Settings > General Settings > System Settings > Remote Control, Keypad, and Power**.
2. Select the **Channel ID**.
3. Click **Save**.

The channel ID must be the same on the remote control and in the web interface.

Connect Control and Accessibility Equipment

The RealPresence Group 300, RealPresence Group 310, RealPresence Group 500 systems provide one serial port to allow you to control the system through a touch-panel using the API.

The RealPresence Group 700 system also provides one serial port, but depending on your system's capabilities, you might be able to use the RS-232 serial port to control the system through a touch panel using the API.

Make sure that the system is powered off before you connect devices to it.

Connect Non-Polycom Touch Panel Controls

As part of a custom room installation, you can connect an AMX or Crestron control panel to a Polycom RealPresence Group system RS-232 serial port. To get started, complete these two main tasks:

- Program the control panel. Refer to the *Polycom RealPresence Group Series Integrator Reference Guide* for information about the API commands.
- Set the desired Login Mode for the control panel on the RealPresence Group system. For information on the available settings for Login Mode, see Configure RS-232 Serial Port Settings.

Configure RS-232 Serial Port Settings

To configure RS-232 serial port settings:

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

Setting	Description
RS-232 Mode	Specifies the mode used for the serial port. Available settings depend on the Polycom RealPresence Group 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. For more information about using third-party cameras, refer to Configure 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. **Note:** If you have a RealPresence Group 300, RealPresence Group 310, or RealPresence Group 500 system, use only the Polycom serial cable with part number 2457-63542-001 to connect devices to the RS-232 serial port.
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. • **adminpassword**—Requires the admin password, if one has been set, when the control system connects. (default) • **usernamepassword**—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**.

Enable and Set Up the RealPresence Touch

The RealPresence Touch graphical interface solution is a highly-intuitive touch control device that enables users to quickly initiate video conferences. By allowing participants to focus on their meeting, the RealPresence Touch accelerates your return on investment in telepresence and video solutions while making your organization more productive and efficient.

After you have paired the RealPresence Touch device to Polycom RealPresence Group system, you can control the system using the device's touch interface.

Enable Touch Devices on the Web Interface

If you want to use either the RealPresence Touch or the Polycom Touch Control device to control a RealPresence Group system, you must enable the device on the room system web interface. Once the touch device is enabled, you can pair it to a RealPresence Group system.

To enable Polycom touch devices:

1. On the web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
2. Select the **Enable Polycom Touch Device** check box and click **Save**.

   Your Polycom touch device is now enabled and you can pair it to a room system. Note that only one device can be paired to a room system at a time.

Set Up the RealPresence Touch Device

Before you can pair the RealPresence Touch device to a RealPresence Group system, you must install the software, set up the hardware, and use the set up wizard.

To set up the RealPresence Touch device:

1. Ensure that the correct software is installed on the Polycom RealPresence Group system that you want to control, and that you have completed the setup wizard on the system.

   For more information about updating the RealPresence Touch software, refer to *Polycom RealPresence Group Series and Accessories Install Software and Options*.
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 RealPresence Group system IP address at **Device Address**, then enter the **Admin ID** and **Password**.

6 Tap **Pair**.

If the RealPresence Group 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 RealPresence Group system. When pairing is successful, the RealPresence Touch splash screen is displayed, followed by the home screen.

For information about pairing, refer to Pair and Unpair a RealPresence Touch Device and a Polycom RealPresence Group System.

Set Up the Polycom Touch Control

The Polycom Touch Control allows you to control a Polycom RealPresence Group system.

Follow these steps to get started with the Polycom Touch Control. Refer to the *Setting Up the Polycom Touch Control* and *Polycom RealPresence Group Series and Accessories Install Software and Options* documents for more information.

To set up the Polycom Touch Control device:

1 Ensure that the correct software is installed on the Polycom RealPresence Group system that you want to control, and that you have completed the setup wizard on the system.

Refer to *Polycom RealPresence Group Series and Accessories Install Software and Options* for more information about updating the Polycom Touch Control software.

2 Connect the Ethernet cable to the underside of the Polycom Touch Control.

3 If you intend to use the Polycom Touch Control to show content from a computer, connect the USB cable to the underside of the Polycom Touch Control.

4 If you want to connect the stand, route the Ethernet and USB cables through the opening in the stand. Then attach the stand to the Polycom Touch Control by tightening the mounting screw with a screwdriver.

5 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 Polycom Touch Control powers on and displays the language selection screen.

6 Choose your language and follow the onscreen instructions to pair the Polycom Touch Control with your RealPresence Group system, or select **Pair Later** on the Pairing screen to skip pairing.

7 After the Polycom Touch Control connects to the network, enter the RealPresence Group system IP address and touch **Connect**. By default, the IP address of the RealPresence Group system is displayed on the bottom of its Home screen. If the RealPresence Group system is configured to allow pairing and you enter the IP address for the system correctly, the Touch Control displays a prompt for the Polycom RealPresence Group system admin user ID and password.

When the Polycom Touch Control has paired and connected with the RealPresence Group system, the Polycom Touch Control displays a success message, and the menus on the RealPresence Group system monitor become unavailable. For more information about pairing, refer to Pair the Polycom Touch Control and a RealPresence Group System.

Pair and Unpair a RealPresence Touch Device and a Polycom RealPresence Group System

When you configure the RealPresence Touch to pair with a particular Polycom RealPresence Group system, the RealPresence Touch makes an IP connection to the RealPresence Group system. If the connection is lost for any reason, the RealPresence Touch automatically attempts to restore the connection.

You can pair the RealPresence Touch and Polycom RealPresence Group system during initial RealPresence Touch setup, as described in Enable and Set Up the RealPresence Touch.

After you have completed RealPresence Touch setup, you can pair to a different RealPresence Group system using RealPresence Touch settings and can unpair using the web interface.

Pair the RealPresence Touch and a RealPresence Group System For the First Time

To pair your RealPresence Touch with a RealPresence Group system that has not been paired before, you must enter the room system's credentials before connection can be established. After the devices are successfully paired, the RealPresence Group remote control no longer has control of the system.

To manually pair for the first time to a RealPresence Group system:

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 RealPresence Group system.
4. Tap **Pair**.

The pairing connection begins, and the Home screen displays when the pairing is successful.

Pair a Previously Paired RealPresence Group System to a RealPresence Touch

If you have paired with a RealPresence Group 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. After the devices are successfully paired, the RealPresence Group remote control no longer has control of the system.

To pair a RealPresence Group system that was previously paired:

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 RealPresence Group system that you want to pair with.

   The pairing connection begins, and the Home screen displays when the pairing is successful.

Note: Disconnection from the RealPresence Group system does not hang up calls

If you unpair from the RealPresence Group 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**.

Note: Cannot pair as a dedicated device

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 Group system. An administrator can determine which device is paired and can unpair the device using the RealPresence Group system web interface. Go to **Admin Settings > General Settings > Pairing**. To unpair the device, select the **Forget this Device** link. Now you can pair a different device.

After the RealPresence Group system and the RealPresence Touch are paired, the Polycom RealPresence Group system web interface and the RealPresence Touch interface display information about each other and about their connection status.

Unpair the RealPresence Touch and a RealPresence Group System

You can unpair the RealPresence Touch and RealPresence Group system using the web interface.

To unpair the RealPresence Touch and Polycom RealPresence Group using the web interface:

1. Go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
2. Clear the check box next to **Enable Polycom Touch Device,** or click **Forget this Device**.
3. Click **Save**.

   The RealPresence Group system cannot pair with any RealPresence Touch while the **Enable Polycom Touch Device** check box is cleared.

RealPresence Touch Pairing and Connection States

The following table describes the pairing and connection states:

State	Description
Paired	The RealPresence Touch is successfully connected to the RealPresence Group system through the pairing process, including providing the RealPresence Group admin ID and password. Once systems are paired, an administrator can access the **Recently Paired** list and switch pairing between RealPresence Group systems without needing to enter admin IDs or passwords again.
Unpaired	The ability to pair or connect to the RealPresence Touch is disabled on the RealPresence Group system. The only way to unpair is to follow the procedure described in Unpair the RealPresence Touch and a RealPresence Group System.

State	Description
Connected	The RealPresence Touch has an active pairing connection to the RealPresence Group system. A single RealPresence Touch can be paired to multiple RealPresence Group systems, but can be connected to only one RealPresence Group system at a time.
Disconnected	The RealPresence Touch does not have an active pairing connection to a RealPresence Group system. However, the RealPresence Touch is still paired if at least one RealPresence Group system that has previously paired with the RealPresence Touch has not unpaired.

Pair and Unpair a Polycom Touch Control Device and a Polycom RealPresence Group System

When you configure the Polycom Touch Control to pair with a particular Polycom RealPresence Group system, the Polycom Touch Control makes an IP connection to the RealPresence Group system. If the connection is lost for any reason, the Polycom Touch Control automatically attempts to restore the connection.

The Polycom Touch Control connects to the RealPresence Group system over a TLS socket, providing a reliable, secure communication channel between the two systems. The Polycom Touch Control initiates all pairing connections and attaches to port 4122 on the RealPresence Group system.

You can pair the Polycom Touch Control and Polycom RealPresence Group system during initial Polycom Touch Control setup, as described in the steps on the previous page.

After you have completed Polycom Touch Control setup, you can pair to a different RealPresence Group system using Polycom Touch Control settings and unpair using the web interface.

When you use a Polycom Touch Control with the Polycom RealPresence Group system, you must be sure to update the RealPresence Group software before you update the Polycom Touch Control software. Only Polycom Touch Control software versions 4.x or later work with Polycom RealPresence Group systems.

The following table describes the pairing states:

State	Description
Paired	The Polycom Touch Control is successfully connected to the Polycom RealPresence Group system through the pairing process, including providing the Polycom RealPresence Group admin ID and password. A single Polycom Touch Control can be paired to multiple Polycom RealPresence Group systems and, once paired, the Polycom Touch Control can switch between RealPresence Group systems without needing to enter admin IDs or passwords.
Unpaired	The ability to pair or connect to the Polycom Touch Control is disabled on the Polycom RealPresence Group system. The only way to unpair is to follow the procedure described in Unpair the Polycom Touch Control and a RealPresence Group System.

State	Description
Connected	A Polycom Touch Control has an active pairing connection to the Polycom RealPresence Group system. A single Polycom Touch Control can be paired to multiple Polycom RealPresence Group systems, but can be connected to only one RealPresence Group system at a time.
Disconnected	The Polycom Touch Control does not have an active pairing connection to an RealPresence Group system, but is still paired if at least one RealPresence Group system that has previously paired with the Polycom Touch Control has not unpaired.

Pair the Polycom Touch Control and a RealPresence Group System

To pair the Polycom Touch Control and Polycom RealPresence Group system during setup:

- » After selecting a language, enter the RealPresence Group system IP address in the Polycom Touch Control interface and touch **Connect**.

Note: Pairing after setup

If you do not want to pair during setup, select **Pair Later**. If you choose to skip pairing, many Polycom Touch Control features are not available. You can pair at a later time.

To pair the Polycom Touch Control and Polycom RealPresence Group system after setup, using the Polycom Touch Control:

1. On the Polycom Touch Control Home screen, touch **System**.
2. Scroll to **Device Connection Status** and then touch Info next to the RealPresence Group system.
3. Touch **View Pairing Settings**.
4. Change the RealPresence Group system IP address and touch **Connect**.

To pair the Polycom Touch Control and Polycom RealPresence Group system after setup, using the Polycom RealPresence Group system web interface:

1. In the web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
2. Enable the **Enable Polycom Touch Device** setting.

After the RealPresence Group system and the Polycom Touch Control are paired, the Polycom RealPresence Group system web interface and the Polycom Touch Control interface display information about each other and about their connection status.

Unpair the Polycom Touch Control and a RealPresence Group System

You can unpair the Polycom Touch Control and RealPresence Group system using the web interface.

To unpair the Polycom Touch Control and Polycom RealPresence Group using the web interface:

1. Go to **Admin Settings > General Settings > Pairing > Polycom Touch Control**.
2. Disable **Allow Pairing** or select **Forget this Device**.

   The RealPresence Group system cannot pair with any Polycom Touch Control while Allow Pairing is disabled.

Customize the RealPresence Touch Home Screen

You can use the RealPresence Group system web interface to configure how information is displayed on the Home screen of the RealPresence Touch device. These settings are included in the RealPresence Group System settings profile, and included in bundled provisioning when using RealPresence Resource Manager.

To configure the RealPresence Touch Home Screen using the web interface:

1. In the web interface, go to **Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration**.
2. Configure the settings on the Home Screen Settings page that are described in the following sections.

Note: Enable Recent Calls and Speed Dial icons in the web interface

To enable the Recent Calls and Speed Dial icons, do the following:

- Recent Calls: Go to **Admin Settings > General Settings > System Settings > Recent Calls**. Select the **Enable Recent Calls** checkbox.
- Speed Dial: Go to **Admin Settings > General Settings > Home Screen Settings > Speed Dial**. Select the **Enable Speed Dial** checkbox.

Choose Icon Buttons That Display on the RealPresence Touch Home Screen

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.

To display the Home screen icons:

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.

Customize the Place a Call Screen Icon Buttons on the RealPresence Touch Device

You can customize the Place a Call screen to display certain icon buttons. Since there are four ways to place a call by default, after you tap the Place a Call button, all the options 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.

To customize the Place A Call screen icon buttons:

1 In the 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 Home screens.

Change the Home Screen Background Image on the RealPresence Touch Device

The RealPresence Touch Home screen displays a default background image that is similar to the “wallpaper” of a computer. You cannot delete this image, but you can upload your own background image to replace it. The same image also appears on the paired RealPresence Group system home screen.

Note: Background image size and format
Your background image must be a 1920 x 1080 pixels and in a JPEG format.

To upload and use a background image:

1. In the web interface, Go to **Admin Settings > General Settings > Home Screen Settings > Background.**
2. Click **Choose File** to select the image you want to upload.
3. When the image name appears next to **Choose File**, click **Upload**.

   The image now displays as the Home screen background.

Remote Management of the RealPresence Touch

You can remotely manage certain features of your RealPresence Touch. The following browsers are supported: Microsoft Internet Explorer, version 11; Google Chrome, version 41; Mozilla Firefox, version 37.

To open the remote management window for the RealPresence Touch:

1. In a web browser window, 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. You can return to the **Dashboard** by clicking the Home icon.

This list describes the features you can manage 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 Polycom RealPresence Group 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.

Remote Management of the Polycom Touch Control

You can remotely manage certain features of your Polycom Touch Control from within your enterprise environment using Microsoft Internet Explorer version 9 and higher.

To open the remote management window for the Touch Control:

1. In one of the supported web browser windows, enter the IP address of the Polycom Touch Control.

2 In the login window, enter the **ID** and **Password** you use to access the administrative features of the Polycom Touch Control.

   You can access the remote management features by using the **Dashboard** or the **Navigation** menu. You return to the **Dashboard** by clicking the Home icon.

This list describes the features you can manage remotely:

- **Download Logs**: Downloads the Polycom Touch Control 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 Polycom Touch Control become available on the web.
- **Pair**: Pairs and unpairs from Polycom RealPresence Group 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 Polycom Touch Control.
- **Software Updates**: Updates the Polycom Touch Control software. You can update from the default Polycom server or your own server by entering the appropriate IP address. You can configure the updates to occur automatically or manually.
- **View Polycom Touch Control Screens**: Shows the screen currently being displayed on the Polycom Touch Control. You can click **Refresh** at any time to see if the screen has changed.

Enable SmartPairing

SmartPairing allows you to detect and pair a RealPresence Group system from the RealPresence Mobile application on an Android or Apple iPad tablet. After you pair the application and the RealPresence Group system, you can use the RealPresence Mobile application to perform two basic functions:

- Use the application as a remote control for the RealPresence Group system.
- Swipe to transfer a call from the RealPresence Mobile application to the RealPresence Group system.

Be aware that telnet must be enabled before you can use SmartPairing. 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. **2** Send API command or use web interface.

To configure SmartPairing:

1 In the 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 RealPresence Group 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.

Note: Viewing paired devices
View paired devices in **Diagnostics > System > Sessions**.

Configure Contact Information

You can configure contact information for your Polycom RealPresence Group system so that others know who to call when they need assistance.

To configure system contact information:

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

Configure Regional Settings

You can configure regional settings for the Polycom RealPresence Group systems and for Polycom Touch Control devices. To do so, refer to Configure RealPresence Group System Location Settings and Configure Polycom Touch Control Regional Settings.

Configure RealPresence Group System Location Settings

To configure location settings:

1. In the 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.

Configure RealPresence Group System Language Settings

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

To configure the Polycom RealPresence Group system language settings:

» Do one of the following:

- In the local interface, go to **Settings > Administration > Location > Language** and select the language to use in the interface.
- In the web interface, go to **Admin Settings > General Settings > Language** and select the language to use in the interface.

Configure RealPresence Group System Date and Time Settings

To configure the Polycom RealPresence Group system date and time settings:

1. Go to one of the following locations to configure these settings:
   - In the local interface, go to **Settings > Administration > Location > Date and Time**.
   - In the 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.

Setting	Description
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 optional field.
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 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.

Configure Polycom Touch Control Regional Settings

To configure the Polycom Touch Control regional settings:

1 From the Home screen touch  **Administration.**

2 Touch the **Location** tab.

3 Select a language from the **Language** menu.

4 Configure the following settings under **Date and Time**.

Setting	Description
Time Zone	Specifies the time difference between GMT (Greenwich Mean Time) and your location.
Time Server	Specifies connection to a time server for automatic Touch Control time settings. The date and time must be manually reset every time the Touch Control restarts, in the following cases: • **Time Server** is set to **Off**. • **Time Server** is set to **Manual** or **Auto**, but the Touch Control cannot connect to a time server successfully.
Time Server Address	Specifies the address of the time server to use when **Time Server** is set to **Manual**.
Time Format	Specifies your format preference for the time display and lets you enter your local time.

Configure Sleep Settings

To configure when the system goes to sleep:

1. In the web interface, click **Admin Settings > Audio/Video > Sleep > Sleep**.
2. Select the number of minutes the system can be idle before it goes to sleep.

Diagnostics, Status, and Utilities

The Polycom RealPresence Group systems provide various tools and screens that allow you to review information about calls made by the system, review network usage and performance, perform audio and video tests, and send system messages. See the following topics for details:

- Polycom RealPresence Manageability Instrumentation Solution
- Diagnostics Screens
- Set Up System Logging
- Retrieve Log Files
- Call Detail Report (CDR)

Polycom RealPresence Manageability Instrumentation Solution

The Polycom® RealPresence® Manageability Instrumentation solution simplifies management of Polycom RealPresence video collaboration services.

Prior to the introduction of RealPresence Manageability Instrumentation, Simple Network Management Protocol (SNMP) Management Information Base (MIB) and Syslog formats varied across Polycom endpoint and infrastructure products. RealPresence Manageability Instrumentation now enables you to collect, store, and export data in a consistent format across all Polycom endpoints, and hardware and software infrastructure systems. Polycom video and collaboration environments and infrastructure that include the Manageability Instrumentation solution capabilities are easier to monitor, operate, and secure.

Specifically, RealPresence Manageability Instrumentation equips your Polycom devices with two embedded capabilities that enhance your ability to monitor them:

- The Polycom Unified Simple Network Management Protocol (SNMP) Management Information Base (MIB) provides a consistent and unified data model and common format for all MIBs across Polycom products. The new MIB enables you to translate data you collect with SNMP into a standardized format so you can remotely monitor devices on a network. For more information setting up SNMP on the system, see Set Up SNMP.
- The Polycom Unified System logging Syslog transport format provides a system log message format compliant with RFC 5424 that enables you to log device events locally and remotely in a standardized way. Monitoring system logs is especially useful for troubleshooting and security purposes. For more information on setting up system logging, see Configure System Log Level and Remote Logging.

For detailed information on using the Manageability Instrumentation solution with your Polycom products, see the *Polycom RealPresence Manageability Instrumentation Solution Guide*.

Diagnostics Screens

Use the system diagnostics screens to view call statistics, system status, and system log settings, as well as download system logs and restart or reset the system.

Local Interface System Screens

Most diagnostic information is available in both the web and the local interface, but some of this information is specific to one or the other interface. Read this section to learn how to find diagnostic information in the local interface.

To access the Diagnostics screens on the local interface:

» Go to **Settings > System Information.**

The local interface System Information screen has the following choices:

- Information
- Status
- Diagnostics
- Call Statistics

Information

Diagnostic Screen	Description
System Detail	Displays the following system information: • System Name • Model • Hardware Version • System Software • Serial Number • MAC Address • IP Address

Diagnostic Screen	Description
Network	Displays the following network information: • IP Address • Host Name • H.323 Name • H.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

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 the microphones, SoundStation IP, and SoundStructure.
EagleEye Director	Displays the connection status of the EagleEye™ Director, if one is connected. If the camera system is not connected or is not selected as the current camera source, 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. When a system device or service encounters a problem, you see an alert next to the **System** button on the menu.

Diagnostics

Diagnostic Screen	Description
Near End Loop	Tests the internal audio encoders and decoders, the external microphones and speakers, the internal video encoders and decoders, and the external 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 Polycom RealPresence Group 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 Polycom RealPresence Group 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.
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 Polycom RealPresence Group system web interface during a call, the people at the site you are testing will hear the tone, but you will not.
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. • To check the microphone or microphones, speak into the microphone. • 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. The Audio Meters indicate peak signal levels. Set signal levels so that you see peaks between +3dB and +7dB with normal speech and program material. Occasional peaks of +12dB to +16dB with loud transient noises are considered acceptable. A meter reading of +20dB corresponds to 0dBFS in the Polycom RealPresence Group system audio. A signal at this level is likely clipping the audio system. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the Polycom RealPresence Group 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.
Sessions	Displays the following information about each session connected to the system: • Type • User ID • Remote Address
Reset System	Returns the system to its default settings. When you select this setting using the remote control, you have the option to 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). You might want to download the CDR and CDR archive before you reset the system. Refer to Call Detail Report (CDR). **Note:** If a room password is configured for the admin account, you must enter it to reset the system.

Web Interface Diagnostics Screens

Call statistics are displayed in one format when you are in point-to-point calls and another when you are in multipoint calls. Most diagnostic information is available in both the web and the local interface, but some of this information is specific to one or the other interface. Read this section to learn how to find diagnostic information in the web interface.

Note: Diagnostics for EagleEye Director

If an EagleEye Director camera system is connected to your RealPresence Group system but is not selected as the current camera source, the Diagnostics selection is not available in the left navigation panel. To view the Diagnostics selection, ensure that the EagleEye Director is selected as the current camera source.

To access the Diagnostics screens using the Polycom RealPresence Group system web interface:

1. In your web browser address line, enter the RealPresence Group system's IP address.
2. Enter the Admin ID as the user name (default is `admin`), and enter the Admin Remote Access Password, if one is set.
3. Click **Diagnostics** from any page in the web interface.

You can find some system information by clicking the **System** link in the blue bar at the top of the page.

The web interface's Diagnostics page has the following groups of settings in addition to the Send a Message application:

- System
- Audio and Video Tests

System Diagnostics

Diagnostic Screen	Description

Call Statistics	Displays information about the call in progress. What you see depends on whether you are in a point-to-point or multipoint call.
	• **Point-point calls:** 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 Info**. From an individual stream view you can select **Next Stream** to view the next stream in the stream list.
	• **Multipoint calls:** A list of participants in the call is displayed. Do one of the following:
	  ⅄ To view a participant's details, select **Participants**, navigate to the desired participant, and select **More Info**.
	  ⅄ The participants' active streams are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and select **More Info**. 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 option is available in SVC calls only). Select the desired stream, and select **More Info**.
	If the system is not in a call, the page displays **The System is not currently in a call**.

System Status	Displays the following system status information:
	• Auto-Answer Point-to-Point Video, Remote Control, and Meeting Password
	• Microphones, SoundStation IP, SoundStructure
	• IP Network
	• Servers:
	  ⅄ Always shows: Gatekeeper, SIP Registrar Server
	  ⅄ Shows the active Global Directory Server, LDAP Server, or Microsoft Server
	  ⅄ If enabled, shows Provisioning Service, Calendaring Service, Presence Service
	If the Polycom RealPresence Group system detects an EagleEye Director, a status line for the device is displayed.

Download Logs	Enables you to save system log information.

Diagnostic Screen	Description
System Log Settings	• Specifies the Log Level to use. • Enables Remote Logging, H.323 Trace, and SIP Trace. • Specifies the Remote Log Server Address. • Allows you to Send Diagnostics and Usage Data to Polycom, and get information about the Polycom Improvement Program.
Restart System	Instructs the system to restart (system reboot).
Sessions	View information about everyone logged in to the RealPresence Group system.

The following table describes the information you see when you click **More Info** on the Call Statistics page.

Call Statistics “More Info”
Participant information • System name • System number • System information • Call speed (send and receive) • Call type • Encryption **Participant streams** • Stream ID; possible stream IDs include Audio TX, Audio RX, Video TX, Video RX, Content TX, and Content RX • Stream quality indicator; possible colors are green, yellow, and red. • Protocol in use • Format in use • Data rate in use • Frame rate in use • Number of packets lost and percentage packet loss in IP calls • Jitter in IP calls • Encryption type, key exchange algorithm type, and key exchange check code (if the encryption option is enabled and the call is encrypted) • Error concealment type, such as lost packet recovery (LPR), retransmission, or dynamic bandwidth allocation (DBA)

View Call Statistics on the RealPresence Touch

When your RealPresence Group 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.

To view call statistics about a call in progress:

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**.

View Call Statistics Using the Polycom Touch Control

Call statistics are also available during a call when your system is paired with the Polycom Touch Control.

To view information about a point-to-point call in progress:

1 Touch **Participants**.

Participant information is displayed.

2 Touch **View 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 touch . From an individual stream view you can touch **Next Stream** to view the next stream in the list.

To view information about a multipoint call in progress:

1 Touch **Participants**.

A list of participants in the call is displayed.

2 Touch **View Call Statistics** and do one of the following:

- To view a participant's details, navigate to the desired participant, and touch .
- 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 . 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 option is available in SVC calls only). Select the desired stream, and touch .

Audio and Video Tests

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 RealPresence Group system web interface during a call, the people at the site you are testing will hear the tone, but you will not.
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. • To check the microphone or microphones, speak into the microphone. • 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. The Audio Meters indicate peak signal levels. Set signal levels so that you see peaks between +3dB and +7dB with normal speech and program material. Occasional peaks of +12dB to +16dB with loud transient noises are considered acceptable. A meter reading of +20dB corresponds to 0dBFS in the Polycom RealPresence Group system audio. A signal at this level is likely clipping the audio system. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the Polycom RealPresence Group system.
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.

Set Up System Logging

System log files are essential when troubleshooting system issues. System log files contain information about system activities and the system configuration profile.

In order to set up system logging, you need to do the following tasks:

- Configure System Log Management
- Configure System Log Level and Remote Logging

After setting up system logging, you can retrieve a system log file. For details on how to get log files, refer to Retrieve Log Files.

Configure System Log Management

When the 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

To view the log file status, do one of the following:

- In the local interface, go to **Settings > System Information > Status > Log Management**.
- In the web interface, go to **Diagnostics > System > System Status** and select the **More Info** link for **Log Threshold**.

Note: Log threshold status when red

When the Log Threshold system status indicator is red, automatic log transfers cannot be completed and data may be lost. You must manually transfer the logs to a USB device.

To configure system log management:

1. In the 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**—Optional folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.
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 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.

To configure system log settings:

1. In the 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 Polycom RealPresence Group 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 Polycom RealPresence Group system to send each log message to the specified server in addition to logging it locally. The system immediately begins forwarding its log messages when 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.
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 optional destination port number in the range 1..65535) • **IPv6 Address** (Example: [2001::abcd:1234]:<port>, where <port> is the optional destination port number in the range 1..65535) • **FQDN** (Example: logserverhost.company.com:<port>, where <port> is the optional 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.

Setting	Description
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.

Retrieve Log Files

There are several types of log files available that you might find useful when troubleshooting. Log files exist for the RealPresence Group system, RealPresence Touch, Polycom Touch Control, and EagleEye Director. These sections explain how to retrieve those different log files:

- Download or Transfer System Log Files
- Transfer RealPresence Touch Logs to a USB Storage Device
- Transfer Polycom Touch Control Logs
- Transfer EagleEye Director Logs

Download or Transfer System Log Files

You can use the RealPresence Group system web interface or local interface to get system logs.

Note: Log entry times are GMT
The date and time of system log entries for RealPresence Group systems are shown in GMT.

To download a system log using the web interface:

1. Click **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.

To transfer a system log using the local interface:

1. In the local interface, go to **Settings > Administration > Security > Log Management**.
2. Click **Transfer System Log to USB Device**.
3. The system saves a file in the USB named according to the settings you chose in the web interface.
4. Wait until the system displays a message that the log transfer has completed successfully before you remove the storage device.

Transfer RealPresence Touch Logs to a USB Storage Device

You might need to transfer logs from the RealPresence Touch to a USB storage device.

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**.

Note: Format for the USB storage device
The USB storage device must be in FAT32 format.

Transfer Polycom Touch Control Logs

You can transfer the Touch Control logs to an external USB storage device.

To transfer Polycom Touch Control logs:

1 Ensure that a USB device is connected to the USB port on the right side of the Polycom Touch Control.

2 From the Home screen touch **Administration.**

An admin ID and password might be configured for the Touch Control Administration settings. The default ID is `admin` and the default password is `456`.

3 Under **Security**, select **Transfer Touch Control Logs to USB Device**.

A popup message displays when the log transfer completes successfully.

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 Group system.

To download the log information to a USB device:

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.

Call Detail Report (CDR)

When enabled by going to **Admin Settings > General Settings > System Settings > Recent Calls** in the Polycom RealPresence Group system web interface, the Call Detail Report (CDR) provides the 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 is virtually unlimited, but 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 might set up a schedule to download and save the CDR after about every 1000 - 2000 calls just to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads.

To download the CDR using the web interface:

1. 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.

Information in the CDR

The following table describes the data fields in the CDR.

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 the 24-hour format hh:mm:ss.
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.

Data	Description
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).
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 H.323 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 H.323 call. However, it does report an average of the sampled values.
Average Packets Lost (Tx)	The number of packets transmitted that were lost during an H.323 call.
Average Packets Lost (Rx)	The number of packets from the far site that were lost during an H.323 call.

Data	Description
Average Latency (Tx)	The average latency of packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Average Latency (Rx)	The average latency of packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Maximum Latency (Tx)	The maximum latency for packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Maximum Latency (Rx)	The maximum latency for packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Average Jitter (Tx)	The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Average Jitter (Rx)	The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.
Maximum Jitter (Tx)	The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Maximum Jitter (Rx)	The maximum jitter of packets received during an H.323 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).

Note: Screen saver when paired

When the Polycom RealPresence Group system is paired with a Polycom Touch Control, the screen saver logo displays on the system monitor but not the Polycom Touch Control screen.

Troubleshoot

General Troubleshooting

The following table provides general troubleshooting information, including symptoms, problems and possible solutions.

Symptom	Problem	Solution
The RealPresence Group 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 or Polycom Touch Control, 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.
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.
When using two monitors, the second monitor is blank.	The room system is not configured for more than one monitor.	Go to **Admin Settings > Monitors** and configure the second monitor to **Auto** or **Manual**.
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.

Place 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 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 Polycom RealPresence Group 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.

View RealPresence Group System Details on the Local Interface

You might need to view certain 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.

To view your system details with the remote control:

» Select **>** > **Information**. The following details display:

- System Name
- Model
- Hardware Version
- System Software
- Serial Number
- MAC Address
- IP Address

System Information, Status, and Diagnostics Information on the Local Interface

You can review information about calls, network usage, and performance on the various RealPresence Group systems screens on the local interface.

The System Information screen has the following choices:

- Information

- Status
- Diagnostics
- Call Statistics (in a call only)

Note: Available system menus vary
Available system menus vary based on how your administrator configured the system. Therefore, this section might cover options that you cannot access on your system. To find out more about these options, please talk to your administrator.

Access the Information Screen

To access the Information screen:

» Go to > **System Information** > **Information.**

Information 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 • H.323 Name • H.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

To access the Status screen:

. Go to > **System Information** > **Status.**

Out of Call Status Information

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 either out of a call or in 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, SoundStation IP, and SoundStructure.
EagleEye Director	Displays the connection status of the EagleEye Director, if one is connected. If the camera system is not connected, this choice is not visible on the screen.
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. Your administrator can download system logs, call detail reports, and configuration profiles using the web interface.

In a Call Status Information

There are a couple of things to remember about the In a Call status information:

- If the Polycom RealPresence Group system detects an EagleEye Director, a status line for the device is displayed.
- 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. For more information on this screen, refer to View Call Statistics for an Active Point-to-Point Call with the Remote Control.

Access the System Diagnostics Screen on the Local Interface

To access information about your system diagnostics:

» Select  > **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 Polycom RealPresence Group 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 Polycom RealPresence Group 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.
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. • To check the microphone or microphones, speak into the microphone. • 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. The Audio Meters indicate peak signal levels. Set signal levels so that you see peaks between +3dB and +7dB with normal speech and program material. Occasional peaks of +12dB to +16dB with loud transient noises are considered acceptable. A meter reading of +20dB corresponds to 0dBFS in the Polycom RealPresence Group system audio. A signal at this level is likely clipping the audio system. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the Polycom RealPresence Group system.

Diagnostic Screen	Description
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.
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 RealPresence Group 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 have the option to 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.

View RealPresence Group System Details

You might need to view certain system details to do video conferencing tasks, such as pairing, or to perform troubleshooting tests to provide information for your own testing or for technical support.

To view your system details with the remote control:

» Select **>** > **Information**. The following details display:

- System Name
- Model

- Hardware Version
- System Software
- Serial Number
- MAC Address
- IP Address

View System Details and Connection Status on the RealPresence Touch

You can view certain system details about the paired RealPresence Group system on the RealPresence Touch; this information might be useful for troubleshooting or for technical support.

To view system details and connection status:

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 Polycom Touch Control System Details

You might need to view certain system details to do video conferencing tasks, such as pairing, or to perform troubleshooting tests to provide information for your own testing or for technical support.

To view your Polycom Touch Control system details:

1. On the Home screen, touch **System**. The following Touch Control information displays:
   - Model
   - Hardware Version
   - Serial Number
   - Panel Software
   - Operating System Version
   - Kernel Version
   - MAC Address
   - IP Address
2. To view the paired RealPresence Group system details, touch the **<Product Name> System** tab.

System Information, Status, and Diagnostics Information

You can review information about calls, network usage, and performance on the various RealPresence Group systems screens on the local interface.

The System Information screen has the following choices:

- Information
- Status
- Diagnostics
- Call Statistics (in a call only)

Note: Available system menus vary

Available system menus vary based on how your administrator configured the system. Therefore, this section might cover options that you cannot access on your system. To find out more about these options, please talk to your administrator.

Access the Information Screen

To access the Information screen:

» Go to  > **System Information** > **Information.**

Information Screen	Description
System Detail	Displays the following system information: • System Name • Model • Hardware Version • System Software • Serial Number • MAC Address • IP Address

Information Screen	Description
Network	Displays the following network information: • IP Address • Host Name • H.323 Name • H.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

To access the Status screen:

1. Go to > **System Information** > **Status.**

Out of Call Status Information

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 either out of a call or in 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, SoundStation IP, and SoundStructure.
EagleEye Director	Displays the connection status of the EagleEye Director, if one is connected. If the camera system is not connected, this choice is not visible on the screen.
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.

Status Screen	Description
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. Your administrator can download system logs, call detail reports, and configuration profiles using the web interface.

In a Call Status Information

There are a couple of things to remember about the In a Call status information:

- If the Polycom RealPresence Group system detects an EagleEye Director, a status line for the device is displayed.
- 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. For more information on this screen, refer to View Call Statistics for an Active Point-to-Point Call with the Remote Control.

Access the System Diagnostics Screen

To access information about your system diagnostics:

» Select > **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 Polycom RealPresence Group 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 Polycom RealPresence Group system lists the hops between the system and the IP address you entered.

Diagnostic Screen	Description
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.
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. • To check the microphone or microphones, speak into the microphone. • 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. The Audio Meters indicate peak signal levels. Set signal levels so that you see peaks between +3dB and +7dB with normal speech and program material. Occasional peaks of +12dB to +16dB with loud transient noises are considered acceptable. A meter reading of +20dB corresponds to 0dBFS in the Polycom RealPresence Group system audio. A signal at this level is likely clipping the audio system. Meters function only when the associated input is enabled. **Note:** Some audio meters are unavailable when a SoundStructure digital mixer is connected to the Polycom RealPresence Group 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 RealPresence Group 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 have the option to 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.

Call Statistics on the RealPresence Group System Local Interface

You might need to view call statistics on the local interface to do some troubleshooting for users.

View Call Statistics for an Active Point-to-Point Call with the Remote Control

During a point-to-point call, you can view call statistics about a call participant or about an active stream.

> **User Tip: Shortcut to Call Statistics screen**
> 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.

To view information about a point-to-point call in progress:

» 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 multipoint call, you can view call statistics about any of the call participants or about an active stream.

To view information about a multipoint call in progress:

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 Point-to-Point Call with the Touch Control

During a point-to-point call, you can view call statistics about a call participant or about an active stream.

To view information about a point-to-point call in progress:

1. Touch **Participants**.Participant information displays.
2. Touch **View 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 touch . From an individual stream view you can touch **Next Stream** to view the next stream in the list.

View Call Statistics for an Active Multipoint Call with the Touch Control

During a multipoint call, you can view call statistics about any of the call participants or about an active stream.

To view information about a multipoint call in progress:

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 .
   - 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 . 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 option is available in SVC calls only. Select the desired stream and touch .

Reset a RealPresence Group System

If the 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 one:

- Current software version
- Remote control channel ID setting
- Directory entries
- CDR data and logs

To reset the system using the local interface:

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 Polycom RealPresence Group System

If the RealPresence Group system is not functioning correctly or you have forgotten the Administration password, 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 *not* saved:

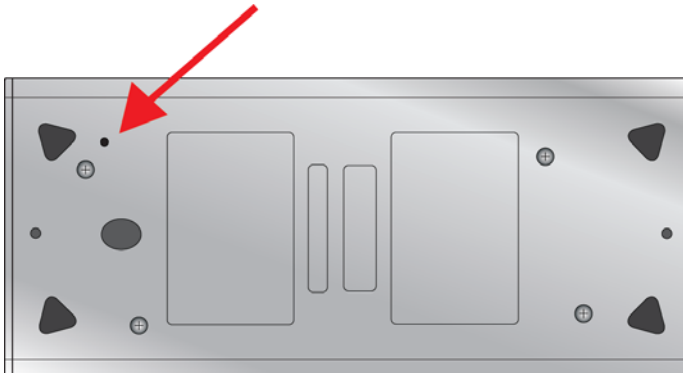
- Software updates
- All system settings including option keys and the remote control channel ID
- Directory entries
- CDR data

During a factory restore on the system or from a USB device, the LED indicator on the front of the system blinks blue and amber.

Use the Restore Button for a Factory Restore

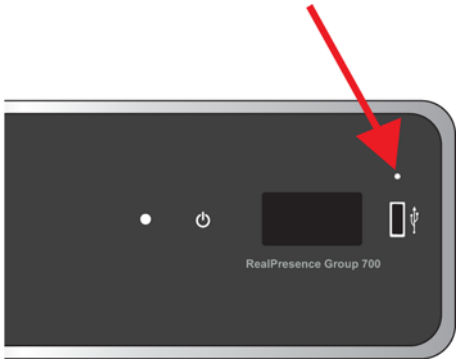
The restore button pinhole is on the bottom of the Polycom RealPresence Group 300, 310, and 500 systems, as shown in the following figure.

Restore button on RealPresence Group 300/310/500 systems



The restore button pinhole is on the front of the Polycom RealPresence Group 700 system, as shown in the following figure.

Restore button on RealPresence Group 700 system



To reset the system to its factory partition software using the restore button:

1. Power off the system.
2. Straighten a paper clip and insert it into the pinhole.
3. Using the paper clip, press and hold the restore button.
4. While continuing to hold the restore button, press the power button once.
5. Keep holding the restore button for 10 more seconds, then release it.

During the factory restore process, the system displays the Polycom startup screen and the usual software update screens on HDMI monitors. Other types of monitors will be blank. Do not power off the system during the factory restore process. The system restarts automatically when the process is complete.

Use a USB Storage Device for a Factory Restore

If you start a factory restore while a USB storage device is connected, the system restores from the USB device instead of the system's factory partition.

For about the first five minutes of the factory restore process, the system is erasing data on the SD card and extracting data from the USB device. This process runs from a special memory partition and graphics are not available, so your monitor will be blank.

If you prefer, you can have the system prepare the SD card by rewriting the data with zeroes and reformatting the card, thereby eliminating any traces of old data. Be aware that this step adds about 20 minutes to the beginning of the factory restore process, when all you will see is a blank screen. You will notice, however, that the LED indicator shows a fast blink of blue and amber lights during this process. The lights blink normally during the rest of the restore process.

To reset the system to its factory partition software using a USB device:

1. Copy the build package (`.tar` file) and the `sw_keys.txt` file to the root directory of a USB device.
2. (Optional) Create a text file named `zeroize.txt` on the root directory of the USB device, then edit the file by entering the word `TRUE` in all capital letters.

   If the `zeroize.txt` file contains the word FALSE, or if the file is not in the root directory of the USB device, the system uses the standard method of erasing data from the SD card.
3. Power down the system and plug the USB device into your system.
4. While holding the restore button, press the power button once.
5. Keep holding the restore button for 10 more seconds, then release it.

   The software version of the update file on the USB device is displayed in the web interface.
6. Click **Start Update** to begin the factory restore.

After the SD card is prepared, the system displays the Polycom startup screen and the usual software update screens on HDMI monitors. Other types of monitors will be blank. Do not power off the system during the factory restore process. The system restarts automatically when the process is complete.

Delete Files

You can remove customer data and configuration information from the system for security purposes.

To perform a logical delete of the system files:

1. Power off the systems by holding down the Power sensor for 3 to 5 seconds. Unplug all network connections.
2. Perform a factory restore.
3. Wait for the system to start up and display the setup wizard.
4. Power off the system.

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 software.

The restore button pinhole is on the back of the RealPresence Touch, as shown in the following figure.

Restore button on the RealPresence Touch Device

Perform Factory Restore

You can perform a a factory restore on the RealPresence Touch device to reinstall the default platform and applications. Do not power off the device during the factory restore process.

To perform a factory restore:

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 Factory Restore with 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.

To perform a factory restore with a USB Storage Device:

1. Copy a build package (`.tar` 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 RealPresence Touch.
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.

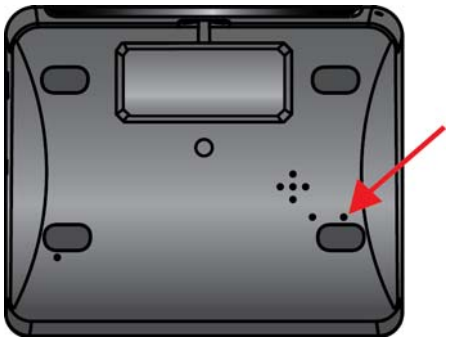
   When the process is complete, the device displays the splash screen and then the home screen.

Perform a Factory Restore on the Polycom Touch Control

If the Polycom Touch Control is not functioning correctly or you have forgotten the Administration password, you can use the restore button to reset the device. This operation completely erases the device's settings and reinstalls the software.

The restore button is on the underside of the Polycom Touch Control, as shown in the following figure.

Restore button on the Polycom Touch Control



To reset the Polycom Touch Control using the restore button:

1. Power off the Polycom Touch Control.
2. Disconnect the LAN cable.
3. Disconnect all USB devices.
4. Press and hold the factory restore button while you reconnect the LAN cable to the device. Continue to hold the factory restore button down for about 10 seconds after the device powers on.

If the device requires login information, the default for the admin ID is `admin` and for the password is `456`.

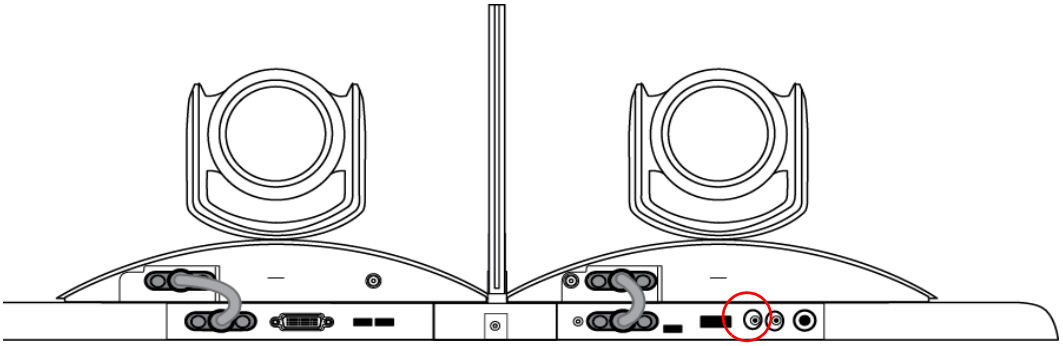
During the factory restore process, the default platform and applications are reinstalled. Do not power off the device during the factory restore process. The device displays a success message when the process is complete.

Perform a Factory Restore on the Polycom EagleEye Director

If the Polycom 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.

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

Restore button on the Polycom EagleEye Director



To reset the Polycom EagleEye Director using the restore button:

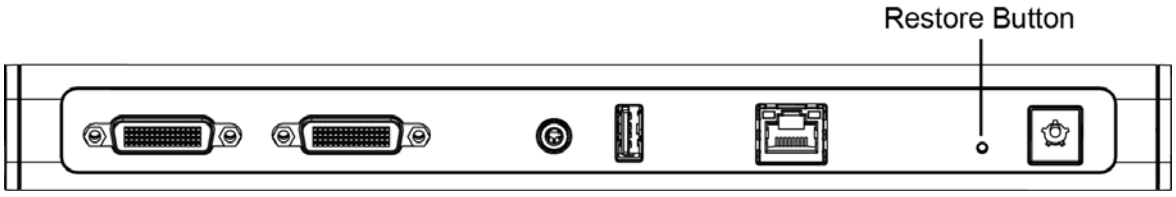
1. Press and hold the restore button on the back of the EagleEye Director for 2-3 seconds while the power light cycles.

   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.

Note: Leave EagleEye Director on while restoring
Be sure to keep the Polycom EagleEye Director powered on during the factory restore.

Perform a Factory Restore on the EagleEye Producer

You can use the hardware restore button on the EagleEye Producer system to perform a factory restore of the 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.



Note: Do not power off.
Do not power off the EagleEye Producer during the factory restore process.

To perform a factory restore:

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. For details, refer to Adjust the Room View.

Find Your System IP Address

You can find your RealPresence Group system's IP address in the local or the web interfaces:

- In the local interface, navigate to **Settings > Administration > LAN Properties: IP Address.**
- In the local interface, if the administrator has configured the system to show the IP address, view the top of the menu that is displayed when you press  with the remote control and on the Home screen.
- In the web interface, you can find it on the upper left of the Home page banner, just under the company logo.

Knowledge Base

For more troubleshooting information, you can search the Knowledge Base at support.polycom.com.

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 support.polycom.com.

Enter the following information about your RealPresence group 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 Group system.

» To locate the system serial number (14 digits), go to  > **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 Group system.

» To locate the software version, go to  > **System Information** > **Information** > **System Detail**.

Locate Active Alert Messages

You can view the active alert messages on the local interface of the RealPresence Group system.

» To locate the active alert messages, go to  > **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 Group system.

» To locate the IP Address and H.323 Extension settings, go to > **System Information** > **Information** > **Network**.

Locate the LAN Status

You can view the LAN status on the local interface of the RealPresence Group system.

» To locate LAN status, go to > **System Information** >**Status** > **LAN**.

Locate Diagnostics

You can view diagnostics on the local interface of the RealPresence Group system.

To locate Diagnostics, go to > **System Information** > **Diagnostics**.

How to Contact 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.

To contact Polycom Technical Support, go to support.polycom.com.

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

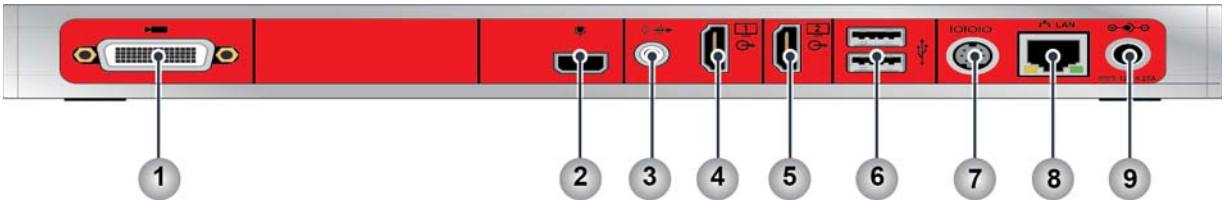
You can find the system detail information in the local interface by going to **Settings > System Information > Information** or in the web interface by clicking **System** in the blue bar at the top of the web interface page.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components 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, and Microsoft Lync Server 2013 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 Back Panel Views

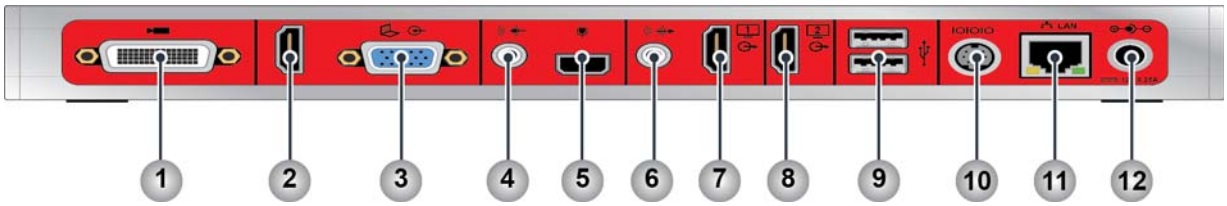
Polycom RealPresence Group 300 System



Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
1	Audio/Video > Video Inputs > Input 1	Video Input	HDCI	Input for the camera
2	N/A	Microphone Input	Polycom Microphone	Audio input for up to two Polycom microphone arrays or a SoundStation IP 7000 speaker phone or SoundStructure mixer
3	Audio/Video > Audio > Audio Output	Audio Output	3.5mm Stereo	Audio output for main monitor audio or external speaker system System tones and sound effects + Audio from the far site +
4	Audio/Video > Monitors > Monitor 1	Video Output 1	HDMI	Output for Monitor 1
5	Audio/Video > Monitors > Monitor 2	Video Output 2	HDMI	Output for Monitor 2 (available only with a monitor option key)
6	N/A	USB Connectors	USB 2.0	USB for Software Update, remote control battery charging
7	General Settings > Serial Ports	Serial Port	RS-232	Serial port

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
8	Network > LAN Properties	LAN Port	Ethernet	Connectivity for IP and SIP calls, People+Content IP, and the system web interface
9	N/A	Power Input	12 V 6.25 A	Power input

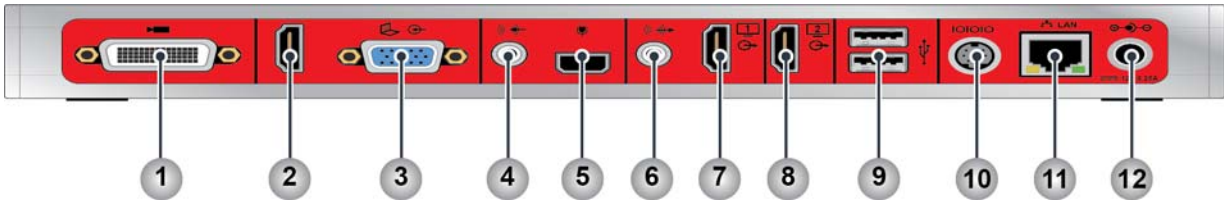
Polycom RealPresence Group 310 System



Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
1	Audio/Video > Video Inputs > Input 1	Video Input 1	HDCI	Input for Camera 1
2	Audio/Video > Video Inputs > Input 2 Audio/Video > Audio > Audio Input > Type: HDMI	Video Input 2/ Audio Input 1	HDMI	Auxiliary video and audio input
3	Audio/Video > Video Inputs > Input 2	Video Input 2	VGA	Video input for Content
Note: Use either the HDMI or VGA video input, but not both.				
4	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
5	N/A	Microphone Input	Polycom Microphone	Audio input for up to two Polycom microphone arrays or a SoundStation IP 7000 speaker phone or SoundStructure mixer

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
6	Audio/Video > Audio > Audio Output	Audio Output 1	3.5mm Stereo	Audio output for main monitor audio or external speaker system Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio connected to audio input 2 when associated with video input 2
7	Audio/Video > Monitors > Monitor 1	Video Output 1	HDMI with embedded audio DVI-D	Output for Monitor 1 When format is HDMI, audio output for main monitor audio Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio connected to audio input 2 when associated with video input 2
8	Audio/Video > Monitors > Monitor 2	Video Output 2	HDMI DVI-D	Output for Monitor 2; does not include embedded audio **NOTE**: RealPresence Group 310 systems require a dual monitor option key to allow dual monitor output.
9	N/A	USB Connectors	USB 2.0	USB for software update, remote control battery charging
10	General Settings > Serial Ports	Serial Port	RS-232	Serial port
11	Network > LAN Properties	LAN Port	Ethernet	Connectivity for IP calls, People+Content IP, and the system web interface
12	N/A	Power Input	12 V 6.25 A	Power input

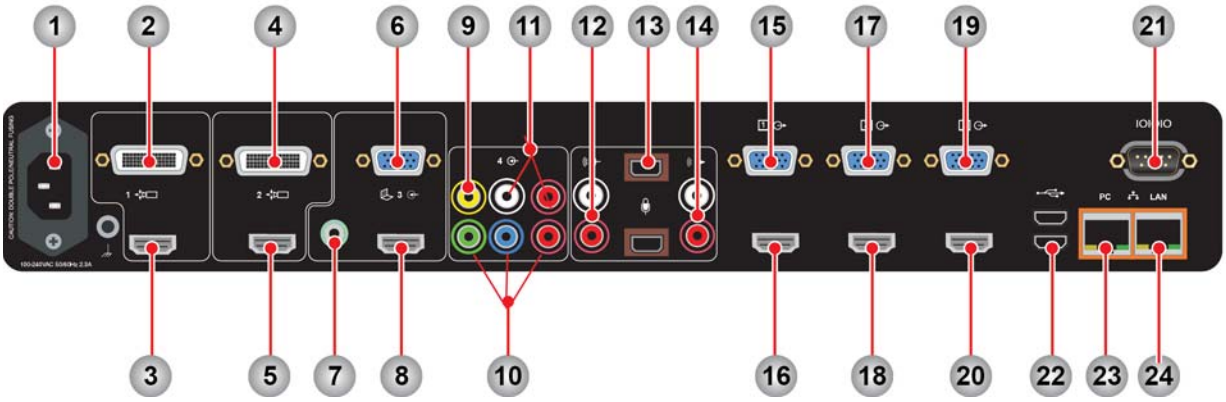
Polycom RealPresence Group 500 System



Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
1	Audio/Video > Video Inputs > Input 1	Video Input 1	HDCI	Input for Camera 1
2	Audio/Video > Video Inputs > Input 2 Audio/Video > Audio > Audio Input > Type: HDMI	Video Input 2/ Audio Input 1	HDMI	Auxiliary video and audio input
3	Audio/Video > Video Inputs > Input 2	Video Input 2	VGA	Video input for Content
Note: Use either the HDMI or VGA video input, but not both.				
4	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
5	N/A	Microphone Input	Polycom Microphone	Audio input for up to two Polycom microphone arrays or a SoundStation IP 7000 speaker phone or SoundStructure mixer
6	Audio/Video > Audio > Audio Output	Audio Output 1	3.5mm Stereo	Audio output for main monitor audio or external speaker system Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio connected to audio input 2 when associated with video input 2
7	Audio/Video > Monitors > Monitor 1	Video Output 1	HDMI with embedded audio DVI-D	Output for Monitor 1 When format is HDMI, audio output for main monitor audio Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio connected to audio input 2 when associated with video input 2
8	Audio/Video > Monitors > Monitor 2	Video Output 2	HDMI DVI-D	Output for Monitor 2; does not include embedded audio
9	N/A	USB Connectors	USB 2.0	USB for Software Update, remote control battery charging

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
10	General Settings > Serial Ports	Serial Port	RS-232	Serial port
11	Network > LAN Properties	LAN Port	Ethernet	Connectivity for IP calls, People+Content IP, and the system web interface
12	N/A	Power Input	12 V 6.25 A	Power input

Polycom RealPresence Group 700 System



Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
1	N/A	Power Input	100-240 VAC 2.3 A	Power input
2	Audio/Video > Video Inputs > Input 1	Video Input 1	HDCI	Input for Camera 1
3	Audio/Video > Video Inputs > Input 1	Video Input 1	HDMI	Input for Camera 1
4	Audio/Video > Video Inputs > Input 2	Video Input 2	HDCI	Input for Camera 2
5	Audio/Video > Video Inputs > Input 2	Video Input 2	HDMI	Input for Camera 2

Note: Use either the HDCI or HDMI for video inputs 1 and 2, but not both.

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
6	Audio/Video > Video Inputs > Input 3	Video Input 3	VGA	Video input associated with audio input 3
7	Audio/Video > Audio > Audio Input > Type: 3.5mm	Audio Input 3	3.5mm Stereo	Audio input for stereo line-level Audio is included in local audio mix when video source is selected 3.5mm audio is independent and not associated with any video input
8	Audio/Video > Video Inputs > Input 3	Video Input 3	HDMI	Video and audio input
Note: Use either the HDMI or VGA for video input 3, but not both.				
9	Audio/Video > Video Inputs > Input 4	Video Input 4	Composite Video	Video input Associated with audio input 4 (audio is disabled until video input 4 is selected)
10	Audio/Video > Video Inputs > Input 4	Video Input 4	Component Video	Video input associated with audio input 4 (audio is disabled until video input 4 is selected)
11	Audio/Video > Audio > Audio Input > Type: Component	Audio Input 4	RCA	Associated with video input 4 Inactive until video input is selected Audio is included in local audio mix when video source is selected
Note: Use either the Composite/RCA or Component for input 4, but not both.				
12	Audio/Video > Audio > Audio Input > Type: Line	Audio Input 2	RCA	Auxiliary audio input Intended as microphone input; sent to far end only
13	N/A	Audio Input 1	Polycom Microphone	Audio input for up to three Polycom microphone arrays or a SoundStation IP 7000 speaker phone or SoundStructure mixer
14	N/A	Audio Output 2	RCA	Audio output for main monitor audio Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio input from audio inputs 3 and 4 when associated video is selected
15	Audio/Video > Monitors > Monitor 1	Video Output 1	VGA	Output for Monitor 1

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
16	Audio/Video > Monitors > Monitor 1	Video Output 1 Audio Output 1	HDMI	Output for Monitor 1 Audio Mix Routed to the Output: System tones and sound effects + Audio from the far site + Audio input from audio inputs 3 and 4 when associated video is selected
17	Audio/Video > Monitors > Monitor 2	Video Output 2	VGA	Output for Monitor 2
18	Audio/Video > Monitors > Monitor 2	Video Output 2	HDMI	Output for Monitor 2
19	Audio/Video > Monitors > Monitor 3	Video Output 3	VGA	Output for Monitor 3
20	Audio/Video > Monitors > Monitor 3	Video Output 3	HDMI	Output for Monitor 3
Note: Use either the HDMI or VGA for video outputs 1, 2, and 3, but not both.				
21	General Settings > Serial Ports	Serial Port	RS-232	Serial port
22	N/A	USB Connectors	USB 3.0	USB for Software Update, remote control battery charging
23	Network > LAN Properties > LAN Options	PC LAN Port	Ethernet	Ethernet switch port
24	Network > LAN Properties	LAN Port	Ethernet	Connectivity for IP calls, People+Content IP, and the system web interface

Port Usage

You might need port usage information when you configure your network equipment for video conferencing. The following tables show IP port usage to and from RealPresence Group systems.

Connections to RealPresence Group Systems

Connections to RealPresence Group Systems

Inbound Port	Type	Protocol	Function	Configuration		
				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
22	Static	TCP	Polycom Touch Control over SSH	Yes	Admin Settings > General Settings > Pairing > Polycom Touch Control > Enable Polycom Touch Device	No
23	Static	TCP	Telnet Diagnostics	No	Admin Settings > Security > Global Security > Access > Enable Telnet Access	No
24	Static	TCP	Polycom API	No	Admin Settings > Security > Global Security > Access > Enable Telnet Access	No
80	Static	TCP	RealPresence Group Web UI 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)

Connections to RealPresence Group Systems

Inbound Port	Type	Protocol	Function	Configuration		
				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	RealPresence Group Web UI 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
5001	Static	TCP	People+Content™ IP	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
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 RealPresence Group Systems

Connections from RealPresence Group Systems

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
80	Static	TCP	Polycom Product Registration	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
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

Connections from RealPresence Group Systems

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
443	Static	TLS	Microsoft Lync 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.
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

Connections from RealPresence Group Systems

Outbound Port	Type	Protocol	Function	Configuration		
				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
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

Connections from RealPresence Group Systems

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
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

RealPresence Group system security profiles provide varying levels of secure access to your RealPresence Group system. The default settings security profile type vary. See these tables for detailed information on security profile defaults:

- Maximum Security Profile Default Settings
- High Security Profile Default Settings
- Medium Security Profile Default Settings
- Low Security Profile Default Settings

To learn how to enable a security profile, refer to Configure Security Profiles .

Maximum Security Profile Default Settings

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?
General Settings			
System Settings			
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

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Pairing				
	Allow Polycom Touch Control Pairing **Note:** Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
	SmartPairing Mode	Disabled	Disabled	Read-only
Serial Ports				
Mode				
	RS-232 Mode **Note:** Some RealPresence Group 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				
	Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes

Admin Settings Area	Maximum Range	Default Value	Configurable?
Audio/Video			
Video Inputs			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Enabled	Read-only
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People+Content IP	Checkbox	Disabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	Maximum	Yes
Authentication			
Active Directory Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
Enable Web Access	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
	Enable 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
	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
	Idle Session Timeout in Minutes	1,3,5,10,15,20,30, 45,60,120,240,480	10	Yes

Admin Settings Area			Maximum Range	Default Value	Configurable?
		Maximum Number of Active Sessions	10,15,20,25,30,35 ,40,45,50	25	Yes
		Allow Video Display on Web	Checkbox	Disabled	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 Cryptography	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
		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

Admin Settings Area		Maximum Range	Default Value	Configurable?
	Login Credentials			
	Use Room Password for Remote Access	Checkbox	Disabled	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)			
	Minimum Length	8-16,32	15	Yes
	Require Lowercase	Off,1,2,All	2	Yes
	Require Uppercase	Off,1,2,All	2	Yes
	Require Numbers	Off,1,2,All	2	Yes
	Require Special Characters	Off,1,2,All	2	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
	User (Room), Admin (Room)			
	Minimum Length	8-16,32	9	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	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	Off,1,2,All	Off	Yes
	Require Uppercase	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?
	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	6-16,32	12	Yes
	Require Lowercase	Off,1,2,All	1	Yes
	Require Uppercase	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

Admin Settings Area			Maximum Range	Default Value	Configurable?
	Banner Text		DoD Custom	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
	Revocation				
		Revocation Method	OCSP CRL	OCSP	Yes
		Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Certificates					
	Certificate Options				
		Certificate Validation (Web Server)	Checkbox	Enabled	Yes
		Certificate Validation (Client Apps)	Checkbox	Enabled	Yes
Servers					
Directory Servers					
	XMPP		Provisioned-only	Disabled	Yes (via provisioning)
	Service Type **Note:** The *Microsoft* selection means Microsoft Lync Server 2013, depending on what is installed.		Off Microsoft Polycom GDS LDAP	Off	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes

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	Yes

Change Maximum Security Profile Default Values

When you configure the RealPresence Group 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**

High Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the **High** security profile.

Admin Settings Area	High		
	Range	**Default Value**	**Configurable?**
General Settings			
System Settings			
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
Pairing			
Allow Polycom Touch Control Pairing **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 Group 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

Admin Settings Area	High		
	Range	Default Value	Configurable?
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
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	Disabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	High	Yes
Authentication			
Active Directory Authentication	Checkbox	Disabled	Yes

Admin Settings Area			High		
			Range	Default Value	Configurable?
	Access				
		Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
		Enable Web Access	Checkbox	Enabled	Yes
		Enable 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
		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
		Allow Video Display on Web	Checkbox	Disabled	Yes

Admin Settings Area			High		
			Range	Default Value	Configurable?
	Encryption				
		Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	Required- Video Calls	Yes
		Require FIPS 140 Cryptography	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	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	Off,[1..24] hours	Off	Yes
	Login Credentials				
		Use Room Password for Remote Access	Checkbox	Disabled	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

Admin Settings Area		High		
		Range	Default Value	Configurable?
	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
	Password Expiration Warning	1-7	4	Yes
	Remote Access (Admin Remote, User Remote)			
	Minimum Length	1-16,32	6	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	6-16,32	6	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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

Admin Settings Area		High		
		Range	Default Value	Configurable?
	Meeting			
	Minimum Length	Off,1-20,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	6-16,32	8	Yes
	Require Lowercase	Off,1,2,All	1	Yes
	Require Uppercase	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	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

Admin Settings Area			High		
			Range	Default Value	Configurable?
Certificates					
	Certificate Options				
		Certificate Validation (Web Server)	Checkbox	Enabled	Yes
		Certificate Validation (Client Apps)	Checkbox	Enabled	Yes
	Revocation				
		Revocation Method	OCSP CRL	OCSP	Yes
		Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner					
	Enable Security Banner		Checkbox	Disabled	Yes
	Banner Text		DoD Custom	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					
	XMPP		Provisioned-only	Disabled	Yes (via provisioning)
	Service Type **Note:** The *Microsoft* selection means Microsoft Lync Server 2013, depending on what is installed.		Off Microsoft Polycom GDS LDAP	Off	Yes

Admin Settings Area	High		
	Range	Default Value	Configurable?
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes

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

Change High Security Profile Default Values

When you configure the RealPresence Group 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

Medium Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the **Medium** security profile.

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
General Settings			
System Settings			
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	Enabled	Yes
Pairing			
Allow Polycom Touch Control Pairing **Note:** Disabling this setting closes the SSH port.	Checkbox	Enabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Enabled	Yes
Serial Ports			
Mode			
RS-232 Mode **Note:** Some RealPresence Group 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

Admin Settings Area	Medium		
	Range	Default Value	Configurable?
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
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
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	Medium	Yes
Authentication			
Active Directory Authentication	Checkbox	Disabled	Yes

Admin Settings Area			Medium		
			Range	Default Value	Configurable?
	Access				
		Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
		Enable Web Access	Checkbox	Enabled	Yes
		Enable 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)	Yes
		Enable Telnet Access	Checkbox	Disabled	Yes
		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	10,15,20,25,30,35,40,45,50	Yes
		Maximum Number of Active Sessions	10-50	25	Yes
		Allow Video Display on Web	Checkbox	Disabled	Yes

Admin Settings Area			Medium		
			Range	Default Value	Configurable?
	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
		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	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	Off	Yes
		Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes

Admin Settings Area		Medium		
		Range	Default Value	Configurable?
	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	Off,1,2,All	Off	Yes
	Require Uppercase	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
	User (Room), Admin (Room)			
	Minimum Length	8-16,32	8	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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

Admin Settings Area		Medium		
		Range	Default Value	Configurable?
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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
	SNMP **Note:** SNMP passwords are applicable only when the system uses SNMP v3.			
	Minimum Length	3-16,32	3	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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			
	Certificate Validation (Web Server)	Checkbox	Disabled	Yes
	Certificate Validation (Client Apps)	Checkbox	Disabled	Yes

Admin Settings Area			Medium		
			Range	Default Value	Configurable?
	Revocation				
		Revocation Method	OCSP CRL	OCSP	Yes
		Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner					
	Enable Security Banner		Checkbox	Disabled	Yes
	Banner Text		DoD Custom	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					
	XMPP		Provisioned-only	Disabled	Yes (via provisioning)
	Service Type **Note:** The *Microsoft* selection means Microsoft Lync Server 2013, depending on what is installed.		Off Microsoft Polycom GDS LDAP	Off	Yes
SNMP					
	Version1		Checkbox	Disabled	Yes
	Version2c		Checkbox	Disabled	Yes
	Version3		Checkbox	Enabled	Yes
Calendaring Service					
	Enable Calendaring Service		Checkbox	Disabled	Yes

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	UDB	Yes

Change Medium Security Profile Default Values

When you configure the RealPresence Group 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

Low Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the **Low** security profile.

Admin Settings Area	Low		
	Range	**Default Value**	**Configurable?**
General Settings			
System Settings			
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	Enabled	Yes
Pairing			
Allow Polycom Touch Control Pairing **Note:** Disabling this setting closes the SSH port.	Checkbox	Enabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Disabled	Yes
Serial Ports			
Mode			
RS-232 Mode **Note:** Some RealPresence Group systems support only a subset of listed modes.	Off Control Camera Control Closed Caption Pass Thru	Control	Yes

Admin Settings Area	Low		
	Range	Default Value	Configurable?
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto TLS TCP UDP	Auto	Yes
Dialing Preference			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	AVC Only	Yes
Audio/Video			
Video Inputs			
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Enabled	Yes
Enable People+Content IP	Checkbox	Enabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Enabled	Yes
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	Low	Yes

Admin Settings Area	Low		
	Range	Default Value	Configurable?
Authentication			
Active Directory Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Disabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Enable Access to User Settings	Checkbox	Disabled	Yes
Restrict to HTTPS	Checkbox	Disabled	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)	Yes
Enable Telnet Access	Checkbox	Disabled	Yes
Enable SSH Access	Checkbox	Enabled	Yes
Enable SNMP Access	Checkbox	Disabled	Yes
Lock Port after Failed Logins	Off,2-10	Off	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable?
	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
	Allow Video Display on Web	Checkbox	Disabled	Yes
Encryption				
	Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	Off	Yes
	Require FIPS 140 Cryptography	Checkbox	Disabled	Yes
Local Accounts				
Account Lockout				
	Lock Admin Account After Failed Logins	Off,2-10	Off	Yes
	Admin Account Lock Duration	1,2,3,5 minutes	1	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable?
	Reset Admin Account Lock Counter After	Off,[1..24] hours	Off	Yes
	Lock User Account After Failed Logins	Off,2-10	Off	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				
	Use Room Password for Remote Access	Checkbox	Enabled	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

Admin Settings Area		Low		
		Range	Default Value	Configurable?
	Remote Access (Admin Remote, User Remote)			
	Minimum Length	Off,1-16,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	Enabled	Yes
	User (Room), Admin (Room)			
	Minimum Length	Off,1-16,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	Enabled	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable?
	Meeting			
	Minimum Length	Off,1-20,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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
	SNMP **Note:** SNMP passwords are applicable only when the system uses SNMP v3.			
	Minimum Length	8-16,32	8	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	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	Low		
	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
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
Certificates			
Certificate Options			
Certificate Validation (Web Server)	Checkbox	Disabled	Yes
Certificate Validation (Client Apps)	Checkbox	Disabled	Yes
Revocation			
Revocation Method	OCSP CRL	OCSP	Yes
Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes
Security Banner			
Enable Security Banner	Checkbox	Disabled	Yes
Banner Text	DoD Custom	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

Admin Settings Area	Low		
	Range	Default Value	Configurable?
Servers			
Directory Servers			
XMPP	Provisioned-only	Disabled	Yes (via provisioning)
Service Type **Note:** The *Microsoft* selection means Microsoft Lync Server 2013, depending on what is installed.	Off Microsoft Polycom GDS LDAP	Off	Yes
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes

Diagnostics Area	Low		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Yes

Call Speeds and Resolutions

See the following topics to learn about maximum call speeds and resolutions for different call types:

- Point-to-Point Call Speeds
- Multipoint Call Speeds
- High-Profile Call Speeds and Resolutions
- Multipoint Resolutions for High Definition Video
- Resolution and Frame Rates for Content Video

Point-to-Point Call Speeds

The following table shows the maximum allowable H.323/SIP point-to-point call speeds for each type of RealPresence Group system.

Point-to-Point Call Speeds

System	Maximum Call Speed
RealPresence Group 300	3072 kbps
RealPresence Group 310	3072 kbps
RealPresence Group 500	6144 kbps
RealPresence Group 700	6144 kbps

Multipoint Call Speeds

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. RealPresence Group 300 and 310 systems do not support multipoint calling.

Multipoint Call Speeds

Number of Sites in Call	Max Speed for Each Site	Max Speed for Each Site (ICE Enabled, Lync 2013/Skype for Business 2015	Max Speed for Each Site (CCCP Lync 2013/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
7 (RealPresence Group 700 only)	1024 kbps	128 kbps	664 kbps
8 (RealPresence Group 700 only)	832 kbps	128 kbps	664 kbps

Note: Lync interoperability option and CCCP calls
These values do not apply when the Microsoft Lync Interoperability option is enabled, whether it is in a Lync 2013/Skype for Business 2015 environment. When this option 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, Lync 2013, Skype for Business 2015) column are applicable only when both of the following criteria are met:

- The Lync Interoperability option is disabled, so that calls are negotiated with H.263 using Lync 2013 or 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 Group systems. Resolutions and frame rates are based on both the call speed and the **Optimized for** setting of your Camera input.

Note: Resolutions and frame rates for disparate endpoints
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 RealPresence Group system and a different type of endpoint or a multipoint resource. RealPresence Group 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 4 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 RealPresence Group systems with NTSC cameras in H.264 high-profile calls.

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	1024x576	60
832-895	Motion	1024x576	60	1024x576	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 RealPresence Group 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

Polycom offers enhanced high definition (HD) multipoint resolutions, maximizing video quality in multipoint conferences. 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.

MCU Resolutions

Number of Endpoints in the Video Conference	Maximum Transmitting Resolutions	Maximum Receiving Resolutions
2 endpoints	1080p, 60fps	1080p, 60fps
3-4 endpoints	1080p, 30fps	960x544, 30fps
5-8 endpoints	720p, 30fps	640x368, 30fps

Note: Specific limits for RealPresence Group 500 and 700 systems

RealPresence Group 500 systems support one endpoint as a host system and up to 5 other endpoints in a 6-way multipoint conference; RealPresence Group 700 systems supports one endpoint as a host system and up to 7 other endpoints in an 8-way multipoint conference.

Resolution and Frame Rates for Content Video

The high frame rates with high resolution apply only to point-to-point calls above 832 kbps. 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 and Frame Rates for Content Video

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 RealPresence Group 310 or RealPresence Group 500 is set to **Content** in **Admin Settings > Network > IP Network > Network Quality**.