



ADMINISTRATOR GUIDE

6.0.0 | September 2016 | 3725-63706-010A

Polycom[®] RealPresence[®] Group Series



Copyright© 2016, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

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

Before You Begin	17
Audience, Purpose, and Required Skills	17
Get Help	17
Polycom and Partner Resources	18
The Polycom Community	18
Getting Started with a Polycom® RealPresence® Group Series System	19
Polycom® RealPresence® Group Series Systems	19
RealPresence Group 300 Systems	19
RealPresence Group 310 Systems	19
RealPresence Group 500 Systems	20
RealPresence Group 700 Systems	20
Polycom® RealPresence Touch™ Device	21
Polycom® Touch Control™ Device	21
Polycom® VisualBoard™ Application	22
Setting Up System Hardware	23
Setting Up Your Hardware and Remote Control Device	23
Recharge the Remote Control Battery	23
Position the RealPresence Group System	24
Positioning the Polycom® EagleEye™ Acoustic Camera	25
Positioning the Polycom® EagleEye™ Director	25
Powering the System On and Off	27
Power On RealPresence Group 300, 310, and 500 Systems	27
Powering RealPresence Group 700 Systems On and Off	28
Remote Control Operation on RealPresence Group 700 Systems	28
Power Button on the Remote Control	29
Indicator Lights	29
RealPresence Group System Indicator Lights	29
RealPresence Group 700 Indicator Lights	30
EagleEye Acoustic Camera Indicator Lights	31
EagleEye Director Indicator Light	31

EagleEye Producer Indicator Lights	32
Install the System Software	33
Installing the System Software Locally or Remotely	33
Naming Conventions for the System Admin ID and Password	33
Run the Setup Wizard Locally	34
Run the Setup Wizard From a Remote Location	34
Update Polycom System Software and Apply Software Options	35
Preparing to Update a RealPresence Group System	35
Ensuring System Compatibility with Peripherals	36
Polycom EagleEye Producer and EagleEye Director Software Updates	36
Serial and License Numbers	36
Create a Serial and License Number File for Multiple Systems	37
Software and System Option Keys	37
Key File Formats	38
Available Software Options	38
Obtain Software or System Option Keys	39
Create a Single Key File to Update Multiple Systems	39
Activate System Options	40
RealPresence Group System Software Updates	40
Dynamic RealPresence Group System Software Updates	40
Configure Your Web Server as the Update Site	40
Updating System Software from a Web Server	41
Manually Update Software	41
Automatically Update Software	42
Update System Software from a USB Storage Device	43
Update System Software from a .tar File	43
Installing an Older Software Version	44
Determine the Software Version	44
Delete System Settings	44
Downgrading Tips	44
Manage the System Remotely	46
System Web Interface	46
Access the System Web Interface	46
Enable Room and Call Monitoring	47
Remotely Monitor a Room or Call	47
Managing System Profiles on the Web Interface	47
Store a Setting Profile	48

Upload a Profile	48
Send a Message to a System	48
Set Up and Configure Directory Servers	48
Setting Up a Directory Server	48
Configuring a Directory Server	49
Configure the Polycom GDS Directory Server	49
Configure the LDAP Directory Server	50
SNMP Condition Reports	51
Download MIBs	51
Configure SNMP Management	51
Using a Provisioning Service	53
Enable the Provisioning Service	54
Configure the Provisioning Service	54
Disable a Provisioning Service	55
Multitiered Directory Navigation	55
Polycom® RealPresence® Cloud Service	56
Enable RealPresence Cloud Mode in the System Web Interface	56
Configure System Software	57
Configuring the RealPresence Group System	57
Enable PKI Certificates	57
Set Up the System Name	58
View System Software Options	58
Activate System Options	58
Customize What Users See on the System Home Screen	59
Speed Dial	59
Enable Speed Dial	59
Add Speed Dial Contacts	59
Image File Requirements for Speed Dial Contacts	60
Upload an Image File for Speed Dial Contacts	60
Remove Speed Dial Contacts	60
Calendaring Service	60
Configure the Calendaring Service	61
Change the Background Image on the Home Screen	62
Change the Background Startup Image on the Home Screen	63
Kiosk Mode	63
Enable Kiosk Mode	63
Home Screen Icons	64
Address Bar	64
Choose Where to Display Elements on the Address Bar	64

Enable Access to User Settings	65
Restrict Access to User and Administrative Settings	65
Microsoft Interoperability	67
Microsoft Directory Servers	67
SIP Settings for Integration with Microsoft Servers	67
RTV and Skype-Hosted Conference Support	67
AES Encryption for Skype Calls	68
RealConnect	68
RealConnect Limitations	68
Skype for Business Client 2015 Content Viewing	68
RDP Content Sharing	69
Microsoft Skype Mode	70
Configuring System Network Settings	71
Connecting to the LAN	71
LAN Status Lights	71
Configure LAN Properties	72
LLDP and LLDP-MED Support	76
Behavior When LLDP is Enabled	76
Enable LLDP Using a USB Storage Device	77
Enable LLDP After the Setup Wizard Process	77
IP Network Settings	77
Configure H.323 Settings	77
Configure the System to Use a Gatekeeper	78
SIP Settings	79
Configure SIP Settings	79
SIP Settings for Integration with the Telepresence Interoperability Protocol (TIP) ...	81
AS-SIP Settings	81
Enable the AS-SIP Setting	82
Configure AS-SIP Settings for MLPP	82
Add an AS-SIP Service Code	82
Delete an AS-SIP Service Code	82
Define AS-SIP Outbound Precedence Call Defaults	83
Multilevel Precedence and Preemption (MLPP)	83
Define MLPP Network Domains	83
Add an MLPP Network Domain	84
Alternative Network Address Type (ANAT) for RealPresence Group Systems	84
Configure Network Quality Settings	84
Lost Packet Recovery and Dynamic Bandwidth Settings	86

Configure the Room System for Use with a Firewall or NAT	87
H.460 NAT Firewall Traversal	88
Configure the H.460 NAT Firewall Traversal	89
Basic Firewall/NAT Traversal Connectivity	90
Setting Call Preferences for SVC	90
Configure Dialing Options	90
Enable Automatic Answering of SVC Point-to-Point Calls	91
Enable SVC Preference (H.264) for Calls	92
Configure Preferred Call Speeds	92
Monitors and Cameras	93
Receiving and Displaying Video in High Definition	93
Full-Motion HD Video and Audio	94
Configuring Monitor Settings	94
Configure Monitor Settings	94
Monitor Profiles and Video Layout Panel Views	95
Configure Monitor Profile Settings	95
Touch Monitor User Interface	97
Configure Secondary Monitors for Content in a Multiple Touch Monitor Environment	98
Monitor Resolutions for the RealPresence Group System Model Types	99
Recording Calls with Polycom® RealPresence® Media Suite	100
Enable Recording Controls	100
Recording Calls Remotely	100
Enable Recording on a RealPresence Group System	102
Configure Monitor Settings for Recording on a RealPresence Group 700 System	102
Maximize HDTV Video Display	103
Sleep Settings Prevent Monitor Burn-In	103
CEC Monitor Controls	103
Enabling Monitors to Support CEC	104
Enable CEC Controls	104
Disable CEC Controls	104
Polycom Cameras	105
Polycom EagleEye IV	105
Polycom EagleEye Acoustic	105
Polycom® EagleEye™ Producer Camera	105
Polycom EagleEye Director	106
Connecting Cameras to RealPresence Group Systems	106
Powering Cameras with RealPresence Group Systems	107
Sleep and Wake States for Cameras	107
Configuring Camera Settings	107

Configure Camera and Video Settings	107
Configure General Camera Settings	108
Configuring Video Input Settings	108
Configure a Third-Party Camera	111
EagleEye IV Camera Orientation	112
Enable an Inverted Camera Position for the EagleEye IV Camera	112
Enable a Normal Camera Position	112
Setting Up the EagleEye Producer	113
Updating EagleEye Producer with RealPresence Group Systems	113
Change Camera Tracking Settings	113
Turn on Camera Tracking for the EagleEye Producer	114
Turn Off camera Tracking for the EagleEye Producer	114
Automatically Calibrate the EagleEye Producer	115
View System Status for the EagleEye Producer	115
Configure the Polycom EagleEye Director	115
Calibrate the EagleEye Director Cameras	116
Adjust the Room View of the EagleEye Director	117
Enable Camera Tracking with EagleEye Director	117
Disable Camera Tracking with EagleEye Director	118
EagleEye Director Camera Tracking in the Local Interface	118
Camera Presets	118
Configure FECC on a Far-end Site Camera	119
Microphones and Speakers	120
Available Microphone Inputs by System	120
Audio Input Tips by Microphone Type	121
Polycom RealPresence Group System Table or Ceiling Microphone Arrays	121
Polycom EagleEye Acoustic Microphones	121
Polycom SoundStation IP 7000 Conference Phone	121
Audio Input Configuration Selections	121
Microphone Inputs for RealPresence Group 300/310	122
Microphone Inputs for RealPresence Group 500/700	122
Third-Party Microphones	122
SoundStructure Digital Mixer	122
Polycom Microphone Placement to Send Stereo from Your Site	123
Audio Output	124
Speaker Placement to Receive Stereo from Far Sites	125
Set the Speaker Volume	126
Configure Audio Settings	126
Configure Audio Input Settings	127

3.5mm Audio Input	129
Enable 3.5mm Audio Input	129
Enable 3.5mm Audio Input for Content Sharing	129
Configure Audio Output Settings	129
Stereo Settings	130
Test StereoSurround	131
Set Up Third-party Microphones	131
Acoustic Fence Technology	131
Configure the Acoustic Fence	132
Content Sharing	134
Sharing Content During Calls	134
Configure Content Sharing	134
Connect Computers to Polycom RealPresence Group Systems	135
Configuring DVD Player Settings	135
Configure DVD Settings	135
Multipoint Resolution and Frame Rates for People and Content	136
Configure and Install a Polycom Content Display Application	136
Configure Closed Captioning	137
Dial-Up Connection to the System's RS-232 Serial Port	137
Enter Closed Captions Using Equipment Connected to a Serial RS-232 Port	139
Enter Closed Captions on the Web Interface	139
Placing and Answering Calls	141
Configure Call Settings	141
Configure Call Answering Mode	143
Enable Flashing Incoming Call Alerts	143
Multipoint Calling	144
Enter a Multipoint Option Key	144
Select a Multipoint Viewing Mode	145
Configuring and Placing Audio-Only Calls	146
Enable Audio-Only Calls	146
Disable Audio-Only Calls	146
Select the Call Type Order for Audio-Only Calls	146
Place an Audio-Only Call from the System Web Interface	147
Including Multiple Sites in a Cascaded Call	147
Place a Cascaded Call	148
Managing Directories in the Web Interface	148
Searching Directory Contacts to Call	149
Prerequisite for Using the Global Directory Service (GDS)	149

Search for Directory Contacts to Call	149
Manage Favorites Contacts and Groups	150
Create a Favorites Contact	150
Create a Favorites Group	150
Edit a Favorites Group	150
Delete a Favorites Group	151
Importing and Exporting Favorites	151
Export Favorites Groups and Contacts	151
Import Favorites Groups and Contacts	152
Types of Favorites Contacts	152
Join Scheduled Meetings	153
Using the Web Interface Place a Call Page	153
Perform a Search for Web Interface Screens	153
Place a Call to Favorite Contacts	153
Place a Call to Speed Dial Contacts	154
Place a Call to Recent Call Contacts	154
Configure the Recent Calls List	154
Security	156
Security Settings in the Web Interface	156
Configure Security Profiles	157
Managing System Access and External Authentication	158
Enable External Authentication	159
Login and Credentials	159
Configure Local Access	160
Configure Remote Access Settings	161
Managing User Access to Settings and Features	162
Detecting Intrusions	163
Secure API Access	163
Access the API with SSH	164
Local Accounts	164
Configure Password Policies Settings	164
Account Lockout to Prevent Unauthorized System Access	166
View Connections to Your System in a Sessions List	167
Enabling a Whitelist for IPv4 and IPv6 Addresses	168
Enable a Whitelist	168
Add IP Addresses to a Whitelist	168
IPv4 Address Formats	168
IPv6 Address Formats	168
Port Lockout	169

Configure the Port Lockout Setting to Lock the Login Port	170
Encryption	170
Configure Encryption	171
Configure Encryption Settings for SVC Calls	172
Set AES Encryption for SVC Calls	172
Configure Encryption Settings for Skype for Business 2015	173
Verify H.323 Media Encryption	173
Visual Security Classification	173
Enable Visual Security Classification	174
Managing Certificates and Revocation	174
Configure Certificate Validation Settings	175
Install Certificates	176
Certificate Signing Requests (CSRs)	176
Create Certificate Signing Requests (CSRs)	177
Certificate Revocation Settings	178
Configure the Certificate Revocation List (CRL) Method	179
Certificates and Security Profiles within a Provisioned System	180
Delete Certificates and CRLs	181
RealPresence Server Address Configuration in PKI-enabled Environments	181
Configure a Security Banner	182
Configure a Meeting Password	182
Control and Navigation	184
Remote Control	184
Configure Remote Control Behavior	184
Configuring the Remote Control Channel ID for a Specific System	185
Confirm a Channel ID	186
Save a Channel ID for a Specific System	186
Configure a Channel ID for the Remote Control	186
Connecting Control and Accessibility Equipment	187
Third-Party Touch Panel Controls	187
Configure RS-232 Serial Port Settings	187
Polycom® RealPresence® Medialign™ Solution	188
Polycom® Concierge Solution	188
Add the System Pairing Code to the System Home Screen	189
Check the Polycom Concierge Service Status	189
SmartPairing	189
SmartPairing Prerequisites	189
Configure SmartPairing	190
View Remote Sessions on the System	190

Configure Contact Information	190
Configure System Location Settings	191
Configure Room System Language Settings	191
Configure System Date and Time Settings	192
Configure Sleep Settings	193
Diagnostics, Status, and Utilities	194
Polycom RealPresence Manageability Instrumentation Solution	194
Diagnostics Screens	195
Access Diagnostic Screens in the Local Interface	195
Information	195
Status	196
Diagnostics	196
Access Diagnostics Screens in the Web Interface	198
System Diagnostics	198
Audio and Video Tests	199
System Log Files	200
Configure System Log Management	200
Configure System Log Level and Remote Logging	201
Retrieving Log Files	202
Download System Log Files	203
Transfer System Log Files	203
Transfer EagleEye Director Logs	203
Call Detail Report (CDR)	204
Download a Call Detail Report (CDR)	206
Polycom Touch Device Software Updates	207
Required Prerequisites for RealPresence Touch Software Updates	207
Required Prerequisites for Polycom Touch Control Software Updates	208
Dynamic Polycom Touch Device Software Updates	208
Configure Your Web Server as the Update Site	208
Configure Your Web Server as the Update Site	209
Managing Polycom Touch Device Software on Your Server	209
Set a RealPresence Touch Software Version as Current	210
Remove a RealPresence Touch Software Version	210
Set a Polycom Touch Control Software Version as Current	210
Remove a Polycom Touch Control Software Version	211
Update Software from the RealPresence Touch Web Interface	211
Update Software from the RealPresence Touch Local Interface	212
Updating RealPresence Touch Software from a USB Storage Device	212

Update the RealPresence Touch With a USB Storage Device	212
Update RealPresence Touch Software from a USB Storage Device	213
Update Polycom Touch Control Software Manually	213
Update Polycom Touch Control Software Automatically in the Web Interface	214
Update Polycom Touch Control Software Automatically in the Local Interface	215
Manually Update Polycom Touch Control Software in the Local Interface	215
Update Polycom Touch Control Software from a USB Storage Device	216
Troubleshooting for Software Upgrade Issues	217
Test the Download URL	217
Polycom Touch Devices	218
Positioning the RealPresence Touch Device	218
Positioning the Polycom Touch Control	218
Powering On the Polycom Touch Control	219
Polycom Touch Control Indicator Light	219
Enable the RealPresence Touch	219
Enable the Polycom Touch Control	219
Set Up the RealPresence Touch Device	220
Pairing the RealPresence Touch with a RealPresence Group System	220
RealPresence Touch Pairing and Connection States	220
Pair the RealPresence Touch and a System For the First Time	221
Pair a Previously Paired System to a RealPresence Touch	221
Unpair the RealPresence Touch and a System	222
Remove a System from the Paired System List	222
Power Off the RealPresence Touch	222
Wake the RealPresence Touch	222
Remote Management of the RealPresence Touch	223
Open a Remote Management Window for the RealPresence Touch	223
Download Logs Using the RealPresence Touch	223
Pair the RealPresence Touch and a System on the Web Interface	223
Use the RealPresence Touch to Unpair a System on the Web Interface	224
Change the User Name and Password for the RealPresence Touch	224
Customize the RealPresence Touch Home Screen	224
Choose Icon Buttons to Display on the RealPresence Touch Home Screen	225
Customize the Place a Call Screen Icon Buttons on the RealPresence Touch Device	225
Change the Home Screen Background Image on the RealPresence Touch	226
Troubleshooting the RealPresence Touch Device	226
View System Details and Connection Status on the RealPresence Touch	226
View Call Statistics on the RealPresence Touch	227
Transfer RealPresence Touch Logs to a USB Storage Device	227

Perform a Factory Restore on the RealPresence Touch	227
Perform a RealPresence Touch Factory Restore Using a USB Storage Device	228
Set Up the Polycom Touch Control	228
Pairing States for the Polycom Touch Control Device	229
Pair the Polycom Touch Control and a RealPresence Group System	230
Unpair the Polycom Touch Control and a RealPresence Group System	231
Power Off the Polycom Touch Control	231
Wake the Polycom Touch Control	231
Configuring the Polycom Touch Control Software	232
Configure Polycom Touch Control LAN Settings	232
Configure Polycom Touch Control Location and Time Settings	233
Configure Admin ID and Password for the Polycom Touch Control	233
Managing the Polycom Touch Control Remotely	234
Open the Remote Management Window for the Polycom Touch Control	234
Troubleshooting on the Polycom Touch Control Device	235
View Call Statistics for an Active Point-to-Point Call on the Polycom Touch Control ...	235
View Call Statistics for an Active Multipoint Call on the Polycom Touch Control	235
Transfer Polycom Touch Control Logs to a USB Storage Device	236
View Polycom Touch Control System Details	236
Factory Restore on the Polycom Touch Control	236
Perform a Factory Restore on a Polycom Touch Control	237
Perform a Factory Restore on a Polycom Touch Control Using a USB Storage Device	237
VisualBoard Application	239
VisualBoard Application Support	239
Prerequisites for the VisualBoard Application	239
Touch Monitor Support	240
Enable the VisualBoard Application	240
Prerequisites to Install a Second Monitor for Use with the VisualBoard Application	240
Install a Second Monitor for Use With the VisualBoard Application	241
Configure Monitor 1 as the Content Monitor	241
Configure Monitor 2 as the Content Monitor	242
Polycom® UC Board	242
Configure the Polycom UC Board	243
Troubleshooting	244
General Troubleshooting	244
Placing a Test Call	245
Viewing System Details on the Local Interface	245
Access the Information Screen	246

Access the Status Screen	247
Access the System Diagnostics Screen in the Local Interface	248
Audio Meters	249
Set Audio Meter Levels	250
View Call Statistics for an Active Point-to-Point Call With the Remote Control	250
View Call Statistics for an Active Multipoint Call with the Remote Control	250
Power-On Self Test (POST)	251
System Reset	251
Reset a System	251
Factory Restore on the RealPresence Group System	252
Perform a Factory Restore of a System	252
Perform a Factory Restore to Install a Specific Software Version	253
Delete Data and Configuration System Files	254
Perform a Factory Restore on the Polycom EagleEye Director	254
Perform a Factory Restore on the EagleEye Producer	255
Before You Contact Polycom Technical Support	255
Locate the System Serial Number	255
Locate the Software Version	256
Locate Active Alert Messages	256
Locate the IP Address and H.323 Extension Settings	256
Locate the LAN Status	256
Locate Diagnostics	256
Contacting Technical Support	256
Knowledge Base	257
Polycom Solution Support	257
System Panel Views	258
Polycom RealPresence Group 300 System	258
Polycom RealPresence Group 310 System	259
Polycom RealPresence Group 500 System	261
Polycom RealPresence Group 700 System	263
Port Usage	267
Connections to RealPresence Group Systems	267
Connections from RealPresence Group Systems	269
Security Profile Default Settings	273
Maximum Security Profile Default Settings	273
Change Maximum Security Profile Default Values	284
Other Restrictions when Using the Maximum Security Profile	284

High Security Profile Default Settings	286
Change High Security Profile Default Values	295
Medium Security Profile Default Settings	296
Change Medium Security Profile Default Values	305
Low Security Profile Default Settings	306
Call Speeds and Resolutions	317
Point-to-Point Call Speeds	317
Multipoint Call Speeds	317
High-Profile Call Speeds and Resolutions	318
Multipoint Resolutions for High Definition Video	319
Resolution and Frame Rates for Content Video	320

Before You Begin

The *Polycom RealPresence Group Series Administrator Guide* is for administrators who need to install system software, options, and accessories, and to configure, customize, manage, and troubleshoot Polycom® RealPresence® Group systems. This guide covers the RealPresence Group 300, RealPresence Group 310, RealPresence Group 500, RealPresence Group 550, 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 at support.polycom.com:

- *Polycom RealPresence Group Series Setup Sheet*: Describes the contents of your package, how to assemble the system and accessories, and how to connect the system to the network. The setup document is included in the system package.
- *Polycom RealPresence Group Series Quick Tips*: Quick reference on how to use basic features
- *Polycom RealPresence Group Series User Guide*: Describes how to perform video conferencing tasks in the local interface
- *Polycom RealPresence Group Series Integrator Reference Guide*: Provides cable information and API command descriptions
- *Polycom RealPresence Group Series Regulatory Notices*: Describes safety and legal considerations for using Polycom RealPresence Group systems
- Release notes

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 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](http://support.polycom.com).

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.

Getting Started with a Polycom® RealPresence® Group Series System

The following topics provide an overview of the Polycom video conferencing systems.

- [Polycom® RealPresence® Group Series Systems](#)
- [Polycom® RealPresence Touch™ Device](#)
- [Polycom® Touch Control™ Device](#)
- [Polycom® VisualBoard™ Application](#)

Polycom® RealPresence® Group Series Systems

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

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.



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.

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.



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. Multipoint conference calls are not supported.

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 the ability to share content make it an ideal fit for most standard-sized meeting rooms.



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.

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.



Powerful video processing and several inputs and outputs 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 systems makes it easy for even novice users to control the system and get the most out of their video collaboration experience with no hassles.

Polycom® RealPresence Touch™ Device

The Polycom® RealPresence Touch™ is a highly-intuitive touch control device that enables you to quickly initiate video conferences. By allowing participants to focus on their meeting, the device 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 a room system, you can control the room system using the device's touch interface.



You can use speed dial for quick access to people, rooms, or virtual meeting rooms. You can also search a directory to quickly connect to the right person or location. Once in a call, you have easy access to share content, adjust camera views, and change participant layouts.

The design includes a 10" touch display so you can see everything clearly, while staying compact enough to be out of sight during your meetings. The background image can be customized to match your branding or provide information about the room. The home screen buttons and default screens can be selected by administrators.

Polycom® Touch Control™ Device

The Polycom® Touch Control™ graphical interface solution is an intuitive touch screen device that enables users to quickly initiate video conferences. The device features a high-resolution display that provides simplified navigation and menu selection. It allows users to control all aspects of their conference experience, including finding colleagues, placing calls and sharing content.



Users can connect to one another using a shared address book, on-screen keypad, and calendar entry. For quick access to room information, the Polycom Touch Control communicates with the RealPresence Group

Series room telepresence solution, which can be integrated with Microsoft Exchange software to provide complete location detail.

The Polycom Touch Control device uses Power Over Ethernet (PoE) for connectivity. Individual Polycom Touch Control devices can be paired and dedicated to any network-connected RealPresence Group system. Polycom Touch Control devices can be deployed in an identical configuration to provide users with a consistent experience regardless of environment, or devices can be individually tailored to unique workflows.

Polycom® VisualBoard™ Application

The Polycom® VisualBoard™ application allows you to show and annotate content in real time from 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.

Setting Up System Hardware

The following topics provide information on how to set up and configure Polycom video systems and peripherals:

- [Setting Up Your Hardware and Remote Control Device](#)
- [Position the RealPresence Group System](#)
- [Powering the System On and Off](#)
- [Indicator Lights](#)

Setting Up Your Hardware and Remote Control Device

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

Recharge the Remote Control Battery

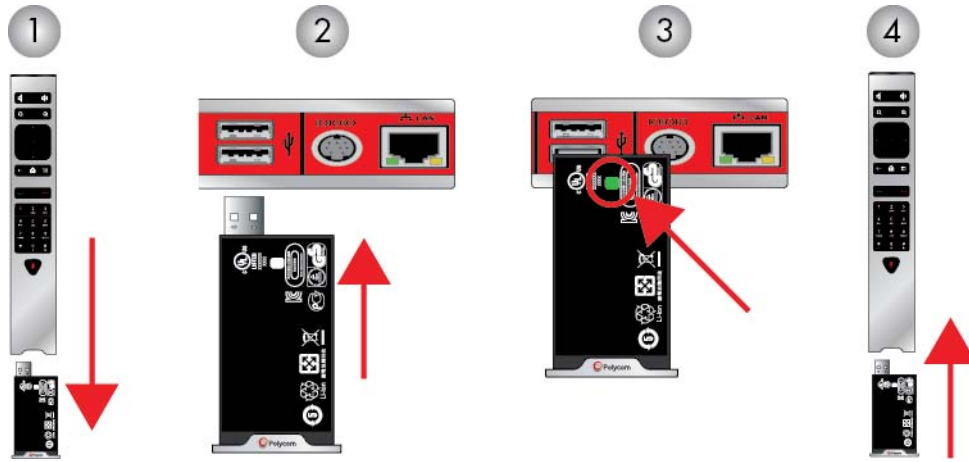
Your system setup sheet shows how to charge the battery in the remote control the first time. When the remote control battery power is at 10% or less, a notification is displayed on the home screen. The low battery notification returns after you dismiss other notifications, and is not displayed while 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 Insert the USB plug into any USB 2.0 port, such as the one on your system.
- 4 While the battery is charging, the status light is orange. After the status light on the battery turns green, remove it from the port.
- 5 Insert the charged battery into the remote control.

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

The following figure illustrates these steps for the RealPresence Group 300, RealPresence Group 310, RealPresence Group 500, and RealPresence Group 700 systems.



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 RealPresence Group System

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.

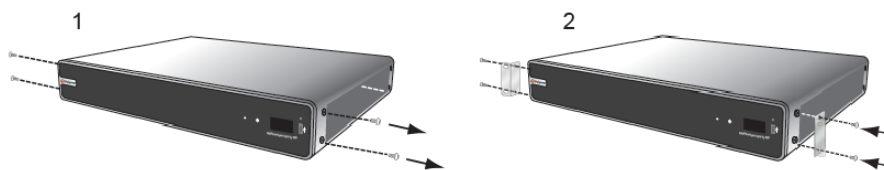




Caution: Keep ventilation openings free of any obstructions.

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.



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.

Positioning the Polycom® EagleEye™ Acoustic Camera

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



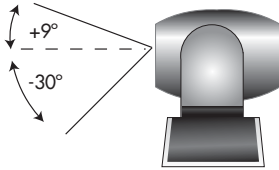
Positioning the Polycom® EagleEye™ Director

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:

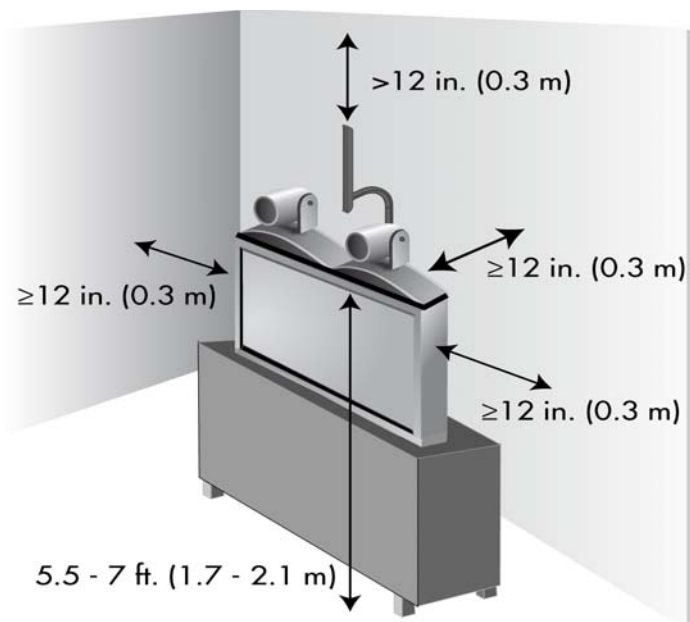
- Avoid setting the Polycom EagleEye Director in the corner of a room. The EagleEye Director should be at least 12 inches away from all of the walls.

- 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.

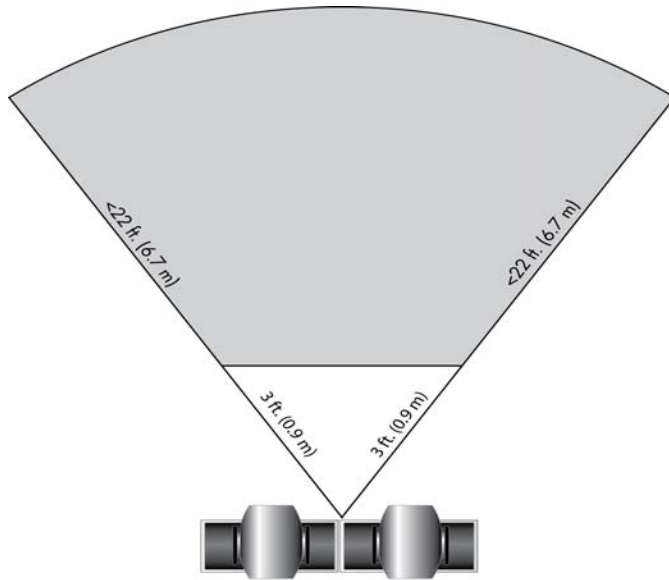


- To ensure optimal performance of the Polycom EagleEye Director facial recognition feature, follow these suggestions:
 - Provide ample lighting on faces of participants. This allows the system to correctly frame faces, using the eyes, noses, and mouths as guidelines.
 - Allow only minimal backlighting.
- 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.


The following figure shows EagleEye Director placement:



- Ensure that people are sitting within the viewing range of between 3 and 22 feet from the device. The following figure shows the EagleEye Director viewing range.



Powering the System On and Off

After you have connected all of the equipment that you will use with the RealPresence Group system, connect the power cable and power on the system. 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.




Note: Make sure that the system is powered off before you connect devices to it or before you unplug the power cable. Do not unplug the power cable when the system is powered on.

Power On RealPresence Group 300, 310, and 500 Systems

You can use the remote control or the power sensor to power on the RealPresence Group 300, 310, and 500 systems.


To power on the RealPresence Group 300, 310, or 500 system, do one of the following:

- 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.
For more information about programming the remote control, refer to [Configure Remote Control Behavior](#).
- Touch the power sensor on the front of the system.
The Polycom screen is displayed within about 10 seconds.

Power Off RealPresence Group 300, 310, and 500 Systems

You can use the remote control or the power sensor to power off the RealPresence Group 300, 310, and 500 systems.

To power off the RealPresence Group 300, 310, or 500 system, do one of the following:

- Press and hold  on the remote control.
For more information about programming the remote control, refer to [Configure Remote Control Behavior](#).
- 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.

Powering RealPresence Group 700 Systems On and Off

You can use the remote control or the power sensor to power off the RealPresence Group 700 system. The RealPresence Group 700 system can be powered on and off with the remote using the same buttons as shown for the other RealPresence Group systems; 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 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.

Remote Control Operation on 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.

Power Button on the Remote Control

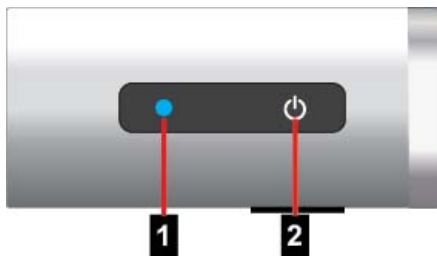
Use the remote control to power on and off your system, or to put the system to sleep or wake it. You can program this behavior using the web interface at **Admin Settings > System Settings > Remote Control, Keypad, and Power**. For information about remote control programming, refer to [Configure Remote Control Behavior](#). For details about how to use the remote control, refer to the *Polycom RealPresence Group Series User Guide*.

Indicator Lights

Indicator lights and power sensors display when the system or device is powered on.

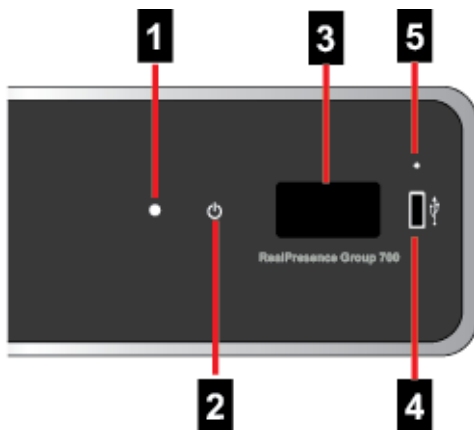
RealPresence Group System Indicator Lights

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

RealPresence Group 700 Indicator Lights

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.
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.

EagleEye Acoustic Camera Indicator Lights

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



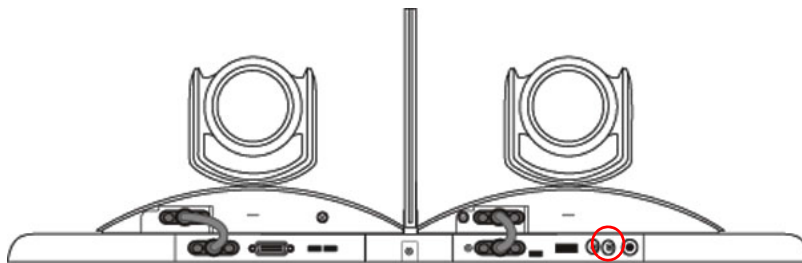
Ref. Number	Description
1	IR Sensor
2	System Status

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.

EagleEye Director Indicator Light

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



This indicator light provides the following information.

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 device. These LED lights emit colors that refer to various system states and allow you to identify the current state for the EagleEye Producer system. Detailed LED and system states mappings are shown in the following table.

LED	System State
Blue	Power On, EagleEye Producer normal state
Blinking Blue	On, not in a call, receive IR EagleEye Producer boot up
Fast Blinking Blue	Calibrate webcam room view
Amber	Standby - asleep
Alternate Amber and Blue	Software update, Factory restore, USB image update
Blinking Amber	USB disk plugged in
Green	On, In a call
Blinking Green	On, in a call, receive IR in a call
Fast Blinking Red	System error
Blink	Needs attention, receive IR

Install the System Software

The following topic provides information on how to install your system software:

- [Installing the System Software Locally or Remotely](#)

Installing the System Software Locally or Remotely

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

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

- In the room with the system — Use the remote control to navigate the screens and enter information. You can use the number pad on the remote control to enter text. Point the remote control at the camera to control the RealPresence Group system.
- From a remote location — If you know the IP address of the system, you can access and configure the system by using the system's web interface. For more information about using the web interface, refer to [System Web Interface](#).

Naming Conventions for the System Admin ID and Password

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

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



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

Run the Setup Wizard Locally

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

To run the setup wizard locally:

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

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

Run the Setup Wizard From a Remote Location

You can launch and run the setup wizard from a remote location to begin configuring your system on the web interface. If you know the IP address of the RealPresence Group system, you can access and configure it using the web interface. For more information about using the web interface, refer to [System Web Interface](#).

To run the setup wizard from a remote location:

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

After the RealPresence Group system starts up from the setup wizard (OOB) wizard, 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.

Update Polycom System Software and Apply Software Options

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

- [Preparing to Update a RealPresence Group System](#)
- [Ensuring System Compatibility with Peripherals](#)
- [Polycom EagleEye Producer and EagleEye Director Software Updates](#)
- [Serial and License Numbers](#)
- [Software and System Option Keys](#)
- [RealPresence Group System Software Updates](#)
- [Configure Your Web Server as the Update Site](#)
- [Updating System Software from a Web Server](#)
- [Update System Software from a USB Storage Device](#)
- [Update System Software from a .tar File](#)
- [Installing an Older Software Version](#)

Preparing to Update a RealPresence Group System

Polycom recommends that you upgrade your software to the latest available release. You can easily update your RealPresence Group system software and system options by performing a few tasks outlined here.

Be aware of these points when performing system upgrades:

- If you did not purchase additional system options, you need only to provide a serial number to activate the software. You do not need an option key.
- If you do not have a support agreement, contact an authorized Polycom dealer to get an upgrade key.
- If you are running a major or minor software version (x.y), you can update to a maintenance version (x.y.z) without an upgrade key. For example, you do not need a software key to update from version 4.3.0 to 4.3.1 or from 4.1.0 to 4.1.5.
- If you are running a major software version and the software has had a major upgrade, you need a software update key. For example, you need a key to update from version 4.0.0 to 5.0.0.
- If you are running a major or minor software version and the software has had a minor upgrade within the same major version (x.y1 to x.y2), you need a software update key to get the new software. For example, you need a key to update from version 4.2.0 to 4.3.0.



Note: For DoD Unified Capabilities Approved Product List (UC APL) software releases, go to www.polycom.com/solutions/industry/federal_government/certification_accreditation.html.

Ensure you have the required information ready before you begin installing and activating software updates or options:

- License numbers and system serial numbers. For more information, refer to [Serial and License Numbers](#).
- Software or option keys. Obtain these by logging in to support.polycom.com and requesting them from the Activation/Upgrade link. If you do not have a support agreement, contact an authorized Polycom dealer to get a key. For more information, refer to [Obtain Software or System Option Keys](#).

RealPresence Group systems perform several internal restarts while running software updates. Each restart takes about 2 or 3 minutes and improves the reliability of the update process by freeing up memory. If you are updating a system using a web browser, the internal restart is not visible from the web interface.

You can downgrade software to an earlier version at any time. For more information on downgrading software, refer to [Installing an Older Software Version](#).



Note: You need an account on support.polycom.com before you begin. Be sure to set up an account if you don't already have one.

Ensuring System Compatibility with Peripherals

If your system is used with an EagleEye Producer, EagleEye Director, or a Polycom touch device, such as a RealPresence Touch or Polycom Touch Control device, you must ensure that the version of the system is compatible with the peripheral software version.

For additional details on software compatibility, see the release notes for the system version you are going to use at support.polycom.com.

If you need to update your Polycom system and your RealPresence Touch, or Polycom Touch Control, complete your updates in this order:

- RealPresence Group system (which includes the Polycom EagleEye Producer and the Polycom® EagleEye™ Director update)
- RealPresence Touch or Polycom Touch Control device

Polycom EagleEye Producer and EagleEye Director Software Updates

Updates to EagleEye Producer and EagleEye Director software is included with the RealPresence Group system software updates. No license number or key is needed to update these peripherals.

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

Serial and License Numbers

Make a note of your system serial number and license number. You must provide these numbers in order to get the keys that activate software updates and system options.

- The 14-digit *serial number* is the unique number that identifies your system. You can find it on the System Information screen and on a label on the system. Serial numbers are case sensitive.
- The *license number* is the number that you receive when you purchase a software update or system option. License numbers have the following format:

Software update license: U1000-0000-0000-0000-0000

System option license: K1000-0000-0000-0000-0000

Create a Serial and License Number File for Multiple Systems

If you have multiple systems, you can save time when you request keys for purchased software updates or system options from Polycom. To do this, create a text file that has all of the necessary information in it before you visit the Polycom support site. This saves you the time of entering each serial and license file number individually on the site. Instead, you can just upload your text file.

To create a serial and license number text file:

- 1 Create a new file in a text editor.
- 2 Do one of the following:
 - If you do not have a software service plan on all of your systems, enter the license numbers and serial numbers of your systems in the text file.
 - If you do have a software service plan on all of your systems, enter only the serial numbers of the systems in the text file.
- 3 Save and close the text file.

Use the following format for text files that contain license numbers and serial numbers:

license number<TAB>*system serial number*

A text file with software update license numbers and serial numbers might look like this:

```
U1000-000-000-0000<TAB>82040903F01AB1
U1000-000-000-0000<TAB>82043604G18VR2
```

A text file with system option license numbers and serial numbers might look like this:

```
K1000-000-000-5001<TAB>82040903F01AB1
K1000-000-000-5003<TAB>82043604G18VR2
```

A text file with only serial numbers might look like this:

```
82040903F01AB1
82043604G18VR2
```

Software and System Option Keys

To perform a major or minor software update or activate options, obtain a key before you run the software update. A *key* is the number that activates software or options on a specific system. A key is valid only on the system for which it is generated.

There are two types of keys:

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

To obtain these keys, log in to support.polycom.com and request them using the Activation/Upgrade link. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.

Key File Formats

Most key files use this format:

License Number <TAB>Serial Number<TAB>Key

For example, a text file with update license numbers, serial numbers, and keys might look like this:

U1059-3131-6042-3609<TAB>8213190FFAE7D5<TAB>UBA5-1D6E-EB00-0000-0192

The following example shows a software update key file:

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

The following example shows an option key file:

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

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

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

Available Software Options

The following system options are available for your RealPresence Group system. Activated system options have checkmarks next to them. Some options are not available for certain systems. For example, RealPresence Group 300 and 310 systems do not support Multipoint Video Conferencing.

- **Multipoint Video Conferencing:** This option enables your system to make video calls to more than one site at a time. It is available for RealPresence Group 500 and RealPresence Group 700 systems. For more information, refer to [Multipoint Calling](#).
- **Telepresence Interoperability Protocol (TIP):** This option improves the interoperability of systems in environments with certain Cisco telepresence systems. For more information, refer to [RTV and Skype-Hosted Conference Support](#).
- **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.
 - ◆ 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 Skype 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, while simultaneously far-end systems displaying low resolution images receive low resolution images from the system.
 - ◆ Centralized Conferencing Control Protocol (CCCP) enables seamless participation in multipoint video conferences hosted on Skype's audio/video server.

- ◆ The Skype 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 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 Skype for Business Server 2015 and Skype for Business 2015 client environments with IPv6 networks.

- **Advanced Video 1080p:** This option makes 1080p video and content available to room systems.

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

Obtain Software or System Option Keys

You can obtain software or option keys for a single system or for multiple systems. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.

To obtain software or option keys:

- 1 Open a browser and navigate to support.polycom.com.
- 2 Under Licensing & Product Registration, click **Activation/Upgrade**.
- 3 Log in to your account.
- 4 Do one of the following:
 - To update one system, click **Site & Single Activation/Upgrade**. Follow the onscreen instructions to enter your system license number and serial number.
 - To update multiple systems that are covered by a software service agreement, click **Batch Upgrade** and then select your product. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers, or serial numbers only.
 - To update multiple systems not covered by a software service agreement, click **Batch Activation**. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers, or serial numbers only.

Polycom sends a text file containing the requested keys for each system.

Create a Single Key File to Update Multiple Systems

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

To create a single key file to upgrade multiple systems:

- 1 Open the key files with a text editor, such as Notepad.
- 2 Copy the contents of one file to the end of the other file. Repeat, as necessary.
- 3 Save the combined file with the name `sw_keys.txt`.

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

Activate System Options

To activate certain features on your room system, you must use the system's web interface. Some of the features of a RealPresence Group system are optional. If you want to activate your system options without upgrading your software, you do not need to download software or run the software update. The only thing you need is your system option key. For more information about software and option keys, refer to [Software and System Option Keys](#).

To activate system options:

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

RealPresence Group System Software Updates

You can configure your system to get software updates using any of the following methods:

- A Polycom® RealPresence® Resource Manager system
- A server on your network
- The online software server hosted by Polycom
- Distribution files uploaded from your computer using a web interface to access the system
- A USB 2.0 storage device that you connect to the system



Note: If you use your system within a Department of Defense (DoD) environment, contact your Information Assurance Office (IAO) for approval before using a USB device with your system.

For additional details on RealPresence Group hardware and software compatibility, see the product release notes available at support.polycom.com.

Dynamic RealPresence Group System Software Updates

You can use a Polycom RealPresence Resource Manager system to update multiple endpoint systems after you complete the steps in the following topics:

[Serial and License Numbers](#)

[Software and System Option Keys](#)

For more information about updating system software in dynamic mode, setting an automatic software update policy, and testing a trial version software update package, refer to the *Polycom RealPresence Resource Manager System Operations Guide* available at support.polycom.com.

Configure Your Web Server as the Update Site

You can post system software to your web server and then configure the system to get updates from that location.

To set up your web server as the update site:

- 1 Make sure that your server allows clients to download files with the following extensions:
 - .plcm
 - .txt
 - .sig
- 2 Define a URL on your server that the system can use for software updates, and create a corresponding root directory to it.
- 3 Using a browser, navigate to support.polycom.com.
- 4 Under **Documents and Downloads**, select **Telepresence and Video**.
- 5 Navigate to the page that has the update for your system.
- 6 Save and extract a software package (.tar) file from the Polycom website to the root directory of the your web server.
- 7 If you are updating to a major or minor release, obtain a software update key (.txt) file from the Polycom website. Save the file as `sw_keys.txt` and place it in `rseries/platform/` on your web server.

Updating System Software from a Web Server

You can manually or automatically install software updates from the Polycom web server or from your own web server.

For a list of supported browsers, refer to the appropriate version of the *Polycom RealPresence Group Series Release Notes*.

Manually Update Software

You can manually install software updates from the Polycom server or your own web server.

To manually install software updates:

- 1 Open a supported browser, and configure it to allow cookies.
- 2 In the browser address line, enter the IP address of the RealPresence Group system using the format `http://IPAddress` (for example, `http://10.11.12.13`).
- 3 In the system web interface, select **Admin Settings**.
If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password, if one is set.
The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.
- 4 Go to **General Settings > Software Updates**.
- 5 Under Software Server in the **Server Address** field, enter the path and address of the update site where you posted the system software (for example, `http://10.11.12.100/rpsystem_repo`). To use the Polycom server, enter `polycom`.
- 6 Click **Check for Software Updates** to have the system detect updates. The system contacts the designated server to find available updates.

- 7 If the system indicates an update is available, click **Start Update** to install it.
- 8 When the Export Restrictions notice appears, click **Accept Agreement**. Follow the on-screen instructions to complete the update.

Automatically Update Software

You can automatically install software updates from the Polycom server or your own web server.

To automatically install software updates:

- 1 Open a supported browser and configure it to allow cookies.
- 2 Next, enter the IP address of the RealPresence Group system using the format `http://IPAddress` (for example, `http://10.11.12.13`).
- 3 In the system web interface, select **Admin Settings**.
If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password, if one is set.
The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.
- 4 Go to **General Settings > Software Updates**.
- 5 Under Software Server in the **Server Address** field, enter the path and address of the update site where you posted the system software (for example, `http://10.11.12.100/rpsystem_repo`). To use the Polycom server, enter `polycom`.
- 6 Under **Automatic Software Updates**, select **Automatically Check for and Apply Software Updates**.
- 7 When the Export Restrictions notice appears, click **Accept Agreement**.
- 8 Specify the automatic update options:
 - a Set the **Hour**, **Minute**, and **AM/PM** to specify the beginning of the time window within which the system checks for updates.
 - b From the **Duration** list, select the length of the time within which the system can check for updates.
 - c After the **Start Time** and **Duration** settings are configured, the system calculates a random time within the defined update window at which to check for updates. It then checks for updates at this time on a daily basis as long as the **Start Time** and **Duration** values do not change. If the **Start Time** or **Duration** values change, a new random time within the new time window is calculated.
- 9 Click **Save**.

For information about the latest software version, including version dependencies, refer to the *release notes for your system*.

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



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

Update System Software from a USB Storage Device

You can use a USB storage device to update one or multiple RealPresence Group systems. A setup wizard guides you through the simple process. The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the factory restore button.

If the system is paired with a Polycom touch device, you cannot use the touch device USB port to update the system software. If you use your system within a DoD environment, be sure to contact your Information Assurance Office (IAO) for approval before using a USB device with your system.

To update system software using a USB device:

- 1 If you are updating to a major or minor release (x.y), obtain keys (.txt) for each system that you want to update from the Polycom website. Save the text file as `sw_keys.txt` and place it in the root directory of the USB storage device.
- 2 Open a browser and navigate to support.polycom.com.
- 3 Under **Documents and Downloads**, select **Telepresence and Video**.
- 4 Navigate to the page that has the desired update for the RealPresence Group system or systems.
- 5 Save a software package (.tar) file from the Polycom website to the root directory of a USB storage device.
- 6 Connect the USB storage device to the USB port on the back of the system. The system detects the USB storage device and prompts you to confirm that you want to update the software.
- 7 Click **OK**. Follow the setup wizard instructions to complete the update.

Update System Software from a .tar File

You can manually install system software from a .tar file.

To manually install software by uploading a .tar file in the web interface:

- 1 Open a supported browser.
- 2 Configure the browser to allow cookies.
- 3 In the browser address line, enter the IP address of the RealPresence Group system using the format `http://IPaddress` (for example, `http://10.11.12.13`).
- 4 In the system web interface, select **Admin Settings**.
If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password, if one is set.
The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.
- 5 Go to **General Settings > Software Updates > Manual Software Updates > Browse**.
- 6 Select a .tar software file to upload and click **Open**.
- 7 Select **Start Transfer**.
- 8 After the .tar file transfers to the system, select **Start Update**.
- 9 Follow the on-screen instructions to complete the update.

Installing an Older Software Version

When your RealPresence Group system is provisioned with a provisioning server, such as Polycom RealPresence Resource Manager, the system automatically detects software on the provisioning sever and downgrades to the software version on the provisioning server.

If your system is not provisioned, you can put the software package on a USB device to downgrade the system to an earlier version. For information on using a USB device for loading system software, refer to [Update System Software from a USB Storage Device](#).

Determine the Software Version

Before you downgrade system software, Polycom recommends that you check the current system software version you are running.

To determine the software version you are running:

- » In the local interface go to **Settings > System Information > Information > System Detail** or click the **System** link in the web interface.

Delete System Settings

When you want to reinstall an older version of software with a USB device after upgrading to a later version, Polycom recommends first deleting your system settings.

To delete your system settings:

- » In the local interface, go to **Settings > System Information > Diagnostics > Reset System** and select **Delete System Settings**.

Downgrading Tips

Polycom recommends you review the following tips before downgrading your RealPresence Group system software:

- When you use your system within a DoD environment, be sure to contact your Information Assurance Office (IAO) for approval before using a USB device with your system.
- Before downgrading, use the release notes to verify the interoperability of the camera, peripheral, hardware, and software versions you plan to install.
- When you downgrade the RealPresence Group system software, the Polycom EagleEye Producer and the Polycom EagleEye Director are automatically downgraded to a compatible version.
- When you downgrade the system software, the Polycom RealPresence Touch software is automatically downloaded to a compatible version after being paired. However, the RealPresence Touch platform version 2.0 might not automatically downgrade to version 1.0. In this case, to manually downgrade from version 2.0 to 1.0, you must use a USB storage device or initiate a downgrade from a server repository that includes version 1.0.
- You must downgrade Polycom Touch Control software with a USB storage device.

- Because of changes in software functionality and the user interface, some settings might be lost when you upgrade or downgrade. Polycom recommends that you store your system settings using profiles and download your system directory before updating your system software. Do not manually edit locally saved profile and directory files.

Manage the System Remotely

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

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

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

See the following topics for remote management details:

- [System Web Interface](#)
- [Set Up and Configure Directory Servers](#)

System Web Interface

You can use the system web interface to perform most of the calling and configuration tasks you can perform on the local system. The system web interface supports the most commonly used web browsers. For a list of supported browsers, refer to the *Polycom RealPresence Group Series Release Notes* at support.polycom.com.

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

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

Access the System Web Interface

To access your system's web interface, you must open a web browser and enter the system's IP address.


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`).
- 3 Enter the Admin Remote Access Password, if one is set.

Enable Room and Call Monitoring

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

To enable room and call monitoring:

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

Remotely Monitor a Room or Call

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

To remotely monitor a room or call:

- 1 In the web interface, go to **Utilities** > **Tools** > **Remote Monitoring**.
- 2 You can perform the following tasks out of a call:
 - Wake the system
 - Show content
 - Adjust the near camera
 - Adjust system volume
 - View camera presets
- 3 You can perform these additional tasks in a call:
 - Change camera sources
 - Adjust the far camera
 - End a call

Managing System Profiles on the Web Interface

Administrators who manage systems that support multiple applications can use profiles to change system settings. You can store a 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: 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.

Store a Setting Profile

You can store the current setting profile on your computer.

To store a profile:

- 1 In the web interface, go to **Utilities > Services > Profile Center**.
- 2 Click **Download** next to **Current Settings Profile** to download the profile file from the system.
- 3 Save the file to a location on your computer.

Upload a Profile

You can upload a setting profile from your computer.

To upload a profile:

- 1 Reset the system to restore default settings.
- 2 In your web browser address line, enter the system's IP address.
- 3 In the web interface, go to **Utilities > Services > Profile Center**.
- 4 Next to **Upload Settings Profile**, click **Browse** and browse to the location of the profile `.csv` file on your computer.
- 5 Click **Open** to upload the `.csv` file to your system.

Send a Message to a System

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

To send a message to a system:

- 1 In the web interface, go to **Utilities > Send a Message**.
- 2 On the Send a Message screen, enter a message (up to 100 characters in length), then click **Send**.
The message is displayed for 15 seconds on the screen of the system that you are managing.

Set Up and Configure Directory Servers

To allow your users to search the directory servers to add contacts, you must set up and configure the directory servers in the RealPresence Group system web interface at **Admin Settings > Servers > Directory Servers**.

Setting 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 also use the RealPresence Touch device to set up directory servers. In the RealPresence Touch web interface, go to **Admin Settings > Servers > Directory Servers**. The following topics for system setup also apply to the RealPresence Touch.

Configuring a Directory Server

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
Microsoft Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: <ul style="list-style-type: none"> SIP address (SIP URI)
LDAP with H.350 or Active Directory	Any of the following: <ul style="list-style-type: none"> NTLM v2 only Basic Anonymous 	Not Supported	Might include: <ul style="list-style-type: none"> H.323 IP address (raw IPv4 address, DNS name, H.323 dialed digits, H.323 ID, or H.323 extension) SIP address (SIP URI) ISDN number Phone number*
Polycom GDS	Proprietary	Not Supported	Might include: <ul style="list-style-type: none"> H.323 IP address (raw IPv4 address, DNS name, or H.323 extension) ISDN number

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

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

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

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include: <ul style="list-style-type: none"> 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

For Microsoft configuration information, refer to [Microsoft Directory Servers](#).

Configure the Polycom GDS Directory Server

You can configure the Polycom GDS Directory Sever in standard operating mode.

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 screen.

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

Configure the LDAP Directory Server

You can configure the LDAP Directory Server in standard operating mode.

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 screen.

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

SNMP Condition Reports

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

- All alert conditions found on the system alert screen
- Details of jitter, latency, and packet loss
- Low battery power is detected in the remote control
- A system powers on
- Administrator logon is successful or unsuccessful
- A call fails for a reason other than a busy line
- A user requests help
- A telephone or video call connects or disconnects

SNMP features specific to version 3 include the following:

- Allows for secured connectivity between the console and the SNMP agent
- Supports both IPv4 and IPv6 networks
- Logs all configuration change events
- Supports a user-based security model
- Supports trap destination addresses

Download MIBs

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 system web interface.

To download a Polycom MIB:

- 1 In the web interface, go to **Admin Settings > Servers > SNMP**.
- 2 Click the desired link:
 - Download Legacy MIB
 - Download MIB

Configure SNMP Management

You can configure SNMP Management to give system administrators access to manage the system remotely.

To configure the 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 <code>public</code> . 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • CFB-AES128 • CBC-DES
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.
Engine ID	Specifies the unique ID of the SNMPv3 engine. This setting might be needed for matching the configuration of an SNMP console application. The Engine ID is automatically generated, but you can create your own ID, as long as it's between 10 and 32 hexadecimal digits. Each group of 2 hex digits can be separated by a colon character (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (therefore, <code>:F:</code> is equivalent to <code>:0f:</code>). 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.

Setting	Description
Transport Protocol	Specifies the transport protocol used: <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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.

Using a Provisioning Service

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

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

You can register your video conferencing 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 systems detect and register with it, refer to the *Polycom RealPresence Resource Manager System Operations Guide*.

- You can enter the registration information and attempt to register by going to the **Admin Settings** in the Polycom system web interface.

To enable 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.

Configure the Provisioning Service

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

To configure a provisioning service for Automatic Provisioning:

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

Setting	Description
Server Type	Specifies the type of provisioning server. Select RPRM, DMS, or CLOUD. <ul style="list-style-type: none"> • RPRM is the RealPresence Resource Manager. • DMS is the Broadsoft BroadWorks Device Management System. • CLOUD is the RP Cloud server.
Domain Name	Specifies the domain for registering to the provisioning service.
User Name	Specifies the endpoint's user name for registering to the provisioning service.
Password	Specifies the password that registers the system to the provisioning service.
Server Address	Specifies the address of the system running the provisioning service.

- 4 Select **Save** or **Update**. The system tries to register with the RealPresence Resource Manager or with a DMS system using NTLM authentication.

- 5 Verify that **Registration Status** changes from **Pending** to **Registered**. You might need to wait for a minute or two before the status changes.



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 RealPresence Group system, too. To avoid unintentionally locking a user out of network access in this case, systems do not automatically retry registration until you update the settings and register manually on the Provisioning Service screen.

Disable a Provisioning Service

You can disable the provisioning service.

To disable a provisioning service:

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



Note: For information on the provisioning discovery process, refer to the topic “Provision Server Discovery” in the *Polycom Zero Touch Provisioning Guide* at http://downloads.polycom.com/voice/ZTP/ZTP_ProvisioningGuide.pdf.

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 video conferencing 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 [Setting Up a Directory Server](#).
- Go to **Admin Settings > Servers > Provisioning Service** and enable provisioning. For more information about these settings, refer to [Using a Provisioning Service](#).

Polycom® RealPresence® Cloud Service

The Polycom® RealPresence® Cloud service enables service providers to configure RealPresence Group systems with a provisioning service. During the first-time system setup, the RealPresence Cloud service might be automatically configured and provisioned according to the service provider's parameters. If needed, you can enable and configure RealPresence Cloud mode in the system web interface.

Enable RealPresence Cloud Mode in the System Web Interface

If your system was not automatically configured and provisioned, you can enable and configure RealPresence Cloud mode in the system web interface.

To enable RealPresence Cloud mode:

- 1 In the system web interface, go to **Admin Settings > Servers > Provisioning Service**.
- 2 At **Enable Provisioning**, select the checkbox.
- 3 At **Server Type**, select **CLOUD**.
- 4 Click **Save**.

The registration status changes to **Registered** after 1 to 2 minutes.

Configure System Software

The following topics provide information on how to configure the software for Polycom video room systems and peripherals:


- [Configuring the RealPresence Group System](#)
- [View System Software Options](#)
- [Customize What Users See on the System Home Screen](#)
- [Enable Access to User Settings](#)
- [Restrict Access to User and Administrative Settings](#)

Configuring the RealPresence Group System

This section describes how to configure your RealPresence Group system by using the configuration screens on the local interface.

If you are in the room with the system, you can navigate the screens and enter information by using the remote control and the onscreen keyboard. When you reach a text field, press the **Select** button on the remote control to display the onscreen keyboard. Note that the onscreen keyboard is automatically displayed when you reach the **System Name** field in the setup wizard.

Be aware that only those configuration screens needed to get the system connected are included in the local interface. Most of the administrative settings are available only in the web interface.

Go to  > **Settings > Administration** in the system's local interface. The local interface has a subset of the administration settings that are available in the web interface. For information on accessing the web interface, refer to [System Web Interface](#).

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 at support.polycom.com.

Enable PKI Certificates

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

To enable PKI Certificates

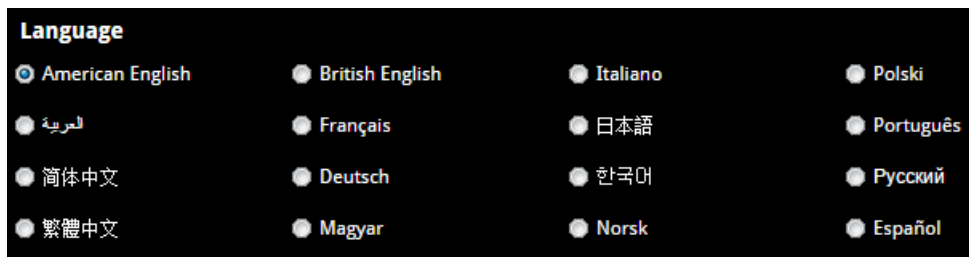
- 1 On the web interface, go to **Admin Settings > Network > LAN Properties > LAN Options**.
- 2 At **Host Name**, use the same name that the RealPresence Resource Manager uses to provision the system.

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

For more information about PKI certificates, refer to [Managing Certificates and Revocation](#). For more information about provisioning, refer to [Using 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 16 language fonts listed in the following figure. Other languages might not display correctly. The first character of a System Name must be a letter or a number instead of a dollar sign (\$) or underscore (_) character. Polycom supports double-byte characters for the system name.



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**.

View System Software Options

You can view the software options available on your system.

To view system options:

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

Activate System Options

If you want to activate your system options without upgrading your software, you do not need to download software or run the software update. The only thing you need is your system option key.

To activate system options:

- 1 Open a supported browser and go to the system's web interface.

- 2 Navigate to **Admin Settings > General Settings > Options**.
- 3 Enter the option key and click **Save**.

For more information about software and system option key codes, refer to [Available Software Options](#).

Customize What Users See on the System Home Screen

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

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 screen that are described in the following sections.

Speed Dial

You use speed dialing to quickly call an IP address designated as a Favorite. Speed Dial contacts are displayed on the system's local interface and on a paired RealPresence Touch device. Speed dial entries do not appear when the RealPresence Group system is paired with a Polycom Touch Control.

Enable Speed Dial

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

To enable speed dialing:

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

Add Speed Dial Contacts

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

To add speed dial contacts:

- 1 In the system web interface at **Speed Dial**, click **Edit**.
- 2 Enter a contact name and click **Search**.

- 3 For the contact you want to add, click **Add**.
- 4 To save your changes, click **Save**.

Image File Requirements for Speed Dial Contacts

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

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

Upload an Image File for Speed Dial Contacts

You can upload a photo or graphic for contacts in the system Speed Dial list.

To add an image file for speed dial contacts:

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

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

Remove Speed Dial Contacts

You can remove contacts from the Speed Dial list.

To remove speed dial contacts:

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

For details about calling Speed Dial contacts, refer to [Place a Call to Speed Dial Contacts](#).

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. The room system connects to Microsoft Exchange Server using the credentials you provide, or by automatically discovering the connection information based on an email address or SIP server address.

Connection to a calendaring service allows the room system to:

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



Note: 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.

Configure the Calendaring Service

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

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 room video system to connect to a calendaring service and retrieve meeting information.
Email	Specifies the mailbox account this system should monitor for calendar information. This should match the Primary SMTP Address for the account on Microsoft Exchange Server 2013/Skype for Business 2015, which displays as the value of the mail attribute in the account properties.
Domain	Specifies the domain for registering to the Microsoft Exchange Server 2013/Skype for Business 2015, in either NETBIOS or DNS notation, for example, either <code>company.local</code> or <code>COMPANY</code> . If you are using the Auto Discover Using setting, do not provide a value in this field.
User Name	Specifies the user name for registering to Microsoft Exchange Server 2013/Skype for Business 2015, with no domain information included. This can be the system name or an individual's name. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the user name for that account in this field.
Password	Specifies the system password for registering with Microsoft Exchange Server 2013/Skype for Business 2015. This can be the system password or an individual's password. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the password for that account in this field.

Setting	Description
Auto Discover Using	<p>Specifies how the system obtains the Microsoft Exchange Server/Skype for Business 2015 address. If you select Email Address, the system uses the value provided in the Email field. If you select SIP Server, the system uses the registered SIP server domain name configured for the RealPresence Group system.</p> <p>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.</p> <p>If after configuring the Calendaring Service a message displays that the system was unable to discover the service, ensure the information you provided is correct. For example, make sure the email address is in a valid <username@domain> format.</p> <p>You can also use an API command to automatically discover the Microsoft Exchange Server address. For more information, refer to the <i>Polycom RealPresence Group Series Integrator Reference Guide</i>.</p>
Microsoft Exchange Server	<p>Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access Server/Skype for Business 2015. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server's Virtual IP Address. If required, an IP address can be used instead of an FQDN, but Polycom recommends using the same FQDN that is used for Outlook clients.</p> <p>Provide a value in this field only if you want to manually provide connection information to Microsoft Exchange Server/Skype for Business 2015. Otherwise, use the Auto Discover Using setting that allows the system to automatically determine the connection information for Microsoft Exchange Server/Skype for Business 2015 and populate this field.</p>
Secure Connection Protocol	Specifies the connection protocol to use to connect to the server. Select Automatic or TLS 1.0 .
Meeting Reminder Time in Minutes	Specifies the number of minutes before the meeting that a reminder will display on the system.
Play Reminder Tone When Not in a Call	Specifies whether to play a sound along with the text reminder when the system is not in a call.
Show Information for Meetings Set to Private	Specifies whether to display details about meetings marked private.

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

Change the Background Image on the Home Screen

You can upload a custom image to display as the background of all monitors for a multi-screen system or on the main monitor of a single system. For a custom image on the RealPresence Group Series system, use the following guidelines.

You must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format with a file size less than 5 MB.

For details on changing the RealPresence Touch background image, refer to [Change the Home Screen Background Image on the RealPresence Touch](#).

To upload a background monitor image:

- 1 In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > Background**.
- 2 Browse to the desired image file and click **Choose File > Upload**.

The custom image displays on the main monitor or monitors.

Change the Background Startup Image on the Home Screen

The RealPresence Group system local interface displays a default background image when the system first powers on. You cannot delete this image, but you can upload your own image to replace it. When you change the image in the web interface, the new image also appears on the RealPresence Touch device.

You must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format.

To upload and use a startup background image:

- 1 In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > Startup Background**.
- 2 Click **Choose File** to search for and select the image you want to upload.
- 3 When the image name appears next to **Choose File**, click **Upload**.

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, users can call speed dial numbers, join calendar meetings, and answer calls.

You must create your speed dial numbers before users can access 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.

Enable Kiosk Mode

You must enable Kiosk Mode in the web interface before users can use it in the local interface. You also must either enable and configure Speed Dial or Calendaring before Kiosk Mode is available.




To enable Kiosk Mode:

- 1 In the system web interface, do one of the following:

- Enable and configure Speed Dial at **Admin Settings > General Settings > Home Screen Settings**. For details, see [Speed Dial](#).
 - Enable and configure the Calendaring Service at **Admin Settings > Servers > Calendaring Service**. For details, see [Calendaring Service](#).
- 2 Open **Kiosk Mode**, select **Enable Kiosk Mode** and click **Save**.

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
	<p>Camera</p> <p>This icon takes you to the Camera Control screen.</p>
	<p>Place a Call</p> <p>This icon takes you to the Place a Call screen, where you can manually dial a call, or can select a contact name from a list.</p>
	<p>Content</p> <p>This icon appears only when a content source is detected.</p>

Address Bar

The room system local interface displays an address bar at the bottom of the Home screen. The address bar can contain the following information:

- None
- IP Address
- H.323 Extension
- SIP Address
- Pairing Code

Choose Where to Display Elements on the Address Bar

You can customize where address bar elements appear on the Home screen of the local interface.

To display system information in the address bar:


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

Setting	Description
Address Bar (Left Element)	Allows you to select which element you want displayed on the left side of the address bar on the local interface. The choices are: <ul style="list-style-type: none"> • None • IP Address • H.323 Extension • Pairing Code
Address Bar (Right Element)	Allows you to select which element you want displayed on the right side of the address bar on the local interface. The choices are: <ul style="list-style-type: none"> • None • SIP Address • H.323 Extension • Pairing Code

Enable Access to User Settings

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

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 in the local interface, 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**.

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**.

Microsoft Interoperability

The following topics provide information for RealPresence Group system administrators on interoperability with Microsoft products and features:

- [Microsoft Directory Servers](#)
- [RTV and Skype-Hosted Conference Support](#)
- [AES Encryption for Skype Calls](#)
- [RealConnect](#)
- [Skype for Business Client 2015 Content Viewing](#)
- [Microsoft Skype Mode](#)

Microsoft Directory Servers

To allow your users to search the directory servers to add contacts, you must set up and configure the Microsoft directory servers in the RealPresence Group system web interface. 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.

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

For information on how to configure directory servers for Microsoft environments, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.

SIP Settings for Integration with Microsoft Servers

Integration with Microsoft servers allows Skype for Business 2015 and Polycom RealPresence Group system users to place audio and video calls to each other. For information about SIP settings and other Microsoft interoperability considerations, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.

RTV and Skype-Hosted Conference Support

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

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

AES Encryption for Skype Calls

AES encryption is a standard feature on all RealPresence Group systems. When it is enabled, the system automatically encrypts calls to other systems that have AES encryption enabled. For details on configuring AES encryption for Skype calls, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.

RealConnect

With the Native Support for RealConnect for Skype for Business Server 2015, 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 system, Polycom DMA, Polycom RealPresence Collaboration Server (RMX), and Skype for Business Server 2015 infrastructure automatically connects all of the environments together. This feature makes it easy for Skype and traditional videoconferencing system users to click to join calls from a Skype meeting invitation.

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

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

Skype for Business Client 2015 Content Viewing

RealPresence Group systems can view content from Skype for Business 2015 clients in active calls. Microsoft clients must initiate the content sharing request. The following content types from Skype clients are available:

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

There are a few limitations with Skype during content sharing and receiving, as follows:

- RealPresence Group systems can view content from Skype clients, but are not able to share content with Skype clients.

- RealPresence Group systems cannot share content, including content shared through People+Content IP and through the VisualBoard application, while actively receiving content from Skype clients.
- RealPresence Group systems do not support viewing PowerPoint (Office Web App), Whiteboard, Poll, and Q & A content from Skype clients. In multipoint conferences with more than one Skype client, Skype clients can choose these content sharing selections, but systems in the conference do not receive the content.
- For content to display properly, the room 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 Skype content viewing on RealPresence Group systems, Polycom recommends you deploy Skype Room System accounts instead of regular Skype user accounts for all room-based RealPresence Group systems. By using these accounts, enterprises avoid sharing content within the same room which results in an audio echo. To deploy these accounts, refer to the *Microsoft Skype for Business Room System Deployment Guide* on the Microsoft site.
- You can scroll and zoom content on the RealPresence Group system monitor, and RealPresence Group systems can control content received from Skype clients. For details, see the *Polycom RealPresence Group Series User Guide*.
- RealPresence Group systems do NOT support audio transmission from a Skype client.
- RealPresence Group systems do not initialize a desktop control request.
- If a Skype client wants to share its content with a RealPresence Group system, it needs to connect an A/V call with the system before sharing content.
- Because there is no cropping support for application sharing, the far site sees an application with a black background.
- While receiving content, the system cannot send content. You are prompted with a message indicating the restriction. As result, during content receiving, the system is not able to send a content source such as PPCIP or the VisualBoard application. The Skype client must stop sharing before the system is able to send 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 information on how to share content from Skype clients, refer to Microsoft documentation.

For details on configuring Skype for Business content viewing, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.



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

RDP Content Sharing

You can use Remote Desktop Protocol (RDP) to send content from a Skype for Business client to a RealPresence Group system.

Ending a Skype conference while RDP content is being shared ends all audio, video, and RDP content sessions. If a Skype client ends a call while sending RDP content, the video display might become unresponsive. Do one of the following:

- Ask the Skype client to stop presenting RDP content either before or after ending the call.
- Ask a Skype client in the AVMCU call to remove the Skype 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.

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

Microsoft Skype Mode

When a RealPresence Group system is registered with Skype for Business Online, Skype for Business 2015 Server, or Lync 2013 Server, and is paired with a RealPresence Touch device, you can enable the RealPresence Touch in Skype Mode user interface. In Skype Mode, the RealPresence Group system local interface has limited operations.

For information on enabling Skype mode, refer to the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

For information on using the Skype Mode user interface, refer to the *Polycom RealPresence Touch in Skype Mode Quick Tips* or the *Polycom RealPresence Group Series User Guide* at support.polycom.com.

Configuring System Network Settings

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

The 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:

- [Connecting to the LAN](#)
- [LLDP and LLDP-MED Support](#)
- [IP Network Settings](#)
- [Setting Call Preferences for SVC](#)
- [Configure Preferred Call Speeds](#)

Connecting 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 RealPresence Touch device
- Connect to a Polycom Touch Control (see [Configuring the Polycom Touch Control Software](#))

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.

Indicator Light	Connection Status
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 RealPresence Group systems.

To configure 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**.
- For IPv4, configure the following IP Address settings on the LAN Properties screen.

Setting	Description
IP Address	Specifies how the system obtains an IP address. <ul style="list-style-type: none"> 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.

- For IPv6, configure the following IP Address 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. <ul style="list-style-type: none"> Obtain IP address automatically—Select if the system gets an IP address from a SLAAC or a DHCP server on the LAN. Enter IP address manually—Select if the IP address will not be assigned automatically.

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

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

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

5 Configure the following LAN Options settings in the web interface at **Admin Settings > Network > LAN Properties > LAN Options**.

Setting	Description
Host Name (web interface only)	<p>Indicates the system's name. If the system discovers a valid System Name during the software installation process, a Host Name is automatically created. However, if an invalid system name is found, such as a System Name with a space, the system creates a Host Name with the following format: SystemType-XXXXXX, where XXXXXX is a set of random alphanumeric characters.</p> <p>IPv4 networks: The system sends the host name to the DHCP server to enable it to register the host name with the local DNS server, or it looks up the domain where the endpoint is registered (if supported).</p> <p>IPv6 networks: This function is not supported, so you can leave this field blank. However, configuring the field to contain the registered host name is recommended.</p>
Domain Name (web interface only)	<p>Displays the domain name currently assigned to the system.</p> <p>If the system does not automatically obtain a domain name, enter one here.</p>
Autonegotiation (under General Settings in local interface)	<p>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.</p> <p>Polycom recommends that you use autonegotiation to avoid network issues.</p>
LAN Speed (under General Settings in local interface)	<p>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.</p>
Duplex Mode (under General Settings in local interface)	<p>Specifies the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch.</p>
Ignore Redirect Messages (web interface only)	<p>Enables the system to ignore ICMP redirect messages.</p> <p>You should enable this setting under most circumstances.</p>
ICMP Transmission Rate Limit (millisec) (web interface only)	<p>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.</p> <p>This setting applies only to "error" ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests and replies.</p>
Generate Destination Unreachable Messages (web interface only)	<p>Generates an ICMP <code>Destination Unreachable</code> message if a packet cannot be delivered to its destination for reasons other than network congestion.</p>
Respond to Broadcast and Multicast Echo Requests (web interface only)	<p>Sends an ICMP <code>Echo Reply</code> message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the system.</p>

Setting	Description
IPv6 DAD Transmit Count (web interface only)	Specifies the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The system sends DAD messages to determine whether the address it is requesting is already in use. Select whether to transmit 0, 1, 2, or 3 DAD requests for an IPv6 address.
Enable PC LAN Port	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. The following authentication protocols are supported on RealPresence Group systems. <ul style="list-style-type: none"> • EAP-MD5 • EAP-PEAPv0 (MSCHAPv2) • EAP-TTLS • EAP-TLS
EAP/802.1X Identity (under EAP 802.1X in local interface)	Specifies the system's identity used for 802.1X authentication. This setting is available only when EAP/802.1X is enabled. The field cannot be blank.
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.

Setting	Description
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	<p>Sets the priority of control traffic on the LAN. Control traffic is any traffic consisting of control information associated with a call:</p> <ul style="list-style-type: none"> H.323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for room systems, is the Allow Other Participants in a Call to Control Your Camera setting under Admin Settings > Audio/Video > Video Inputs > General Camera Settings) SIP—SIP Signaling, FECC, Binary Floor Control Protocol (BFCP) <p>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.</p>

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

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 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.

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 room system discovers any of the following VLAN types in LLDP data from the network switch, the system automatically configures itself for one of them. The chosen VLAN type is based on the order of precedence, as follows:

- Video Conferencing VLAN
- Voice VLAN
- Voice Signaling VLAN

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

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

Enable LLDP Using a USB Storage Device

When you install a new room 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 system is powered off.
- 4 Insert the USB storage device into the system USB drive.
- 5 Power on the system.

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

Enable LLDP After the Setup Wizard Process

If you have already used 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**.

IP Network Settings

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

- H.323
- SIP

Configure 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.

To configure H.323 Settings:

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

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

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. <ul style="list-style-type: none"> • Off—Calls do not use a gatekeeper. • Auto—System attempts to automatically find an available gatekeeper. • Specify—Calls use the specified gatekeeper. This setting must be selected to enable H.235 Annex D Authentication. When you select a setting other than Off , the Registration Status is displayed below the Enable IP H.323 setting.
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	<ul style="list-style-type: none"> 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). <p>The primary gatekeeper IP address contains the IPv4 address the system registers with. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the system unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper.</p>

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 *Polycom RealPresence Group Series Release Notes*.

Configure SIP Settings

You can configure SIP settings in the system web interface.

To configure SIP settings:

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

Setting	Description
Enable SIP	Allows the SIP settings to be displayed and configured.
Enable AS-SIP	Enables the room 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 determines which protocol is required for the room system. Auto —Enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. TCP —Provides reliable transport via TCP for SIP signaling. UDP —Provides best-effort transport via UDP for SIP signaling. TLS —Provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. Select TLS if you want to encrypt SVC calls.
Force Connection Reuse	This setting is disabled by default (recommended). When disabled, it causes the system to use an ephemeral source port for all outgoing SIP messages. When enabled, it causes the system to use the active SIP listening port as the source port (5060 or 5061, depending on the negotiated SIP transport protocol in use). This can be useful to establish correct operation with remote SIP peer devices, which require that the source port match the contact port in SIP messages.
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	<p>Specifies the IP address or DNS name of the SIP Registrar Server. The address can be specified as either an IP address or a DNS fully qualified domain name (FQDN). If registering a remote system with an Edge Server, use the FQDN of the edge server.</p> <p>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.</p> <p>Enter the address and port using the following format:</p> <p><IP_Address>:<Port></p> <p><IP_Address> can be an IPv4 or IPv6 address, or a DNS FQDN such as <code>servername.company.com:6050</code>.</p> <p>Syntax Examples:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>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.</p> <p>The syntax used for this field is the same as for the Registrar Server field.</p>
Registrar Server Type	Specifies the registrar server type. Select Microsoft or Unknown .



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

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

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

When SIP is enabled on a RealPresence Group system that has the TIP option key code, the system can interoperate with TIP endpoints. 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: You cannot configure TIP without purchasing and installing a Telepresence Interoperability Protocol (TIP) option key code.

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.

Enable the AS-SIP Setting

The AS-SIP settings define service codes, network domains, and precedence levels for MLPP. You must enable AS-SIP settings before you can configure the settings for MLPP.

To enable AS-SIP:

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

Configure AS-SIP Settings for MLPP

You can configure AS-SIP settings for MLPP in the web interface.

To configure AS-SIP settings:


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

Add an AS-SIP Service Code

You can add an AS-SIP service code in the web interface.

To add an AS-SIP 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.

Delete an AS-SIP Service Code

You can delete an AS-SIP service code in the web interface.

To delete a AS-SIP service code:

You can delete an AS-SIP service code in the web interface.

- » Click .

Define AS-SIP Outbound Precedence Call Defaults

You can define AS-SIP outbound precedence call default settings for your system.

To define AS-SIP 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.

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

Define MLPP Network Domains

You can define MLPP network domain names for your system.

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**.

Add an MLPP Network Domain

You can add an MLPP network domain for your system.

To add an MLPP network domain:

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

Alternative Network Address Type (ANAT) for RealPresence Group Systems

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.

Consider the following best practices 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.

Configure Network Quality Settings

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

To configure Network Quality settings:

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

Setting	Description
Automatically Adjust People/Content Bandwidth	Specifies whether the system should automatically adjust the bandwidth necessary for the People stream or Content stream depending on the relative complexity of the people video, content video, or both. If this setting is enabled, the Quality Preference setting is not available.
Quality Preference	<p>Specifies which stream has precedence when attempting to compensate for network loss:</p> <ul style="list-style-type: none"> • Both People and Content streams • People streams • Content streams <p>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.</p> <p>This setting is not available when the Automatically Adjust People/Content Bandwidth setting is enabled.</p>
Type of Service	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Note: If AS-SIP is enabled and you select DiffServ, the DSCP values for audio and video defined for the negotiated call precedence level in the default network domain that was configured for outbound calls override the Video and Audio settings defined on this screen of the web interface. If you have not enabled AS-SIP, the Video and Audio values defined here are used.</p>
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	<p>Specifies the IP Precedence or Diffserv value for control traffic on any of the following channels:</p> <ul style="list-style-type: none"> • H.323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, which, for room systems, is the Allow Other Participants in a Call to Control Your Camera setting under Admin Settings > Audio/Video > Video Inputs > General Camera Settings) • SIP—SIP Signaling, FECC, Binary Floor Control Protocol (BFCP)
OA&M	Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC.
Maximum Transmission Unit Size	Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or select a maximize size.

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. For more details, see Lost Packet Recovery and Dynamic Bandwidth Settings .
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. For more details, see Lost Packet Recovery and Dynamic Bandwidth Settings .
MRC Bandwidth Allocation	Adjusts media bit stream bandwidth, reducing packet loss. Specifically designed for SVC-based calls. For more information on SVC, see Setting Call Preferences for SVC .
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 Settings

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 Room 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 the following settings.

Setting	Description
Fixed Ports	<p>Lets you specify whether to define the TCP and UDP ports.</p> <ul style="list-style-type: none"> • If the firewall is not H.323 compatible, enable this setting. The system assigns a range of ports starting with the TCP and UDP ports you specify. The system defaults to a range beginning with port 3230 for both TCP and UDP. <p>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.</p> <ul style="list-style-type: none"> • If the firewall is H.323 compatible or the system is not behind a firewall, disable this setting. <p>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.</p> <p>Range of UDP Ports: Because systems support ICE, the range of fixed UDP ports is 112. The system cycles through the available ports from call to call. After the system restarts, the first call begins with the first port number, either 49152 or 3230. Subsequent calls start with the last port used, for example, the first call uses ports 3230 to 3236, the second call uses ports 3236 to 3242, the third call uses ports 3242 through 3248, and so on.</p> <p>Fixed Ports Range and Filters:</p> <p>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.</p>
TCP Ports UDP Ports	<p>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.</p> <p>Note: You must also open the firewall's TCP port 1720 to allow H.323 traffic.</p>
Enable H.460 Firewall Traversal	<p>Allows the system to use H.460-based firewall traversal for IP calls. For more information, refer to H.460 NAT Firewall Traversal.</p>

Setting	Description
NAT	Specifies whether the system should determine the NAT Public WAN Address automatically. <ul style="list-style-type: none"> If the system is not behind a NAT or is connected to the IP network through a Virtual Private Network (VPN), select Off. If the system is behind a NAT that allows HTTP traffic, select Auto. If the system is behind a NAT that does not allow HTTP traffic, select Manual.
NAT Public (WAN) Address	Displays the address that callers from outside the LAN use to call your system. If you chose to configure the NAT manually, enter the NAT Public Address here. This field is editable only when NAT Configuration is set to Manual .
NAT is H.323 Compatible	Specifies that the system is behind a NAT that is capable of translating H.323 traffic. This field is visible only when NAT Configuration is set to Auto or Manual .
Address Displayed in Global Directory	Lets you choose whether to display this system's public or private address in the global directory. This field is visible only when NAT Configuration is set to Auto or Manual .
Enable SIP Keep-Alive Messages	Specifies whether to regularly transmit keep-alive messages on the SIP signaling channel and on all RTP sessions that are part of SIP calls. Keep-alive messages keep connections open through NAT/Firewall devices that are often used at the edges of both home and enterprise networks. When a system is deployed or registered in an Avaya SIP environment, Polycom recommends that you disable this setting to allow calls to connect fully.

In environments set up behind a firewall, firewall 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.

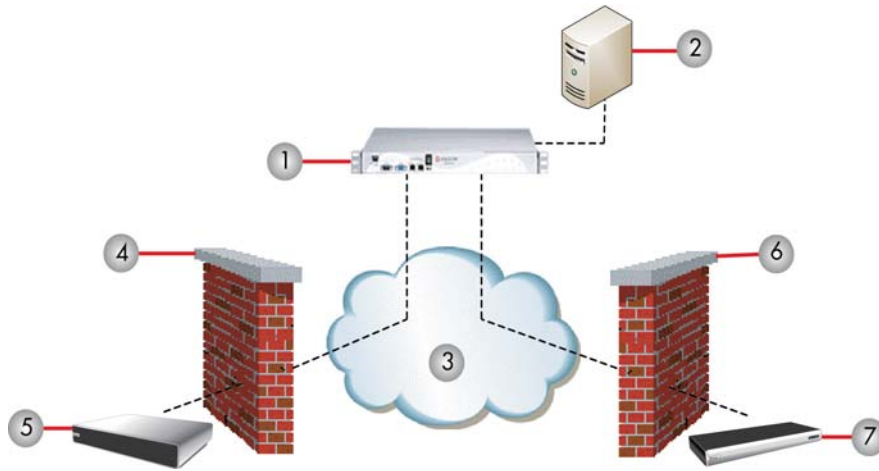


Caution: Systems deployed outside a firewall are potentially vulnerable to unauthorized access. Visit the Polycom Security section of the Knowledge Base at support.polycom.com for timely security information. You can also register to receive periodic email updates and advisories.

H.460 NAT Firewall Traversal

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

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



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

Configure the H.460 NAT Firewall Traversal

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

To configure the RealPresence Group system and firewall traversal:

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

Basic Firewall/NAT Traversal Connectivity

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

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

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

Setting Call Preferences for SVC

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

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

Configure 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)	<p>Specifies whether to use scalable or advanced video coding:</p> <ul style="list-style-type: none"> • SVC then AVC—Use SVC when possible; otherwise, use AVC. • AVC Only—This setting disables SVC. <p>This setting is not applicable to Skype-hosted calls, since SVC is negotiated automatically by Skype for Business Server 2015 or the Skype for Business 2015 client.</p>
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this setting if you know that H.239 is supported by the far -end sites you call.
Enable Audio-Only Calls	Specifies one additional outbound audio-only call from the RealPresence Group system. This occurs when a multipoint conference call hits the maximum number of calls allowed for the license type.
TIP	Specifies that TIP is enabled on a RealPresence Group system and that the system can interoperate with TIP endpoints. For details, refer to SIP Settings for Integration with the Telepresence Interoperability Protocol (TIP) .
Video Dialing Order	<p>Specifies how the system places video calls to directory entries that have more than one type of number.</p> <ul style="list-style-type: none"> • IP H.323 • SIP <p>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.</p>
Audio Dialing Order Preference 1	<p>Specifies the first audio preference for calls. The choices are:</p> <ul style="list-style-type: none"> • IP H.323 • SIP <p>Preference 1 will be attempted first, while Preference 2 will be attempted second.</p>
Audio Dialing Order Preference 2	<p>Specifies the second audio preference for calls. The choices are:</p> <ul style="list-style-type: none"> • IP H.323 • SIP <p>Preference 2 will be attempted second, while Preference 1 will be attempted first.</p>

Enable Automatic Answering of SVC Point-to-Point Calls

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

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

To enable Auto Answer Point-to-Point Video:

- 1 In the web interface, go to **Admin Settings > General Settings > System Settings > Call Settings**.

- From the Auto Answer Point-to-Point Video list, select **Yes**.

Enable SVC Preference (H.264) for Calls

You can enable the order preference for SVC and AVC calls.

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

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

Configure Preferred Call Speeds

You can configure calls speeds in the web interface.

To configure call speeds:

- In the web interface, go to **Admin Settings > Network > Dialing Preference > Preferred Speeds**.
- Configure the following 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: <ul style="list-style-type: none"> 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: 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.

Monitors and Cameras

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

- [Receiving and Displaying Video in High Definition](#)
- [Configuring Monitor Settings](#)
- [Monitor Profiles and Video Layout Panel Views](#)
- [Touch Monitor User Interface](#)
- [Monitor Resolutions for the RealPresence Group System Model Types](#)
- [Recording Calls with Polycom® RealPresence® Media Suite](#)
- [Polycom Cameras](#)
- [Connecting Cameras to RealPresence Group Systems](#)
- [Powering Cameras with RealPresence Group Systems](#)
- [Configuring Camera Settings](#)
- [Configuring Video Input Settings](#)
- [Camera Presets](#)

Receiving and Displaying Video in High Definition

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

Systems with HD capability can send video in wide-screen, HD format. For information about frame rates for content, refer to [Content Sharing](#).

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.

When the far site sends HD video, 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). 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 system or a conferencing platform that supports HD such as Polycom RealPresence Collaboration Server 1500 or 2000.
- The system host must have the appropriate option keys installed.
- All systems in the call must support HD (720p at 30 fps) and H.264.
- The call rate must be high enough to support HD resolution, as shown in [Multipoint Call Speeds](#).
- The call cannot be cascaded.

For more information about multipoint calls, refer to [Multipoint Call Speeds](#).

Full-Motion HD Video and Audio

With RealPresence Group 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 RealPresence Group systems, you share full-motion HD people and content at the same time, which helps eliminate compromises when sharing across distances.

Configuring 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.



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

For more information about connecting monitors to RealPresence Group systems, refer to [System Panel Views](#).

Configure Monitor Settings

You might need to configure monitor settings for the monitors connected to your system.

To configure monitors:

- 1 In the system web interface, go to **Admin Settings > Audio/Video > Monitors**.
- 2 Configure these settings on the Monitors screen. The settings for Monitor 1, Monitor 2, and Monitor 3 are nearly the same, although the available features can be different. Monitor 3 is available for RealPresence Group 700 systems only.

Setting	Description
Enable	<p>Specifies the monitor setting:</p> <ul style="list-style-type: none"> • 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 (not available for Monitor 1)
Monitor Profile	<p>Specifies which profile to use for this monitor. The choices depend on how many monitors the system uses and which monitor you are configuring. For details, Monitor Profiles and Video Layout Panel Views.</p>
Video Format	<p>Specifies the monitor's format. Depending on which RealPresence Group system and monitor you configure, the choices are:</p> <ul style="list-style-type: none"> • HDMI • DVI • Component • VGA <p>This setting is unavailable when you select Auto for the Enable setting.</p> <p>Note: To disable HDMI output when using 3.5mm audio output, do the following. In the web interface, go to Admin Settings > Audio/Video > Monitors and set the Monitor 1 Enable setting to Manual. At Video Format, select DVI.</p>
Resolution	<p>Specifies the resolution for the monitor.</p> <p>Note: This setting is unavailable when you select Auto for the Enable setting.</p>

Monitor Profiles and Video Layout Panel Views

Monitor Profiles set the preferences for which video layout panel views are shown on each monitor connected to the system. You can customize the monitor configuration to match your environment or your desired meeting experience.

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

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

Configure Monitor Profile Settings

You can configure monitor layout profile settings for each monitor connected to the RealPresence Group system.

To configure monitor layout profile settings:

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

Monitor Profile Name	Description	Monitor 1	Monitor 2	Monitor 3 (RealPresence Group 700 only)
Content, then Far, then Near	Sets Monitors 1 or 2 to share content. The system displays the panels in this order of priority: Content first in the largest panel, then any remote speakers (Far), then the local camera (Near). Default for Monitor 1 if only one monitor is connected to the system. Default for Monitor 2 if 2 or more monitors are connected to the system.	Yes	Yes	No
Far, then Near	Sets Monitor 1 or 2 to show the far-end in the largest panel, then the near-end. Default for Monitor 1 if there are 2 or more monitors connected to the system.	Yes	Yes	No
Far Only	Sets Monitors 1, 2, or 3 to show the far-end only.	Yes	Yes	Yes
Content, then Near	Sets Monitor 2 to display shared content in the larger panel. If no content is displayed, the monitor shows the person speaking at the near-end.	No	Yes	No
Content, then Far	Sets Monitors 1 or 2 to display shared content in the larger panel. If no content is shared, the monitor displays the far-end speaker panel only.	Yes	Yes	No
Content Only	Sets Monitor 2 or 3 to display shared content as the only panel. If no content is shared, the monitor shows the room background.	No	Yes	Yes
Near Only	Sets Monitor 2 or 3 to show the near-end site only. Another name for this view is Self View.	No	Yes	Yes

Monitor Profile Name	Description	Monitor 1	Monitor 2	Monitor 3 (RealPresence Group 700 only)
Record Mode	Sets Monitor 3 to display shared content or the person speaking. Content sharing takes priority over displaying the person speaking. Select this setting to record near, far, and content audio. If someone is sharing content, the video is recorded in full screen. If no one is sharing content, the speaker is recorded in full screen. Available only on RealPresence Group 700 systems.	No	No	Yes
Record Mode With Content	Sets Monitor 3 to show the current person speaking, regardless of the speaker's location. Select this setting to record near, far, and content audio. Only the speaker is recorded in full screen. Available only on RealPresence Group 700 systems.	No	No	Yes

The Automatic Self View setting can also affect what displays on the monitors. For more information, refer to [Configure Call Settings](#).

Touch Monitor User Interface

RealPresence Group systems have touch user interface capability when connected to touch-capable monitors. The local user interface works with both touch interaction and the RealPresence Group system remote control. When VisualBoard or Skype for Business content is playing, the touch is redirected to those interfaces for control and annotation. When these tools are minimized to show the main user interface, or when a notification comes up, touch is directed to the primary monitor so that user can control the user interface. These are the supported monitor scenarios:

- Single touch monitor: If only one touch monitor is detected, touch interactions are enabled by default. You can now interact with the primary user interface using touch. When VisualBoard or Skype for Business content is playing, the touch is redirected to those interfaces for control and annotation. When these tools are minimized to show the main user interface, or when a notification is displayed, touch is directed to primary so that user can control the primary user interface.
- Two or more monitors: For multiple monitor setups, and if at least one monitor is touch, touch interaction is not enabled by default.
 - If the touch monitor is attached as primary, and is configured as a touch monitor, touch interaction is enabled on that monitor to control the primary user interface.

- The Diagnostic configuration setting appears only if there is more than one monitor attached, and there is at least one touch monitor attached.




Note: To enable the touch monitor interface on RealPresence Group 300 and RealPresence Group 310 systems, you must activate the dual monitor option key in the system's web interface. For information on the activation procedure, refer to [Software and System Option Keys](#).

Configure Secondary Monitors for Content in a Multiple Touch Monitor Environment

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

To configure secondary monitors for content:

- 1 In the local interface, use a remote control to navigate to  > **Settings** > **Administration** > **Touch Monitor** > **Configure**.
- 2 Under **Enable touch interaction on this monitor**, click **Start**.
- 3 Click the screen on the area indicated.
The system recognizes the monitor as a touch monitor.
- 4 In the system's web interface, go to **Admin Settings** > **Audio/Video** > **Monitors**.
- 5 For Monitor 1 at **Enable**, select **Auto** or **Manual**. At **Monitor Profile**, select **Far, Then Near** or **Far Only**.
- 6 For Monitor 2, at **Monitor Profile**, select **Content Only** or one of the other content profiles.

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

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

Monitor Resolutions for the RealPresence Group System Model Types

You might need to know the monitor resolutions for the particular RealPresence Group system that you are using. The following tables provide resolution rates for the video standards NTSC and PAL for Monitor 1, Monitor 2, and Monitor 3 (RealPresence Group 700 system only).

Monitor 1 Resolution Rates

RealPresence Group System Type	NTSC Video Standard	PAL Video Standard
RealPresence Group 300/500	HDMI/DVI: 1080p60, 720p60, 1080i60	HDMI/DVI: 1080p50, 720p50, 1080i50
RealPresence Group 700	HDMI/DVI: 1080p60, 720p60, 1080i60	HDMI/DVI: 1080p50, 720p50, 1080i50
	VGA: 1080p60, 720p60	VGA: 1080p60, 720p60
	Component: 1080p60, 720p60, 1080i60	Component: 1080p50, 720p50, 1080i50

Monitor 2 Resolution Rates

RealPresence Group System Type	NTSC Video Standard	PAL Video Standard
RealPresence Group 300/500	HDMI/DVI: 1080p60, 1280x1024p60, 720p60, 1080i60, 1024x768p60	HDMI/DVI: 1080p50, 1280x1024p60, 720p50, 1080i50, 1024x768p60
RealPresence Group 700	HDMI/DVI: 1080p60, 1280x1024p60, 720p60, 1080i60, 1024x768p60	HDMI/DVI: 1080p50, 1280x1024p60, 720p50, 1080i50, 1024x768p60
	VGA: 1080p60, 1280x1024p60, 720p60, 1024x768p60	VGA: 1080p60, 1280x1024p60, 720p60, 1024x768p60
	Component: 1080p60, 720p 60, 1080i60	Component: 1080p50, 720p 50, 1080i50

Monitor 3 Resolution Rates

RealPresence Group System Type	NTSC Video Standard	PAL Video Standard
RealPresence Group 700	HDMI/DVI 1080p60, 1280x1024p60, 720p60, 1080i60, 1024x768p60	HDMI/DVI 1080p50, 1280x1024p60, 720p50, 1080i50, 1024x768p60
	VGA: 1080p60, 1280x1024p60, 720p60, 1024x768p60	VGA: 1080p50, 1280x1024p60, 720p60, 1024x768p60
	Component: 1080p60, 720p 60, 1080i60	Component: 1080p50, 720p 50, 1080i50

Recording Calls with Polycom® RealPresence® Media Suite

Users can use Polycom® RealPresence® Media Suite solution to record calls directly from the RealPresence Group Series system, remotely log in to Polycom RealPresence Media Suite to record or live stream calls, or use Monitor 3 for the RealPresence Group 700 system.

RealPresence Media Suite is an enterprise recording, streaming and video content management solution that offers users and administrators a self-service user portal to record calls on RealPresence Group systems.

Enable Recording Controls

After you enable RealPresence Media Suite for a system, users can record video calls, create a live stream, and control recordings on the system. Once enabled, recording controls display on the system, and users can initiate and control a recording using the remote control and the touch interface.

To enable RealPresence Media Suite recording for a system, an administrator must enter user credentials for the system.

To enable recording controls:

- 1 In the web interface, navigate to **Admin Settings > Servers > Recording Service**.
- 2 Select the **Enable RealPresence Media Suite** check box.
- 3 Enter the user credentials and server address for the system's RealPresence Media Suite account.

Recording Calls Remotely

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

The RealPresence Media Suite solution allows users to record and live stream a call by dialing into a system from a RealPresence Media Suite portal. If users have access to a RealPresence Media Suite portal, they can log in to the portal to dial in to a system from which they want to record a call. This method is also ideal for an administrator of a remote system. For information about using this method, refer to the *Polycom*

RealPresence Media Suite, Appliance Edition User Guide or *Polycom RealPresence Media Suite, Virtual Edition User Guide* at support.polycom.com.

Users of a system can also remotely record calls in the following ways:

- **Dial RealPresence Media Suite directly:** Use the default recording settings defined by a RealPresence Media Suite administrator. Before recording a call using this method, users must obtain the IP address, H.323 extension, or SIP URL of the RealPresence Media Suite.
- **Dial a RealPresence Media Suite Video Recording Room (VRR):** A VRR is a virtual capture server with a specific recording profile that is defined by a RealPresence Media Suite administrator. Before recording a call using this method, users must obtain the VRR number and the IP address, H.323 ID, or SIP address of the RealPresence Media Suite.

When a recording is initiated remotely from the RealPresence Media Suite user portal, users cannot control the recording from the system.

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



Note: If you have access to a RealPresence Media Suite portal, you can use additional features, such as copying the URL for a recording to share with others. For more features, see the *Polycom RealPresence Media Suite User Guide* at support.polycom.com.

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 both the RealPresence Group and the RealPresence Media Suite system are not registered to the gatekeeper or to a SIP server, dial the RealPresence Media Suite IP address.	10.11.12.13
	If both the RealPresence Group and the RealPresence Media Suite system are registered to a gatekeeper, dial the RealPresence Media Suite E.164 extension for H.323.	1234
	If both the RealPresence Group and the RealPresence Media Suite system are registered to a SIP server, dial the RealPresence Media Suite SIP address.	CS123

Media Suite Type	Connection Method	Example
VRR	For 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 System

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

To enable recording on a RealPresence Group 700 system:

- 1 In the system web interface, go to **Admin Settings > Servers > Recording Service**.
- 2 At **Enable RealPresence Media Suite**, select the checkbox.
- 3 Enter the connection information in the following settings.

Setting	Description
Domain Name	Enter the server domain name for RealPresence Media Suite.
User Name	Enter the server user name for RealPresence Media Suite.
Password	Enter the server password for RealPresence Media Suite.
Server Address	Enter the IP address for the RealPresence Media Suite server.

- 4 Click **Save** to save the connection settings.

Configure Monitor Settings for Recording on a RealPresence Group 700 System

You can configure monitor settings for recording on a RealPresence Group 700 system.

To configure monitor settings for recording:

- 1 In the system web interface, select **Admin Settings > Audio/Video > Monitors**.
- 2 Select one of the following settings for Monitor 3:
 - **Record Mode with Content.** Select this setting to record what the speaker says, along with any content audio. This records near, far, and content audio.
 - **Record Mode.** Select this setting to record only what the speaker says. This records near, far, and content audio.

Maximize HDTV Video Display

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

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

Before attaching your RealPresence 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.

Sleep Settings Prevent Monitor Burn-In

Monitors and 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.

CEC Monitor Controls

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

The following CEC features are available:

- **One Touch Play**—Use the system remote to wake up the monitors. All connected CEC-capable monitors are powered on, and their displays are switched to room system input.

- **System Standby**—When the room system enters sleep mode, all connected CEC-capable monitors are switched to standby mode for power saving. When waking up, the monitors are powered up before they display system video.

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

Enabling Monitors to Support CEC

CEC functionality is enabled by default on RealPresence Group systems. 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: Each monitor brand might have different CEC feature and sub-feature settings. Ensure that all monitors connected to the RealPresence Group system are all enabled for CEC.

Enable CEC Controls

You can enable CEC on RealPresence Group systems.

To enable CEC controls:

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

Disable CEC Controls

You can disable CEC on RealPresence Group systems.

To disable CEC controls:

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



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

Polycom Cameras

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 can receive IR signals. RealPresence Group systems have built-in IR receivers to receive signals from the remote control. 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 RealPresence Group systems. They support 1080p60 resolution and are available with either 12x or 4x zoom capabilities. Additional digital cables of 300mm, 457mm and 1m lengths are available.



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 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™ Producer Camera

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

When an EagleEye Producer is connected to a RealPresence Group system, camera tracking starts automatically when you initiate a call and stops automatically when you hang up from a call. You can also manually start camera tracking in the local interface of the RealPresence Group system. EagleEye Producer

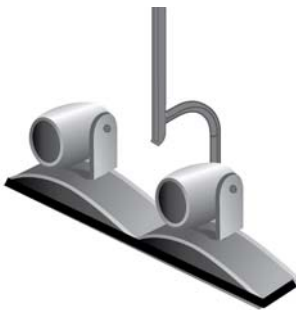
detects the people in the room and sets up framing. You can set the tracking mode and speed, and specify the type of group framing, which enables automatic tracking of group participants in the room and frames the active speaker.

Polycom EagleEye Director

The EagleEye Director is a high-end automatic camera positioning system that works in conjunction with a 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: The EagleEye Director is compatible with Polycom EagleEye III cameras.



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.

Connecting 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. Ensure that the system is powered off before you connect devices to it.



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

Powering 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 remote control, use one of these solutions:

- Provide direct power to the EagleEye III or EagleEye IV camera with the elective EagleEye camera power supply, 1465-52748-040. This allows the IR sensor to remain powered on, so that the camera is capable of receiving IR commands from the remote control.
- Position the 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 for Cameras

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 cameras to wake from a Sleep state through a signal received by the camera's IR sensor. The camera does not require any additional power supply or IR extender.

Configuring Camera Settings

For an illustrated view of the inputs and outputs available for each system, refer to [System Panel Views](#). Although you can connect devices that are not automatically discovered, the available choices in the interface might not be the same as they would for automatically discovered devices. For example, if you connect an unsupported camera, the system attempts to show video. Polycom does not guarantee that the results will be optimal or that you can set up the camera the same as for a supported camera.

Configure Camera and Video Settings

You can configure camera settings for cameras connected to your system.

To configure camera settings:

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

Configure General Camera Settings

Setting	Description
Allow Other Participants In a Call to Control Your Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this setting is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site. This is sometimes also called Far End Camera Control (FECC).
Power Frequency	Specifies the power line frequency for your system. In most cases, the system defaults to the correct power line frequency, based on the video standard used in the country where the system is located. This setting allows you to adapt the system in areas where the power line frequency does not match the video standard used. You might need to change this setting to avoid flicker from the fluorescent lights in your conference room.
Make This Camera Your Main Camera	Specifies 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.
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.

Configuring Video Input Settings

Settings for each video input connected to your room system are available in the system web interface at **Admin Settings > Audio/Video > Video Inputs**.



Note: Settings that don't apply to the selected video input are not displayed. For example, if a specific camera is not connected to your room system, the related settings are not displayed.

To configure video input settings:

- » Configure the following video input settings for your system.

Setting	Description
Enable	<p>Specifies the video input type. You can also choose to Auto select the video input type.</p> <p>For RealPresence Group 300/310/500 systems, Input 1 is always HDCI, so the Enable setting is not displayed.</p> <p>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.</p>
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	<p>Specifies whether the video input is to be used for People or Content.</p> <p>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.</p>
Input format	Specifies the source type of the device. This setting is read only unless the system does not detect the device.
Orientation	<p>Specifies the orientation of the camera. You can choose one of the following camera positions:</p> <ul style="list-style-type: none"> • Normal— This default setting is a non-inverted camera orientation. • Inverted—This is an upside-down camera orientation. <p>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.</p>
Optimized for	<p>Specifies Motion or Sharpness for the video input.</p> <ul style="list-style-type: none"> • 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)	<p>Specifies the type of camera tracking:</p> <ul style="list-style-type: none"> • 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. <p>If camera tracking has not been calibrated, Tracking Mode is unavailable.</p> <p>Note: Setting is available only when you have installed an EagleEye Producer.</p>
Tracking Speed (EagleEye Director)	<p>Determines how quickly the system finds someone new and switches to that person.</p> <p>Note: Setting is available only when you have installed an EagleEye Producer.</p>

Setting	Description
Backlight Compensation	<p>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.</p> <p>Enabling this setting helps to relieve a bright background, which can impact the tracking performance of the EagleEye Director.</p>
White Balance	<p>Specifies how the camera compensates for variations in room light sources. Select Auto, Manual, or a color temperature value.</p> <ul style="list-style-type: none"> • Auto - Polycom recommends this setting for most situations. It calculates the best white balance setting based upon lighting conditions in the room. • Manual - Use this setting for rooms where the Auto and fixed values do not provide acceptable color reproduction. <ul style="list-style-type: none"> ▲ After you set the White Balance to Manual, fill the camera's field of view with a flat white object, such as a piece of paper. For best results, the object should be uniformly illuminated with light that is representative of the room lighting that will be used in the conference, rather than light from a display, another area, or a shadow. After the object is in place, click Calibrate. • 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 a sampling of some of the values you might see in the interface: <ul style="list-style-type: none"> • 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 saturated the color is.
Tracking Mode (Polycom EagleEye Producer)	<p>Specifies the tracking mode:</p> <ul style="list-style-type: none"> • Frame Speaker - This is the default setting. Enables automatic tracking of group participants in the room and frames the active speaker. Note that when the tracking mode is set to Frame Speaker and the local microphone is muted, the camera tracking mode automatically switches to Frame Group. • Frame Group - Enables automatic tracking and framing of the group participants in the room without displaying the camera motion between frames. • Frame Group with Transition - Enables automatic tracking and framing of the group of participants in the room. • Off - Disables automatic tracking. All camera control must be handled manually. <p>Note: Setting is available only when you have installed an EagleEye Producer.</p>

Setting	Description
Tracking Speed (Polycom EagleEye Producer)	<p>Specifies the tracking speed:</p> <ul style="list-style-type: none"> • 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. <p>Note: Setting is available only when you have installed an EagleEye Producer.</p>
Framing Size (Polycom EagleEye Producer)	<p>Specifies the group framing view:</p> <ul style="list-style-type: none"> • 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. <p>EagleEye Producer can detect the position of a person within six meters or less.</p> <p>Note: Setting is available only when you have installed an EagleEye Producer.</p>
Automatic Image Calibration	<p>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.</p>

For details about using EagleEye Producer, refer to the *Polycom EagleEye Producer User Guide* at support.polycom.com.

Configure a Third-Party Camera

The RealPresence Group 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 get the serial data to and from the camera.

To configure a third-party 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: 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.

EagleEye IV Camera Orientation

After you have connected your EagleEye IV camera, you might want to change the camera's orientation. EagleEye IV cameras can be mounted upside down to accommodate special video conferencing situations. The orientation of the video display and pan/tilt functions work transparently so that the inverted position is transparent to end users. The default orientation is normal, or not inverted.

Enable an Inverted Camera Position for the EagleEye IV Camera

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

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 a Normal Camera Position

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

To enable the normal 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 [Configuring Video Input Settings](#).

Setting 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.

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

Updating EagleEye Producer with RealPresence Group Systems

Updates to Polycom EagleEye Producer software are included with the RealPresence Group system software updates. To update your EagleEye Producer, connect it to the 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: 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 RealPresence Group system software version. For more information on supported versions, go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html and click the **Current Polycom Interoperability Matrix** link.

Change Camera Tracking Settings

The Polycom EagleEye Producer detects the people in the room and provides framing during a conference. Frame Speaker with a Normal tracking speed and Medium view is enabled by default.

Polycom recommends calibrating the Polycom EagleEye Producer before adjusting camera features. For instructions on how to calibrate the Polycom EagleEye Producer, refer to the *Polycom RealPresence EagleEye Producer User Guide* at 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 > General Camera Settings** and select the input used by the Polycom EagleEye Producer.

2 Configure the following settings.

Setting	Description
Tracking Mode	<p>Specifies the tracking mode:</p> <ul style="list-style-type: none"> • Frame Speaker - This is the default setting. During a conference, this mode frames the active speaker, then when someone else starts speaking, the camera view changes to frame the new speaker. Note that when the tracking mode is set to Frame Speaker and the local microphone is muted, the camera tracking mode automatically switches to Frame Group. • Frame Group - Enables automatic tracking and framing of the group participants in the room without displaying the camera motion between frames. • Frame Group with Transition - 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	<p>Specifies the tracking speed:</p> <ul style="list-style-type: none"> • Slow - Detects meeting participants at a slow speed rate. • Normal - This is the default tracking speed. Detects meeting participants at a normal speed rate. • Fast - Detects meeting participants at a fast speed rate.
Framing Size	<p>Specifies the framing view:</p> <ul style="list-style-type: none"> • 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.

Turn on Camera Tracking for the EagleEye Producer

You can turn on camera tracking in the local interface. If camera tracking is enabled, when you start a call, camera tracking starts automatically; when you end a call, camera tracking stops automatically.

To turn on camera tracking:

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

Turn Off camera Tracking for the EagleEye Producer

You can turn off camera tracking in the local interface.

To turn off camera tracking:

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



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

Automatically Calibrate the EagleEye Producer

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 [Change Camera Tracking Settings](#).
- 3 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 for the EagleEye Producer

You might need to view the system status of an EagleEye Producer on a RealPresence Group system interface.

To view system status for an EagleEye Producer:

- » Do one of the following:
 - In the local interface of the system, go to **Settings > System Information > Status**.
 - In the web interface of the 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 RealPresence Group Series User Guide* on support.polycom.com.

Configure the Polycom EagleEye Director

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

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

To set up the EagleEye Director:

- 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 screen. 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. For details, refer to [Adjust the Room View of the EagleEye Director](#).




Note: 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 screen 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: Ensure that only one person speaks while you are calibrating the cameras and keep the background quiet. If you rearrange or move the 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 of the EagleEye Director

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


To 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 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 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.


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 EagleEye Director.
 - ◆ Enable the **Use Voices to Track People** setting.
 - If the RealPresence Group system is paired with a Polycom touch device, follow these steps:
 - 1 On the touch device, touch **Cameras** on the Home screen or the Call screen.
 - 2 If the EagleEye Director is not currently selected, select it.
 - 3 Touch **Select Cameras** and select the EagleEye Director camera.
 - 4 Touch **Control Camera**.
 - 5 Select **Start Camera Tracking**.

Disable Camera Tracking with EagleEye Director

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

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

EagleEye Director Camera Tracking in the Local Interface

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

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

- Camera tracking starts automatically when you make a call.
- Camera tracking stops after you hang up a call.
- Camera tracking temporarily stops when you mute the RealPresence 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: 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 [Configure the Polycom EagleEye Director](#).

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 a touch device, such as the RealPresence Touch. Each preset stores the camera number, its zoom level, and the direction it points (if appropriate).

If a Polycom touch device is paired with a RealPresence Group system, you must use the touch device to create presets. For more information about creating and using presets, refer to the *Polycom RealPresence Group Series User Guide* or 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: If you use a EagleEye Director with your RealPresence Group system, you cannot use presets for voice tracking.

Configure FECC on a Far-end Site Camera

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

To configure FECC on the far-end site camera:

- » In the web interface, go to **Admin Settings > Audio/Video > Video Inputs > General Camera Settings** and select **Allow Other Participants in a Call to Control Your Camera**.

For details on how to create camera presets, or how to move a camera to a stored preset, refer to the *Polycom RealPresence Group Series User Guide*.

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 system web interface.

- [Available Microphone Inputs by System](#)
- [Audio Input Tips by Microphone Type](#)
- [Audio Input Configuration Selections](#)
- [Audio Output](#)
- [Configure Audio Settings](#)
- [Test StereoSurround](#)
- [Acoustic Fence Technology](#)

For specific details regarding how to connect audio inputs and speakers, refer to the appropriate RealPresence Group system setup sheet and [System Panel Views](#). For information about required audio 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.

Polycom EagleEye Acoustic Microphones

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 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 room system microphone input while an 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 Selections

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 [Configure Audio Input Settings](#).

Microphone Inputs 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
- EagleEye Acoustic with microphones enabled

Microphone Inputs 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
- EagleEye Acoustic with microphones enabled

Third-Party Microphones

You can connect third-party microphones directly to audio input 1 on a RealPresence Group system, or through a line-level mixer to the AUX audio input on any RealPresence Group system. For information about configuring third-party microphones, refer to [Set Up Third-party Microphones](#).

SoundStructure Digital Mixer

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






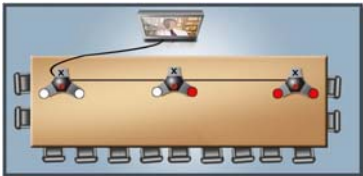
When incorporating a SoundStructure digital mixer, remember the following:


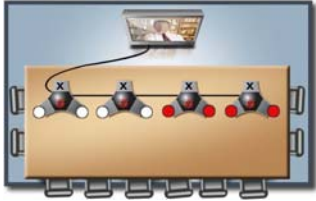
- Connect a SoundStructure digital mixer using the digital microphone input on the room system.
- Adjusting the volume on a room system changes the volume of the SoundStructure digital mixer that is connected.
- The following configuration settings are not available on a RealPresence Group system when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

The digital mixer allows you to provide a microphone for each call participant in a boardroom. For connection details, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.

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.



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 RealPresence Group systems 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 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 Panel Views](#).

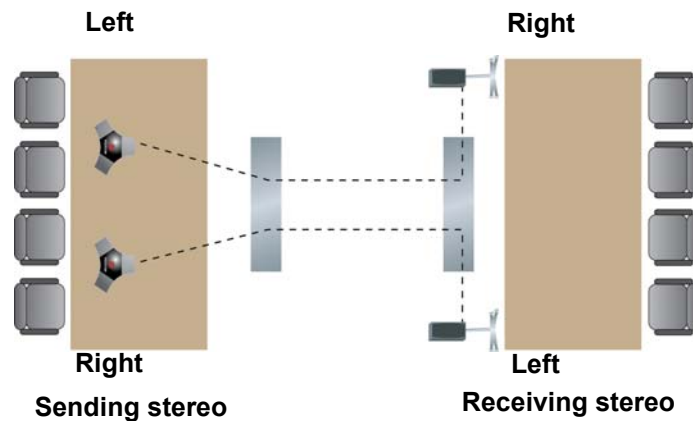
Speaker Placement to Receive Stereo from Far Sites

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

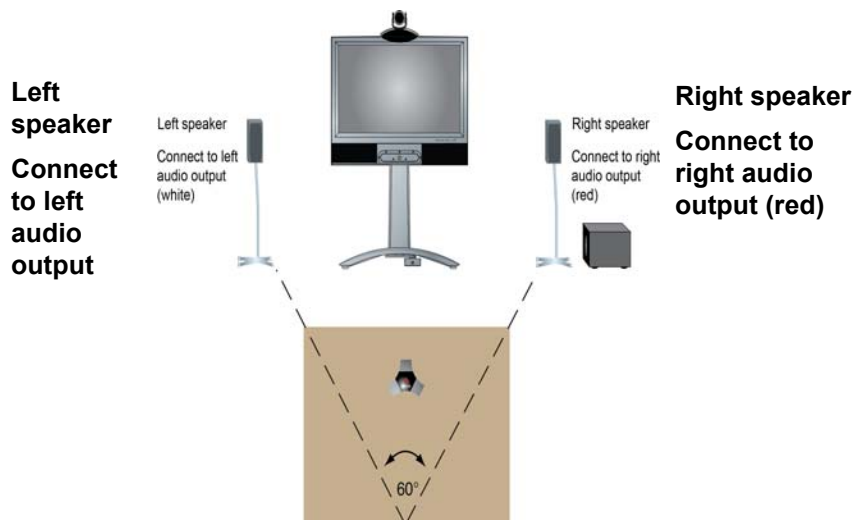
When a RealPresence Group system is configured for Polycom StereoSurround, the audio inputs and outputs are all treated as stereo. Otherwise, all audio inputs and outputs are mono.

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.

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



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



Set the Speaker Volume

You can set and test the volume of external speakers attached to your room system.

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

You can configure audio settings in the web interface. Some audio settings are unavailable when a SoundStructure digital mixer is connected to the RealPresence Group system. For more information, refer to [Configure Audio Output Settings](#).

To configure audio settings:

- 1 In the web interface, go to **Admin Settings > Audio/Video > Audio**.
- 2 Configure the Audio settings described in the following table.

Setting	Description
Polycom StereoSurround	Specifies that Polycom StereoSurround is used for all calls. To send or receive stereo audio, make sure your 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.
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.

Setting	Description
Enable Keyboard Noise Reduction and Polycom NoiseBlock™	Specifies whether the system mutes audio from the RealPresence Group system microphones when keyboard tapping sounds or other extraneous noises are detected, but no one is talking. NoiseBlock unmutes the system when speech is detected, regardless of the existence of background noise. Note: Polycom MusicMode™ is disabled when this setting is enabled. If an external echo canceller is used, keyboard noise reduction is not available.
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 key 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.

Configure Audio Input Settings

You can configure audio input settings for your system type.

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.

To configure audio settings:

- 1 In the web interface, go to **Admin Settings > Audio/Video > Audio > Audio Input**.
- 2 Configure the Audio settings described in the following table.

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.

Setting	Description
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.
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.
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.
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.
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).

Setting	Description
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

Administrators can select how to enable 3.5mm audio input from the RealPresence Group system 3.5mm audio port in the system web interface. In 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 room 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 room system is in an active call, 3.5mm audio input is heard from the 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.

Configure Audio Output Settings

You can configure the audio output settings for your system.

To configure audio settings:

- 1 In the web interface, go to **Admin Settings > Audio/Video > Audio > Audio Output**.
- 2 Configure the Audio settings described in the following table.

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	Displays the current audio output type. This setting is read only.
Output Mode	Specifies whether volume for a device connected to the line out connectors is variable or fixed. <ul style="list-style-type: none"> • 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 Meters	Displays the output level meter for the left and right outputs. This setting is read only. Note: To disable HDMI output when using 3.5mm audio output, do the following. In the web interface, go to Admin Settings > Audio/Video > Monitors and set the Monitor 1 Enable setting to Manual . At Video Format , select DVI .

Stereo Settings

To send or receive stereo audio, make sure your room system equipment is set up as described in [Available Microphone Inputs by System](#) and [Audio Output](#). Then configure the room 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 can do so. The following Stereo Settings are available.

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.

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.
For details on correct placement, refer to [Polycom Microphone Placement to Send Stereo from Your Site](#).
- 2 In the web interface, go to **Admin Settings > Audio/Video > Audio > Audio Input**.
- 3 Gently blow on the left leg and right leg of each Polycom microphone while watching the bar meters to identify the left and right inputs.
- 4 Test the speakers to check volume and verify that audio cables are connected. If the system is in a call, the far site hears the tone.
Exchange the right and left speakers if they are reversed.
Adjust the volume control on your external audio amplifier so that the test tone sounds as loud as a person speaking in the room. If you use a Sound Pressure Level (SPL) meter, it should measure about 80-90 dBA in the middle of the room.
- 5 Repeat the steps above for **Admin Settings > Audio/Video > Audio > Audio Output**.

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**, if available.
 - b Adjust the **Audio Input Level** if necessary.
 - c 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 systems feature Polycom® Acoustic Fence 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: Acoustic Fence Technology is not supported on RealPresence Group 300 and 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 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: 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 microphone sensitivity and 10 is the maximum microphone sensitivity. Higher values increase the radius of the fence area around the primary microphone.

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

Content Sharing

To prepare for sharing content, see the following topics:

- [Sharing Content During Calls](#)
- [Configure Content Sharing](#)
- [Connect Computers to Polycom RealPresence Group Systems](#)
- [Configuring DVD Player Settings](#)
- [Multipoint Resolution and Frame Rates for People and Content](#)
- [Configure and Install a Polycom Content Display Application](#)
- [Configure Closed Captioning](#)

Sharing Content During Calls

You can present content during calls when you use sources such as the following:

- A DVD player connected directly to a video input on a room system
- People+Content IP installed on a computer, with any room system
- A computer connected directly to a RealPresence Group system or a Polycom touch device
- A USB drive connected to a Polycom touch device, such as the RealPresence Touch

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.

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

Configure Content Sharing

You can configure content sharing in the system web interface. 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*.

If 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, 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**.

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

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

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

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 [Configuring Video Input Settings](#). Refer to your system setup sheet for connection details.

Configuring DVD Player Settings

To play content from a DVD, do the following for your room system type:

- 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 supported.

Configure DVD Settings

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.

Multipoint Resolution and Frame Rates for People and Content

The following table shows the maximum multipoint resolution and frame rates for People and Content for each type of RealPresence Group system. For the RealPresence Group 310 and 500 systems, the maximum resolution and frame rates are dependent upon the quality preference settings that are configured on your system. For more information on the **Quality Preference** setting, refer to [Configure Network Quality Settings](#).

System Type	Maximum Resolution/ Frame Rate	People and Content
RealPresence Group 310	1080p/60fps	People or Content
RealPresence Group 500	1080p/60fps	People or Content
RealPresence Group 700	1080p/60fps	Both People and Content at the same time

Configure and Install a Polycom Content Display Application

The People+Content IP application enables a presenter to show content from a computer to other sites in a video conference using only an IP network connection. The presenter can show PowerPoint® slides, video clips, spreadsheets, or any other type of content from a computer. People+Content IP supports any computer desktop resolution with color set to 16-bit or higher.

If the room system is paired with a RealPresence Touch or a Polycom Touch Control, People+Content IP does not require installation. After you connect the PC to the USB connection on the device, a version of People+Content IP launches automatically.

Before a presenter can use a computer to show content with People+Content IP, do the following:

- Download the People+Content IP software application from the Polycom web site to the computer or computers that the presenter will use to show content.

You don't need to change the computer resolutions and you don't need special cables or hardware, but each computer must meet these requirements:

- Operating System: Windows 7 or 8

- Minimum computer: 500 MHz Pentium® III (or equivalent); 256 MB 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 [PPCIP download screen](#).
- 2 Download and install the People+Content IP software listed under **Resources**.

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.

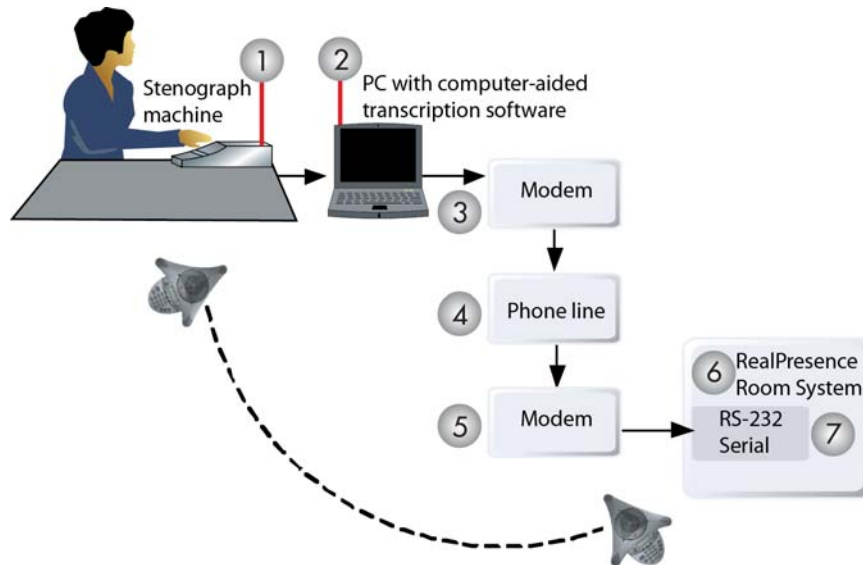
Captions may be provided in any language that uses the Latin alphabet.

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

Dial-Up Connection to the System's RS-232 Serial Port

Closed captioners can provide captions from inside the conference room, or from a remote location, via a dial-up connection to the serial port of the RealPresence Group system, as shown in the following diagram.



Ref. Number	Description
1	Stenograph machine
2	PC with computer-aided transcription software
3	Modem
4	Phone line
5	Modem
6	RealPresence Group system
7	RS-232 serial port

To supply closed captions through a dial-up connection:

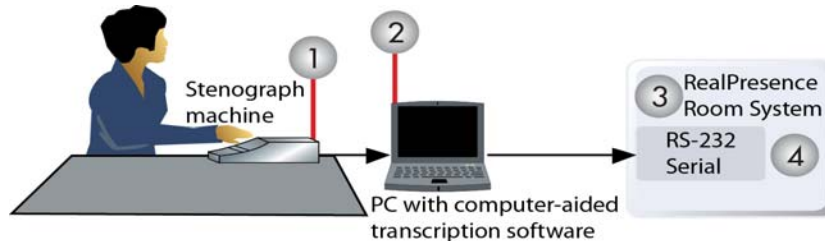
- 1 Ensure that the computer and the RealPresence Group system are configured to use the same baud rate and parity settings.
- 2 In the web interface, go to **Admin Settings > General Settings > Serial Ports**.
- 3 Set the RS-232 Mode to **Closed Caption**.
- 4 Establish a dial-up connection between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

Enter Closed Captions Using Equipment Connected to a Serial RS-232 Port

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



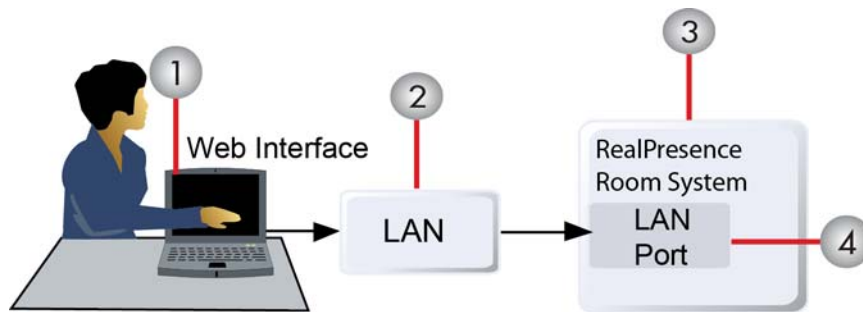
Ref. Number	Description
1	Stenographer machine
2	PC with computer-aided transcription software
3	RealPresence Group system
4	RS-232 serial port

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.

Enter Closed Captions on the Web Interface

Closed captioners can provide captions from inside the conference room, or from a remote location, by entering the captions directly into the RealPresence Group system web interface, as shown in the following diagram.



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

To supply closed captions for a conference:

- 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.

Placing and Answering Calls

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

To get started with calling, see these topics:

- [Configure Call Settings](#)
- [Multipoint Calling](#)
- [Configuring and Placing Audio-Only Calls](#)
- [Managing Directories in the Web Interface](#)
- [Manage Favorites Contacts and Groups](#)
- [Join Scheduled Meetings](#)
- [Using the Web Interface Place a Call Page](#)

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	<p>Enter the maximum number of hours allowed for call length.</p> <p>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.</p> <p>Selecting Off removes any limit.</p> <p>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.</p>
Auto Answer Point-to-Point Video	<p>Sets the answer mode for when the system is not in a call. This setting has three choices:</p> <p>Yes—Instructs the system to automatically answer the incoming point-to-point call.</p> <p>No—Instructs the system to force manual answering of the incoming call.</p> <p>Do Not Disturb—Instructs the system to reject the incoming call with no notification to the user.</p>
Auto Answer Multipoint Video	<p>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:</p> <p>Yes—Instructs the system to automatically answer the incoming multipoint call.</p> <p>No—Instructs the system to force manual answering of the incoming call.</p> <p>Do Not Disturb—Instructs the system to reject the incoming call with no notification to the user.</p>
Multipoint Mode	<p>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:</p> <p>Auto</p> <p>Full Screen</p> <p>Discussion</p> <p>Presentation</p> <p>For detailed information on these settings, refer to Select a Multipoint Viewing Mode.</p>
Display Icons in a Call	<p>Specifies whether to display all on-screen graphics, including icons and help text, during calls.</p>
Enable Flashing Incoming Call Notification	<p>Specifies whether the incoming call notification flashes.</p>

Setting	Description
Preferred 'Place a Call' Navigation	<p>Specifies the default icons that display on the local interface of the Place a Call screen. The available settings are as follows:</p> <p>Dial Pad—Displays a list of recently dialed numbers and a dial pad for entering a number to call.</p> <p>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.</p> <p>Recent Calls—Lists phone numbers, in chronological order, that have been dialed from the RealPresence Group system.</p>
Automatic Self View Control	<p>Specifies whether the Self View setting is visible in the local interface.</p> <ul style="list-style-type: none"> • If Automatic Self View Control is enabled, the Self View setting is not displayed in the local interface, and the system automatically chooses when to display the self view window. Whether the self view window is displayed is dependent on available display space, the display mode, and so on. • If Automatic Self View Control is not enabled, the user can turn Self View on and off from the local interface.

Configure Call Answering Mode

You can configure how your users answer calls when they use the local interface.

To configure 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 users to answer calls manually.
 - **Do Not Disturb**—Disables incoming calls from being processed and routed to the user.

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.

Turn On Flashing Alerts

You can turn on flashing alerts for hearing-impaired users to see when incoming calls are received by the system.

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.

Turn Off Flashing Alerts

You can turn off flashing alerts when the visual cue is not necessary.

To turn off flashing alerts:

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

Multipoint Calling

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



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

Enter a Multipoint Option Key

Depending on your 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. The multipoint option key cannot be used with RealPresence Group 300 and 310 systems, since these systems do not support multipoint calling.

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**.

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

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.

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

Multipoint Layout Panel Configurations for Each System Type

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.

Depending upon your RealPresence Group system, the number of participant panels can vary, as shown in the following table.

System Model	Number of Panels in the Layouts on the Internal MCU	Number of Panels in the Layouts on the Far-End Sites
RealPresence Group 700	8 (all participants are displayed)	8 (Up to 8 participants are displayed, regardless of the latest speakers)
RealPresence Group 500 RealPresence Group 310	6 (all participants are displayed)	4 (Up to 4 latest speakers)

Configuring and Placing Audio-Only Calls

You can now place SIP or H.323 audio-only calls on RealPresence Group systems through the web interface, the local interface, a RealPresence Touch device, API, or a Polycom® SoundStation® IP 7000 conference phone. Keep the following in mind when placing audio-only calls:

- You can place audio and video calls in any order at any time during a conference call.
- You cannot view video or share content as an audio-only participant during a conference call.
- Audio calls are supported when the **Enable Audio-only Calls** setting is enabled or when the system is paired to a Polycom SoundStation IP 7000.

For information on placing audio-only calls on the local interface, refer to the *Polycom RealPresence Group Series User Guide*.

Enable Audio-Only Calls

You can enable audio-only calls in the web interface.

To enable audio-only calls:

- » In the web interface, go to **Admin Settings > Network > Dialing Preference > Dialing Options >** and select **Enable Audio-Only Calls**. Click **Save**.

Disable Audio-Only Calls

You can disable audio-only calls in the web interface.

To disable audio-only calls:

- » In the web interface, go to **Admin Settings > Network > Dialing Preference > Dialing Options** and clear the **Enable Audio-Only Calls** checkbox. Click **Save**.

Select the Call Type Order for Audio-Only Calls

When Audio-Only Calls is enabled, you can choose the audio order and dialing preference.

To choose Audio Dialing Order:

- 1 In the web interface, go to **Admin Settings > Network > Dialing Preference > Dialing Options > Call Type Order**.
 - 2 Select **Phone then Video**.
 - 3 For the **Audio Dial Preference 1** and **Audio Dial Preference 2** settings, choose from the following call types:
 - IP H.323
 - SIP
 - Speakerphone (displays only when system is paired with SoundStation IP 7000 conference phone)
- If the **Enable Audio-Only Calls** checkbox is cleared, the **Audio Dial Preference 1** and **Audio Dial Preference 2** settings are not displayed.
- 4 Click **Save**.

Place an Audio-Only Call from the System Web Interface

You can place audio-only calls from the system web interface.

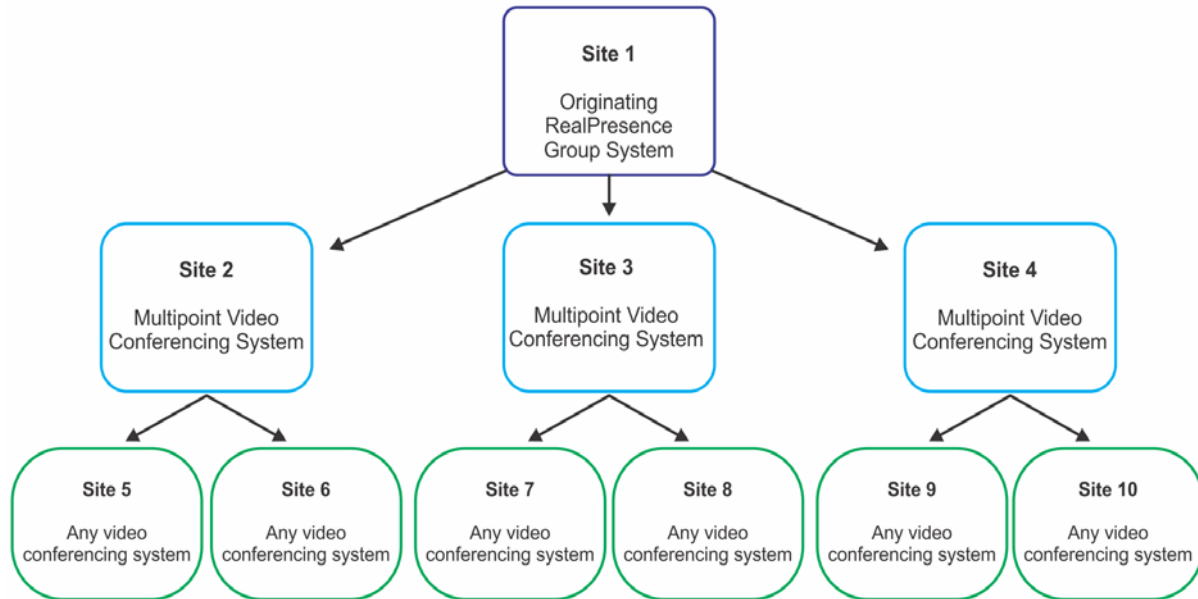
To place an audio-only call from the web interface:

- 1 In the web interface, go to **Place a Call > Manual Dial**.
- 2 Select **audio**.
- 3 To place the call, do one of the following:
 - » Enter the number and click **Call**.
 - » Under **Recent Calls**, click the desired audio call.

Including 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 a cascaded call with multiple sites.



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 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.
- You cannot place group calls on RealPresence Group 300 or 310 systems.

Place a Cascaded Call

You can place a cascaded call on the RealPresence Group system.

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.

Managing Directories in the Web Interface

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

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
- 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.

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, which appear in the Favorites group.



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

Searching Directory Contacts to Call

Directory contacts are called “global contact entries” in the system local interface. These global contact entries are assigned to a default global Favorites group named Global Entry. The global directory contains address book entries downloaded from an enabled global directory server.

You can search the global directory to return a list of all global directory entries that match your search criteria, then select contacts in the global directory to call. Up to 200 search results can be displayed at a time from a Polycom Global Directory Service (GDS) or Lightweight Directory Access Protocol (LDAP) global directory.

Prerequisite for Using the Global Directory Service (GDS)

To use GDS in your environment, you must have H.323 enabled and registered on your system. To enable H.323, go to the system web interface at **Admin Settings > Network > IP Network > H.323** and select the checkbox at **Enable IP H.323**. Enter the required registration information. For more information about registering H.323, refer to [Configure H.323 Settings](#).

GDS API Commands

To access options and settings for the Polycom Global Directory Service (GDS), you can use the following API commands:

- gdsdirectory
- gdspassword
- gdsserverip

For more information about these commands, refer to the *Polycom RealPresence Group Series Integrator Reference Manual*.

Search for Directory Contacts to Call

You can search for directory contacts to call in the web interface global directory.

To search the global directory using the web interface:

- 1 In the web interface, select **Place a Call > Contacts**.

- 2 At **Search**, enter a contact name and click **Search**.
- 3 Select **Call** to place a call or select an entry to view the contact's information.



Note: 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 Contacts and Groups

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 **Manage Favorites** screen.

Create a Favorites Contact

You can create a Favorites contact in the web interface.

To create a Favorites contact:

- 1 In the web interface, go to **Manage Favorites**.
- 2 Click **Create New Favorite**.
- 3 Enter the contact call information and click **Save**.

Create a Favorites Group

You can create a Favorites group in the web interface.

To create a Favorites group:

- 1 In the web interface, go to **Manage Favorites**.
- 2 Click **Create New Group**.
- 3 Enter a **Name** for the group and click **Save**.
A success message is displayed.
- 4 To add contacts to the group, click **Add Contacts** on the success message.
- 5 Enter a contact name in the search box and click **Search**.
- 6 In the entry you want to add to the group, click **Add**.
- 7 Repeat the above steps to add more contacts to the group.
- 8 Click **Done**.

Edit a Favorites Group

You can edit a Favorites group in the web interface.

To edit a Favorites group:

- 1 In the web interface, go to **Manage Favorites**.
- 2 Find the group name in the list of contacts.
- 3 Next to the group contact name, click **Edit Group**.
Do one of the following:
 - To add contacts to the group, click **Search to add contacts to this group**, enter a contact name, click **Search**, and then **Add** to add a contact.
 - To remove contacts from a group, next to a contact name, click **Remove**.
- 4 Repeat the above steps to continue adding or removing contacts.
- 5 Click **Done**.

Delete a Favorites Group

You can delete a Favorites group in the web interface.

To delete a Favorites contact or group:

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

Importing and Exporting Favorites

The Import/Export Directory feature enables you to download Favorites from a RealPresence 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 room 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

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

Keep the following points in mind when performing these tasks:

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

Export Favorites Groups and Contacts

You can export Favorites groups and contacts to your local device.

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.

Import Favorites Groups and Contacts

You can import Favorites groups and contacts and upload the directory file to your 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	<ul style="list-style-type: none"> • Directory entries created locally by the user. 	Unknown
	<ul style="list-style-type: none"> • References to Polycom GDS entries added to Favorites by the user. These entries are available only if the system is successfully registered with Polycom GDS. Users can delete these entries from Favorites. Users can copy these entries to other Favorites and remove them from those groups. Users cannot edit these entries. 	Online/Offline
LDAP with H.350 or Active Directory	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Skype for Business Server 2015 directory entries are saved as Contacts by the user and stored on the Skype 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 RealPresence Group system. Users can copy these entries to other Favorites and remove them from those groups. 	Real-time presence

Join Scheduled Meetings

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

To join a scheduled meeting from the Home screen:

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

For information about displaying the Calendar button on the Home screen, refer to [Customize What Users See on the System Home Screen](#). For more information about joining scheduled meetings, refer to the *Polycom RealPresence Group Series User Guide*. For more information about setting up Microsoft Exchange Server 2013 accounts to use the calendaring service, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.

Using 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

For information on configuring Home screen settings for the local interface, refer to [Customize What Users See on the System Home Screen](#).

Perform a Search for Web Interface Screens

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

To search for a text string:

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

Place a Call to Favorite Contacts

In the **Place a Call** area, you can place a call manually, or search your contacts.

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 Contacts and Groups](#).

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.

Place a Call to Speed Dial Contacts

On the web interface **Place a Call** screen, you can call Speed Dial contacts and can edit the **Speed Dial** contact list. After you have enabled **Speed Dial**, users can use it as a shortcut for calling a contact.

To call speed dial contacts:

- » In the **Speed Dial** section, select a contact from the list and click **Call**.
To place a call within your company's telephone system, enter the internal extension instead of the full number.

Place a Call to Recent Call Contacts

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

To dial a recent call from the web interface:

- » In the web interface **Place a Call** screen's **Recent Calls** section, do one of the following:
 - Find an entry and click the **Call** link next to the entry.
 - Click **More** to view a list of calls with more details, then select an entry and click **Call**.

Configure the Recent Calls List

You can 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 configure Recent Calls:

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

Setting	Description
Call Detail Report	Specifies whether to collect call data for the Call Detail Report. When selected, information about calls can be viewed through the 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 \(CDR\)](#).

Security

For detailed security information, see the following topics:

- [Security Settings in the Web Interface](#)
- [Configure Security Profiles](#)
- [Managing System Access and External Authentication](#)
- [Enabling a Whitelist for IPv4 and IPv6 Addresses](#)
- [Port Lockout](#)
- [Encryption](#)
- [Visual Security Classification](#)
- [Managing Certificates and Revocation](#)
- [Configure a Security Banner](#)
- [Configure a Meeting Password](#)

Security Settings in the Web Interface

To configure your RealPresence Group system security settings using the system web interface, use a supported browser with cookies enabled. For a list of supported browsers and version numbers, refer to the release notes for your system.


To access the web interface, open a web browser and enter the IP address of the system using the `https://IPaddress` (for example, `https://10.11.12.13`).

For more information about using the web interface, refer to [System Web Interface](#).



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

You can find security settings and passwords in the following locations:

- 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 selections, and many settings in the web interface are unavailable in the local interface.



Note: In accordance with local laws and regulations not all security settings are available in all countries.

Configure Security Profiles

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

The security profile is selected during system setup with the setup wizard, but this setting is configurable through 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.

Managing System Access and External Authentication

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

- [Enable External Authentication](#)
- [Login and Credentials](#)
- [Secure API Access](#)
- [Local Accounts](#)
- [Enable Access to User Settings](#)

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.

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

The room system administrator configures the external authentication settings on the 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 room system. The system can map only one Active Directory group to a given role.

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

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



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

Enable External Authentication

You can enable external authentication for your system.

To enable external authentication:

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

Setting	Description
Enable Active Directory External Authentication	Specifies whether to authenticate users through the Active Directory server. When Active Directory authentication is enabled, users are allowed to log in with their network account credentials, using this format: domain\user With this format, users can have accounts on multiple domains.
Active Directory Server Address	Specifies the DNS fully qualified domain name (FQDN) or IP address of the Active Directory server (ADS). If you are using subdomains, append port number 3268 as follows: ad.domain.com:3268 Note: 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 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 the local room system admin credentials to pair the system with a touch device, such as the RealPresence Touch.


Login and Credentials

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

Configure Local Access

You can configure local access so that users can reach 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 <code>admin</code> . 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. 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 <code>user</code> . 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: 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

Configure Remote Access Settings

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 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 Managing 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 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 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 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 Enabling a Whitelist for IPv4 and IPv6 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.

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

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

Detecting Intrusions

The 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 RealPresence Group system using the Secure Shell (SSH) protocol. Secure API access is authenticated for local and Active Directory (AD) accounts.



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

Secure API access using SSH is enabled by default. The `sshenable` API command and **Enable SSH Access** web interface setting 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 system, go to Admin Settings > Security > Global Security > Access and enable the Enable SSH Access setting.
- In a RealPresence Group system API session, enter `sshenable true`.

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

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

Local Accounts

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

Configure Password Policies Settings

You can configure password policies for Admin, User, Meeting, Remote Access, and SNMP passwords. These password settings can ensure that strong passwords are used. Polycom strongly recommends that you create an Admin password for your 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.
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 <code>admin</code> , passwords <code>admin</code> and <code>nimda</code> 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 to Prevent Unauthorized System Access

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

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.

Configure Account Lockout

You can configure account lockout to prevent unauthorized system access.

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 screen, then click **Save**. You can configure account lock for the admin account, user account, or both accounts.

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

View Connections to Your System in a Sessions List

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

- Type of connection, for example, Web
- ID associated with the session, typically Admin or User
- Remote IP address (addresses of people logged in to the 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**.

Enabling a Whitelist for IPv4 and IPv6 Addresses

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

Enable a Whitelist

You can enable a whitelist so that you can add specific IPv4 and IPv6 addresses to the approved list.

To enable a whitelist:

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

Add IP Addresses to a Whitelist

You can add specific IP addresses to a whitelist.

To add addresses to a 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: 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. 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.

Configure the Port Lockout Setting to Lock the Login Port

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

To configure port lockout:

- 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.

Encryption

AES encryption is a standard feature on all 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 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>.

Configure Encryption

You can configure encryption settings on your system.

To configure encryption 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 > Encryption**.
- 2 Configure these settings.

Setting	Description
Require AES Encryption for Calls	<p>Specifies how to encrypt calls with other sites that support AES encryption.</p> <ul style="list-style-type: none"> • 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)	<p>Enables the exclusive use of the FIPS 140-2-validated software cryptography module for cryptographic functions. Also disables all "weak" protocols and ciphers, including:</p> <ul style="list-style-type: none"> • SSLv2 • SSLv3 • Non-FIPS 140-2 approved TLS cipher suites

Configure Encryption Settings for SVC Calls

You must complete two 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**.

Set AES Encryption for SVC Calls

You can set AES encryption for SVC calls.

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 [Setting Call Preferences for SVC](#).

Configure Encryption Settings for Skype for Business 2015

RealPresence Group systems support media encryption in calls with Skype for Business 2015, and the system must be configured to support encryption so that calls can connect with encryption. For more information about encryption configuration in a Skype for Business 2015 environment, refer to the *Polycom Unified Communications for Microsoft Environments Solution Deployment Guide* at support.polycom.com.

Verify 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 encryption 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.

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 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.

Enable Visual Security Classification

You can enable Visual Security Classification on your system.

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**.

Managing 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 systems before you integrate these products with the PKI.

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

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.

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

- 1 A Server certificate—the system’s web server presents this certificate after receiving connection requests from browsers attempting to connect to the system web interface.

- 2 A Client certificate—the system presents this certificate to a remote server when challenged to provide a certificate as part of authenticating the identity of the system before allowing it to connect to the remote server. Examples of remote servers include the RealPresence® Resource Manager system, a SIP proxy/registrar server, or an LDAP directory server.

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

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

To configure certificate validation settings:

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

Setting	Description
Maximum Peer Certificate Chain Depth	Specifies how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host to the RealPresence Group system when a network connection is being established between the two systems.
Always Validate Peer Certificates from Browser	Controls whether the system requires a browser to present a valid certificate when it tries to connect to the 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 to install the client certificate, server certificate, and any required CA-type certificates.

To add a signed certificate on the Certificates screen:

- 1 To open the certificate section, at **Installed Certificates**, click **View and Add**.
- 2 Next to **Add Certificate**, click **Browse** to search for and select a certificate. You might be installing a client or server certificate that has been signed by a CA after having been previously generated as a CSR, or installing a CA certificate needed by the system to validate a certificate it receives from another system.
- 3 Click **Open**.
The system checks the certificate data and adds it to the list. If you don't see the certificate in the list, the system was unable to recognize the certificate. This process is sometimes referred to as *installing* a certificate.
You can select a certificate in the list to view its contents. You can also remove a certificate from the list by clicking **Remove**.
- 4 If needed, click **Close** to close the certificate section of the screen.
- 5 Click **Save**.
When you add a CA certificate to the system, the certificate becomes trusted for the purpose of validating peer certificates.



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

Certificate Signing Requests (CSRs)

The RealPresence Group system allows you to install one client and one server certificate for identification of the system to network peers. In order to obtain these certificates you must first create a Certificate Signing Request (CSR) for each certificate. This request, also known as an unsigned certificate, must be submitted to a CA so that it can be signed, after which the certificate can be installed on the system. 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 system is configured to use any of the following features, and the servers providing those services perform certificate-based authentication before allowing access to them, you must create a client-type CSR and add the resulting certificate signed by the CA:

- RealPresence Resource Manager system Provisioning
- RealPresence Resource Manager system Monitoring
- RealPresence Resource Manager system LDAP Directory
- RealPresence Resource Manager system Presence
- Calendaring

- SIP
- 802.1X

The system web server uses the server-type CSR and resulting certificate whenever a user attempts to connect to the 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 system he or she is connecting to. Settings in the web browser typically control the validation of the server certificate, but you can also validate the certificate manually.

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

Create Certificate Signing Requests (CSRs)

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

To create a CSR:

- 1 In the web interface, go to **Admin Settings > Security > Certificates > Certificate Options**.
- 2 Click **Create** for the type of CSR you want to create, **Signing Request Server** or **Signing Request Client**. The procedure is the same for server and client CSRs.
- 3 Configure these settings on the Create Signing Request screen and click **Create**.

Setting	Description
Hash Algorithm	Specifies the hash algorithm for the CSR. You may select SHA-256 or keep the default SHA-1.
Common Name (CN)	Specifies the name that the system assigns to the CSR. Polycom recommends the following guidelines for configuring the Common Name: <ul style="list-style-type: none"> • 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
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.

Setting	Description
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: 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: 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.

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 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 system to contact an OCSP responder, a network server that provides real-time certificate status through a query/response message exchange.



Note: 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.

Configure the Certificate Revocation List (CRL) Method

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

To configure the CRL revocation method:

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

Setting	Description
Revocation Method	To enable the CRL revocation method, select CRL .
Allow Incomplete Revocation Checks	When this field is enabled, a certificate in the chain is verified without a revocation status check if no corresponding CRL for the issuing CA is installed. 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	<ul style="list-style-type: none"> • Click Browse to search for and select a CRL. • Click Open to add the CRL to the list.

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



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

Configure the OCSP Revocation Method

You can configure the OCSP revocation method settings in the system web interface.

To configure the OSCP revocation method:

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

Setting	Description
Revocation Method	To enable the OSCP revocation method, select OSCP .
Allow Incomplete Revocation Checks	<p>When this field is enabled, the RealPresence Group system treats the following response from the OSCP responder as a successful revocation checks that would otherwise be considered a failed check:</p> <ul style="list-style-type: none"> • If the OSCP responder responds that the status is unknown or if no response is received, the system treats this as a successful revocation check. <p>Regardless of the state of this setting, the following statements apply:</p> <ul style="list-style-type: none"> • If the OSCP responder indicates a known revoked status, the room system treats this as a revocation check failure and does not allow the connection. • If the OSCP responder indicates a known good status, the room system treats this as a successful revocation check and allows the connection.
Global Responder Address	<p>Specifies the URI of the responder that services OSCP requests (for example, <code>http://responder.example.com/ocsp</code>). This responder is used for all OSCP 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.</p>
Use Responder Specified in Certificate	<p>In some cases, the certificate itself includes the responder address. When this field is enabled, the system attempts to use the address in the certificate (when present) instead of the Global Responder Address specified in the previous field.</p> <p>Note: The 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.</p>



Note: For validation of the OSCP response message, if you use OSCP, 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 system 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 system:

- 1 You must install a signed client certificate on the system to enable the provisioning connection to be authenticated by the RealPresence Resource Manager system.
- 2 Decide whether to automatically validate web clients by enabling the **Always Validate Peer Certificates from Browsers** setting. If you do enable the setting, you'll need to install a signed server certificate and all of the CA certificates needed to validate browser certificates for all web clients. Then configure the certificate revocation method.
- 3 Decide whether to validate servers by enabling the **Always Validate Peer Certificates from Servers** setting. If you do enable the setting, you must install all 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 system 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 **Settings > System Information > Diagnostics > Reset System**.
- 2 If needed, enter the **Admin ID** and **Password**.
- 3 Enable the **Delete Certificates** field.
- 4 Select **Reset System**.

The system restarts after deleting all installed certificates and CRLs.

RealPresence Server Address Configuration in PKI-enabled Environments

When configuring the server addresses for the services listed in [Configure Certificate Validation Settings](#) 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.

Configure a Security Banner

Security banners consist of text that displays on the Login screen and in a window when you log in remotely. The security banner is not supported on the Polycom Touch Control.

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.
```

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 instead of a bridge.

Remember the following points about meeting passwords:

- Do not set a meeting password if multipoint calls include audio-only endpoints. Audio-only endpoints are unable to participate in password-protected calls.
- Microsoft Office Communicator clients are unable to join password-protected multipoint calls.
- SIP endpoints are unable to connect to password-protected multipoint calls.
- If a meeting password is set for a call, People+Content™ IP clients must enter the password before joining the meeting.
- Meeting passwords cannot contain spaces or be more than 32 characters.

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.

Control and Navigation

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

- [Remote Control](#)
- [Connecting Control and Accessibility Equipment](#)
- [Polycom® RealPresence® Medialign™ Solution](#)
- [Polycom® Concierge Solution](#)
- [SmartPairing](#)
- [Configure Contact Information](#)
- [Configure System Location Settings](#)
- [Configure Room System Language Settings](#)
- [Configure System Date and Time Settings](#)
- [Configure Sleep Settings](#)

Remote Control

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

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

Configure Remote Control Behavior

You can customize the remote control behavior by configuring settings in the system web interface.

To configure remote control behavior:

- 1 In the system web interface, go to **Admin Settings > General Settings > System Settings > Remote Control, Keypad, and Power**.
- 2 Configure these settings.

Setting	Description
Keypad Audio Confirmation	Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad.
Numeric Keypad Function	Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones). If this is set to Presets , users can generate DTMF tones by pressing the # key on the remote while on a video screen.
Use Non-Polycom Remote	Configures the system to accept input from a programmable, non-Polycom remote control. In most cases the Polycom remote works as designed, even when this feature is enabled. However, try disabling this feature if you experience difficulty with the Polycom remote. For more information about system IR codes, refer to the <i>Polycom RealPresence Group Series Integrator Reference Guide</i> .
Channel ID	Specifies the IR identification channel to which the room system responds. Set the Channel ID to the same channel as the remote control. The default setting is 3. If the remote control is set to channel 3, it can control a room system set to any Channel ID. For more information about changing this setting, refer to Configuring the Remote Control Channel ID for a Specific System .
Hang-up Button Long Press	Specifies the behavior of the remote control Hang-up button when you press it for a long time: <ul style="list-style-type: none"> • Hang-up / Power Off—Holding down the Hang-up button powers off the room system. • Hang-up / Sleep—Holding down the Hang-up button puts the system to sleep. • Hang-up Only—Holding down the Hang-up button has no function other than hanging up the call.
# Button Function	Specifies the behavior of the # button on the remote control: <ul style="list-style-type: none"> • #, 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.

Configuring the Remote Control Channel ID for a Specific System

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



Note: 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 room system set to any Channel ID. If the system does not respond to the remote control, set the remote control channel ID to 3 starting with step 3 in the following procedure. Then follow the entire procedure to configure the system and remote control channel ID settings.

While performing the following procedures, blocking the IR signal from the remote control can prevent the signal from being received by the system, causing the system to take an action that corresponds to any of the remote control button presses.

Confirm a Channel ID

You can confirm the correct channel ID to control your system.



To confirm a channel ID:

- 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.

Save a Channel ID for a Specific System

You can save the channel ID for a system so that it can be configured for your remote control.

To save a channel ID for a specific system:

- 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.

Configure a Channel ID for the Remote Control

You can configure a channel ID to control a specific system in a room with more than one system.

To configure the channel ID:

- 1 In the web interface, go to **Admin Settings > General Settings > System Settings > Remote Control, Keypad, and Power**.
- 2 Select the **Channel ID**.
- 3 Click **Save**.

To find the Channel ID for your monitor, check the connection label on the monitor, or refer to the monitor's manufacturer documentation.

Connecting Control and Accessibility Equipment

The RealPresence Group 300, RealPresence Group 310, and 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.

Ensure that the room system is powered off before you connect devices to it.

Third-Party Touch Panel Controls

As part of a custom room installation, you can connect an AMX or Crestron control panel to a 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

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

To configure RS-232 serial port settings:

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

Setting	Description
RS-232 Mode	<p>Specifies the mode used for the serial port. Available settings depend on the RealPresence Group system model.</p> <ul style="list-style-type: none"> • 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. <p>Note: If you have a RealPresence Group 300, 310, or 500 system, use only the Polycom serial cable with part number 2457-63542-001 to connect devices to the RS-232 serial port.</p>
Baud Rate, Parity, Data Bits, Stop Bits	Set these to the same values that they are set to on the serial device.

Setting	Description
RS-232 Flow Control	This setting works with RS-232 modes that are not currently available. The setting is not currently configurable.
Login Mode	<p>Specifies the credentials necessary for a control system to connect to the RS-232 port.</p> <ul style="list-style-type: none"> • Admin password only—Requires the admin password, if one has been set, when the control system connects. (default) • Username/Password—Requires the user name and the admin password, if one has been set, when the control system connects. • None—No user name or password is required when the control system connects. <p>Note: This setting only displays when RS-232 Mode is set to Control.</p>

Polycom® RealPresence® Medialign™ Solution

The Polycom® RealPresence® Medialign™ solution includes several integrated Polycom components, including a RealPresence Group 500 system codec. Some configuration steps are required in the system's web interface, including single or dual monitor and RS-232 serial port settings. For setup and configuration information, refer to the *Polycom RealPresence Medialign Administrator Guide* at support.polycom.com.

Polycom® Concierge Solution

RealPresence Group systems now support the Polycom® Concierge solution. This enterprise solution is an integrated system of Polycom products that enhance the meeting experience by allowing end users to extend and control their collaboration experience using personal computing devices such as smartphones, laptops, and desktop systems.

When a RealPresence Group system is provisioned as part of a Polycom Concierge deployment, users with supported and provisioned devices can wirelessly connect to the system. The devices must be running Polycom® RealPresence® Mobile or Polycom® RealPresence® Desktop.

Examples of collaboration and control functions that users might perform include the following:

- Join a meeting in progress upon entering the meeting room
- Present content
- Add participants, hang up the call, change the volume, and mute the call
- View and annotate shared content
- Record the call

To access the collaboration and control functions, users must first pair their personal device with a room system. Administrators have three options for providing this information:

- Configure a beacon to broadcast the location details for the room system. For more information, refer to the *Polycom Concierge Solution Deployment Guide* at support.polycom.com.
- Generate a pairing information printout from RealPresence Resource Manager for users to obtain the pairing information. For more information, refer to the *Polycom RealPresence Resource Manager System Operations Guide* and the *Polycom Concierge Solution Deployment Guide* at support.polycom.com.
- Add the pairing code to the RealPresence Group Series system local user interface.

Add the System Pairing Code to the System Home Screen

To display a pairing code on the RealPresence Group system local interface home screen, you must enable a setting in the system web interface.

To add the system pairing code to the system's home screen:

- 1 In the RealPresence Group system web interface, navigate to **Admin Settings > General Settings > Home Screen Settings**.
- 2 Click **Address Bar**.
- 3 Select **Pairing Code** for either the left or right Address Bar element and click **Save**.

The pairing code for the RealPresence Group system displays on the bottom of the system's home screen in the meeting room.

If users encounter problems pairing with the system or you receive a registration error, confirm that the Polycom Concierge service is active.

Check the Polycom Concierge Service Status

You can view the Polycom Concierge service status to determine if it is active.

To check the status of the Polycom Concierge service:

- 1 In the RealPresence Group system web interface, go to **Diagnostics > System > System Status**.
- 2 Confirm that the Polycom Concierge service is active (the status LED is green).

For additional details about the solution, see the *Polycom Concierge Solution Deployment Guide* at support.polycom.com. For product interoperability information, refer to the *Polycom Concierge Solution Release Notes* at support.polycom.com.

SmartPairing

Polycom SmartPairing™ allows you to detect and pair a room system from the RealPresence Mobile application on an Android or Apple iPad tablet. After you pair the application and the room system, you can use the RealPresence Mobile application to perform two basic functions:

- Use the application as a remote control for the room system.
- Swipe to transfer a call from the RealPresence Mobile application to the room system.

SmartPairing Prerequisites

Telnet must be enabled before you can use SmartPairing. 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: <ol style="list-style-type: none"> 1 Enable telnet. In the system web interface, go to Admin Settings > Security > Global Security > Access and at Enable Telnet Access, select the checkbox. 2 Send an API command or use the web interface.

Configure SmartPairing

You can configure SmartPairing so that users can pair mobile devices to the room system.

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 room system, if SmartPairing is enabled: <ul style="list-style-type: none"> • Disabled • Automatic • Manual
Signal Volume	Specifies the relative signal strength of the ultrasonic signal within the loudspeaker audio output signal. The selections are Auto, and levels are 1 to10.

View Remote Sessions on the System

You can view a list of remote sessions that are connected to the system.

To view remote sessions:

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

Configure Contact Information

You can configure contact information for your room system so that users know whom 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 the following settings.

Setting	Description
Contact Person	Specifies the name of the system administrator.
Contact Number	Specifies the phone number for the system administrator.
Contact Email	Specifies the email address for the system administrator.
Contact Fax	Specifies the fax number for the system administrator.
Tech Support	Specifies the name of the person who provides technical support.
City	Specifies the city where the system administrator is located.
State/Province	Specifies the state or province where the system administrator is located.
Country	Specifies the country where the system administrator is located.

Configure System Location Settings

On the web interface, you can configure settings to specify the country and the country code where the system is located.

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 Room System Language Settings

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

To configure the room 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 System Date and Time Settings

On either the local or web interface, you can configure the system date and time settings.

To configure the 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.
Time Server	Specifies whether the connection to a time server is automatic or manual for system time settings. You can also select Off to enter the date and time yourself.
Primary Time Server Address	Specifies the address of the primary time server to use when Time Server is set to Manual .
Secondary Time Server Address	Specifies the address of the time server to use when the Primary Time Server Address does not respond. This is an elective field.
Current Date and Current Time	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Sleep Settings

You can configure when you want a system to go to sleep after a period of inactivity.

To configure when the system goes to sleep:

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

Diagnostics, Status, and Utilities

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](#)
- [System Log Files](#)
- [Retrieving 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 [SNMP Condition Reports](#).
- 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.

Access Diagnostic Screens in the Local Interface

Most diagnostic information is available in both the web and the local interface, but some 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 screens include the following diagnostic information for your system.

Information

Diagnostic Screen	Description
System Detail	Displays the following system information: <ul style="list-style-type: none"> • System Name • Model • Hardware Version • System Software • Serial Number • MAC Address • IP Address
Network	Displays the following network information: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> 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 room 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 room system lists the hops between the system and the IP address you entered.
Color Bars	Tests the color settings of your monitor for optimum picture quality. If the color bars generated during the test are not clear, or the colors do not look correct, the monitor needs to be adjusted.

Diagnostic Screen	Description
Speaker Test	<p>Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct.</p> <p>If you run the test from the system during a call, the far site will also hear the tone.</p> <p>If you run the test from the room system web interface during a call, the people at the site you are testing will hear the tone, but you will not.</p>
Audio Meters	<p>Measures the strength of audio signals from the microphone or microphones, far-site audio, and any device connected to the audio line in.</p> <p>Meters function only when the associated input is enabled.</p> <p>Note: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system.</p> <p>For details on configuring this setting, refer to Audio Meters.</p>
Camera Tracking	<p>Provides diagnostics specific to the EagleEye Director.</p> <p>Audio</p> <p>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.</p> <p>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.</p> <p>After you verify microphone functionality, calibrate the camera again.</p> <p>Video</p> <ul style="list-style-type: none"> • Left Camera shows video from the left camera. • Right Camera shows video from the right camera. • Color Bars displays the color bar test screen. <p>Note: If the EagleEye Director is connected but is not selected as the current camera source, this choice is not visible on the screen.</p>
Sessions	<p>Displays the following information about each session connected to the system:</p> <ul style="list-style-type: none"> • Type • User ID • Remote Address
Reset System	<p>Returns the room system to its default settings. When you select this setting using the remote control, you can do the following:</p> <ul style="list-style-type: none"> • 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). <p>You might want to download the CDR and CDR archive before you reset the system. Refer to Call Detail Report (CDR).</p> <p>Note: If a room password is configured for the admin account, you must enter it to reset the system.</p>

Access Diagnostics Screens in the Web Interface

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: 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 in a system web interface:

- 1 In the web interface, click **Diagnostics**.
- 2 Configure the following settings. Note that some settings are read only and cannot be configured.

System Diagnostics

Diagnostic Screen	Description
Call Statistics	<p>Displays information about the call in progress. What you see depends on whether you are in a point-to-point or multipoint call.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▲ 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 setting is available in SVC calls only). Select the desired stream, and select More Info. <p>If the system is not in a call, the screen displays The System is not currently in a call.</p>
System Status	<p>Displays the following system status information:</p> <ul style="list-style-type: none"> • Auto-Answer Point-to-Point Video, Remote Control, and Meeting Password • Microphones, SoundStation IP, SoundStructure • IP Network • Servers: <ul style="list-style-type: none"> ▲ 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 <p>If the room system detects an EagleEye Director, a status line for the device is displayed.</p>
Download Logs	Enables you to save system log information.

Diagnostic Screen	Description
System Log Settings	<ul style="list-style-type: none"> 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 room system.

The following table describes the information you see when you click **More Info** on the Call Statistics screen.

Call Statistics “More Info”
<p>Participant information</p> <ul style="list-style-type: none"> System name System number System information Call speed (send and receive) Call type Encryption <p>Participant streams</p> <ul style="list-style-type: none"> 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)

Audio and Video Tests

You can perform the following audio and video diagnostic tests.

Diagnostic Screen	Description
Speaker Test	<p>Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct.</p> <p>If you run the test from the system during a call, the far site will also hear the tone.</p> <p>If you run the test from the room system web interface during a call, the people at the site you are testing will hear the tone, but you will not.</p>
Audio Meters	<p>Measures the strength of audio signals from microphones, far-site audio, and any device connected to the audio line in.</p> <p>Meters function only when the associated input is enabled.</p> <p>Note: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system.</p> <p>For details on configuring this setting, refer to Audio Meters.</p>
Camera Tracking	<p>Provides diagnostics specific to the EagleEye Director.</p> <p>Audio</p> <p>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.</p> <p>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.</p> <p>After you verify microphone functionality, calibrate the camera again.</p> <p>Video</p> <ul style="list-style-type: none"> • Left Camera shows video from the left camera. • Right Camera shows video from the right camera. • Color Bars displays the color bar test screen. <p>Note: If the EagleEye Director is connected but is not selected as the current camera source, this choice is not visible on the screen.</p>

System Log Files

System log files are essential when troubleshooting system issues. System log files contain information about system activities and the system configuration profile.

To set up system logging, you need to perform 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 [Retrieving 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: 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 storage 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: <ul style="list-style-type: none"> • 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 <code>marketing_MMddyyymmssSSS</code>. • Timestamp—Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example <code>yyyymmddhhmmssSSS</code>. • Custom—Elective 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: <p>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.</p> <p>Auto at Threshold—The transfer starts automatically when the Percent Filled Threshold is reached.</p>

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 room system's flash memory. <code>DEBUG</code> logs all messages, and <code>WARNING</code> logs the fewest number of messages. Polycom recommends leaving this setting at the default value of <code>DEBUG</code> . When Enable Remote Logging is on, the log level is the same for both remote and local logging.
Enable Remote Logging	Specifies whether remote logging is enabled. Enabling this setting causes the room system to send each log message to the specified server in addition to logging it locally. The system immediately begins forwarding its log messages after you click Save . Remote logging encryption is supported when TLS transport is the transport protocol. If you are using UDP or TCP transport, Polycom recommends remote logging only on secure, local networks.
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: <ul style="list-style-type: none"> • UDP: 514 • TCP: 601 • TLS: 6514 The address and port can be specified in the following formats: <ul style="list-style-type: none"> • IPv4 Address (Example: 10.11.12.13:<port>, where <port> is the elective destination port number in the range 1.65535) • IPv6 Address (Example: [2001::abcd:1234]:<port>, where <port> is the elective destination port number in the range 1.65535) • FQDN (Example: logserverhost.company.com:<port>, where <port> is the elective destination port number in the range 1.65535)
Remote Log Server Transport Protocol	Specifies the type of transport protocol: <ul style="list-style-type: none"> • UDP • TCP • TLS (secure connection)
Enable H.323 Trace	Logs additional H.323 connectivity information.
Enable SIP Trace	Logs additional SIP connectivity information.
Send Diagnostics and Usage Data to Polycom	Sends crash log server information to Polycom to help us analyze and improve the product. Click the Polycom Improvement Program button to view information about how your data is used.

Retrieving Log Files

You might find log files useful when troubleshooting. You can generate log files for the RealPresence Group system, RealPresence Touch, Polycom Touch Control, and EagleEye Director. These sections explain how to retrieve those log files:

- [Download System Log Files](#)
- [Transfer System Log Files](#)
- [Transfer EagleEye Director Logs](#)

Download System Log Files

You can use the RealPresence Group system web interface to get system logs.



Note: The date and time of system log entries for RealPresence Group systems are shown in GMT.


To download a system log in the web interface:

- 1 Go to **Diagnostics > System > Download Logs**.
- 2 Click **Download system log** and then specify a location on your computer to save the file.
In the dialog boxes that appear, designate where you want the file to be saved.

Transfer System Log Files

You can transfer a RealPresence Group system log in the local interface.

To transfer a system log in the local interface:

- 1 Go to  > **Settings > Administration > Security > Log Management**.
- 2 Click **Transfer System Log to USB Device**.
- 3 The system saves a file in the USB storage device named according to the settings in the web interface.
- 4 Wait until the system displays a message that the log transfer has completed successfully before you remove the storage device.

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 RealPresence Group system web interface, the Call Detail Report (CDR) provides the room system's call history. Within 5 minutes after ending a call, the CDR is written to memory and then you can download the data in CSV format for sorting and formatting.

Every call is added to the CDR, whether it is made or received. If a call does not connect, the report shows the reason. In multipoint calls, each far site is shown as a separate call, but all have the same conference number.

The size of a CDR can become unmanageable if you don't download the record periodically. If you consider that 150 calls result in a CDR of approximately 50 KB, you can set up a schedule to download and save the CDR after about every 120 calls just to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads.



Note: The CDR database is limited to the 150 most recent entries. If you are concerned about tracking all CDR records, ensure that you download the records at regular intervals so that the limit is not exceeded and records are not lost.

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.

Data	Description
Transport Type	The type of call — Either H.323 (IP) or SIP.
Call Rate	The bandwidth negotiated with the far site.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.
Call Direction	In—For calls received. Out—For calls placed from the system.
Conference ID	A number given to each conference. A conference can include more than one far site, so there might be more than one row with the same conference ID.
Call ID	Identifies individual calls within the same conference.
Total H.320 Channels Used	Number of narrow-band channels used in the call.
Endpoint Alias	The alias of the far site.
Reserved	Polycom use only.
View Name	Names the web or local interface used in the call.
User ID	Lists the ID of the user who made the call.
Endpoint Transport Address	The actual address of the far site (not necessarily the address dialed).
Audio Protocol (Tx)	The audio protocol transmitted to the far site, such as G.728 or G.722.1.
Audio Protocol (Rx)	The audio protocol received from the far site, such as G.728 or G.722.
Video Protocol (Tx)	The video protocol transmitted to the far site, such as H.263 or H.264.
Video Protocol (Rx)	The video protocol received from the far site, such as H.261 or H.263.
Video Format (Tx)	The video format transmitted to the far site, such as CIF or SIF.
Video Format (Rx)	The video format received from the far site, such as CIF or SIF.
Disconnect Local ID and Disconnect Reason	The identity of the user who initiated the call and the reason the call was disconnected.
Q.850 Cause Code	The Q.850 cause code showing how the call ended.
Total H.320 Errors	The number of H.320 errors experienced during the call.
Average Percent of Packet Loss (Tx)	The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire call. However, it does report an average of the sampled values.
Average Percent of Packet Loss (Rx)	The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire call. However, it does report an average of the sampled values.

Data	Description
Average Packets Lost (Tx)	The number of packets transmitted that were lost during a call.
Average Packets Lost (Rx)	The number of packets from the far site that were lost during a call.
Average Latency (Tx)	The average latency of packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.
Average Latency (Rx)	The average latency of packets received during a call based on round-trip delay, calculated from sample tests done once per minute.
Maximum Latency (Tx)	The maximum latency for packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.
Maximum Latency (Rx)	The maximum latency for packets received during a call based on round-trip delay, calculated from sample tests done once per minute.
Average Jitter (Tx)	The average jitter of packets transmitted during a call, calculated from sample tests done once per minute.
Average Jitter (Rx)	The average jitter of packets received during a call, calculated from sample tests done once per minute.
Maximum Jitter (Tx)	The maximum jitter of packets transmitted during a call, calculated from sample tests done once per minute.
Maximum Jitter (Rx)	The maximum jitter of packets received during a call, calculated from sample tests done once per minute.
Call Priority	The AS-SIP call precedence level assigned to the call (populated only when AS-SIP is enabled on the system).

Download a Call Detail Report (CDR)

You can download a CDR using the system web interface.

To download a CDR:

- 1 In the web interface, click **Utilities > Services > Call Detail Report (CDR)**.
- 2 Click **Most Recent Call Report** and then specify whether to open or save the file on your computer.

Polycom Touch Device Software Updates

The following topics provide information on updating Polycom touch device software:

- [Required Prerequisites for RealPresence Touch Software Updates](#)
- [Required Prerequisites for Polycom Touch Control Software Updates](#)
- [Dynamic Polycom Touch Device Software Updates](#)
- [Configure Your Web Server as the Update Site](#)
- [Configure Your Web Server as the Update Site](#)
- [Update Software from the RealPresence Touch Web Interface](#)
- [Update Software from the RealPresence Touch Local Interface](#)
- [Updating RealPresence Touch Software from a USB Storage Device](#)
- [Update Polycom Touch Control Software from a USB Storage Device](#)
- [Troubleshooting for Software Upgrade Issues](#)

Required Prerequisites for RealPresence Touch Software Updates

The RealPresence Touch must run a software version that is compatible with the software version on the RealPresence Group system.

The RealPresence Touch, after pairing with the RealPresence Group system, verifies the compatibility of the RealPresence Touch panel and operating system software and requests a software update.

For additional details on software compatibility, refer to the appropriate version of the release notes available at support.polycom.com.

If you need to update your RealPresence Group system at the same time you update the Polycom touch device, update the system software first.

Update files for the RealPresence Touch are located on the Polycom support server. You can store the update files on a USB device, RealPresence Resource Manager system, or on your own web server.

No license number or key is needed to update the Polycom RealPresence Touch. You can configure the Polycom touch device to get software updates using any of the following methods:

- A Polycom RealPresence Resource Manager system
- A server on your network
- The online software server hosted by Polycom
- A USB 2.0 storage device in FAT32 format that you connect to the side of the device

Required Prerequisites for Polycom Touch Control Software Updates

The Polycom Touch Control must run a software version that is compatible with the software version on the RealPresence Group system.

It is recommended that you install the latest compatible Polycom Touch Control software for any given RealPresence Group system software version. When checking for software updates, the Polycom Touch Control first checks for the presence of a USB storage device. The system then lists the available Polycom Touch Control updates.

For additional details on software compatibility, refer to the appropriate version of the release notes available at support.polycom.com.

If you need to update a RealPresence Group system at the same time you update the Polycom Touch Control, update the system software first.

Update files for the Polycom Touch Control are located on the Polycom support server. You can store the update files on a USB device, RealPresence Resource Manager system, or on your own web server.

No license number or key is needed to update the Polycom Touch Control. You can configure the device to get software updates using any of the following methods:

- A Polycom RealPresence Resource Manager system
- A server on your network
- The online software server hosted by Polycom
- A USB 2.0 storage device in FAT32 format that you connect to the side of the device

Dynamic Polycom Touch Device Software Updates

You can post software for a Polycom touch device on a RealPresence Resource Manager system. Then, configure the device to get updates from the applicable system by entering the Production URL or Trial URL on the device Software Update screen.

When using a RealPresence Resource Manager system to automatically update the software for a system with an associated Polycom touch device, use the same management server for the touch device updates. This helps you control the version of software installed on the touch device.



Note: When a Polycom touch device is connected to a provisioned RealPresence Group system, a RealPresence Resource Manager system can receive status updates from and provide software updates to the touch device. For supported RealPresence Resource Manager versions, go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html and click **Current Interoperability Matrix**.

For information about configuring production and trial versions of software update packages, refer to the *Polycom RealPresence Resource Manager System Operations Guide* available at support.polycom.com.

Configure Your Web Server as the Update Site

You can post software to your web server and then configure the RealPresence Touch device to receive updates.

To set up your web server as the update site:

- 1 Make sure that your server enables clients to download files with the following extensions or with no extension:
 - .tar.gz
 - .txt
 - .sig
 - .plcm
- 2 Define a URL on your server that the RealPresence Touch can use for software updates, and create a corresponding root directory to it.
- 3 Go to support.polycom.com, and navigate to the page for the RealPresence Group system that you use with the RealPresence Touch.
- 4 Save and extract the RealPresence Touch operating system software package (.tar file) from the Polycom website to the root directory of the web server.

Configure Your Web Server as the Update Site

You can post software to your web server and then configure the Polycom Touch Control to receive updates.

To set up your web server as the update site:

- 1 Make sure that your server enables clients to download files with the following extensions or with no extension:
 - .tar.gz
 - .txt
 - .sig
 - .plcm
- 2 Define a URL on your server that the Polycom Touch Control can use for software updates, and create a corresponding root directory to it.
- 3 Go to support.polycom.com, and navigate to the page for the RealPresence Group system that you use with the Polycom Touch Control.
- 4 Save and extract the Polycom Touch Control Panel software package (.zip file) and the Polycom Touch Control Operating System software package (.zip file) from the Polycom website to the root directory of the web server.
- 5 Open a command line interface and enter the command appropriate for your operating system to generate an info.txt file that lists the folders with updates:
 - Unix or Linux: `<root dir>/dists/venus/geninfo.sh`
 - Windows: `<root dir>\dists\venus\geninfo.bat`

Managing Polycom Touch Device Software on Your Server

When checking for software updates on your server, Polycom touch devices check only for what is referred to as the “current” release of the system software. By default, the current release is the software distribution package that was most recently extracted on your server.

Over time, you might extract other versions of the software on your server, resetting the current release with every extraction. In addition, you could accumulate multiple versions of the same software.

Each software distribution package contains two commands that you can use to maintain all of the software extracted on your server.

- The `setcurrel` command sets a specific version of software as the current release.
- The `removerel` command removes a specific version of a software release from your server.

Set a RealPresence Touch Software Version as Current

Use the `setcurrel` command to set a specific version of RealPresence Touch software as the current release on your server.

To set a version of the software as the current version:

- 1 Run the `setcurrel` command with X.X.X-XXX as the software version you want to set as the current release:
 - Unix or Linux: `<root dir>/vega/platform/setcurrel.sh X.X.X-XXX`
 - Windows: `<root dir>\vega/platform/setcurrel.bat X.X.X-XXX`
- 2 Follow the onscreen instructions for setting the current release.

Remove a RealPresence Touch Software Version

Use the `removerel` command to remove a specific version of a RealPresence Touch software release from your server.

To remove a software version:

- 1 Run the `removerel` command with X.X.X-XXX as the software version you want to set remove from the server:
 - Unix or Linux: `<root dir>/vega/platform/removerel.sh X.X.X-XXX`
 - Windows: `<root dir>\vega/platform/removerel.bat X.X.X-XXX`
- 2 Follow the onscreen instructions for setting the current release.

Set a Polycom Touch Control Software Version as Current

Use the `setcurrel` command to set a specific version of Polycom Touch Control software as the current release on your server.

To set a version of the software as the current version:

- 1 Run the appropriate `setcurrel` command with X.X.X-XXX as the software version you want to set as the current release.

Software Type	Unix or Linux Command	Windows Command
Panel	<root dir>/dists/venus/apps/setcurrel.sh X.X.X-XXX	<root dir>\dists\venus\apps\setcurrel.bat X.X.X-XXX
Operating system	<root dir>/dists/venus/platform/setcurrel.sh X.X.X-XXX	<root dir>\dists\venus\platform\setcurrel.bat X.X.X-XXX

- 2 Follow the onscreen instructions for setting the current release.

Remove a Polycom Touch Control Software Version

Use the `removerel` command to remove a specific version of a Polycom Touch Control software release from your server.

To remove a software version:

- 1 Run the `removerel` command with X.X.X-XXX as the software version you want to set remove from the server.

Software Type	Unix or Linux Command	Windows Command
Panel	<root dir>/dists/venus/apps/removerel.sh X.X.X-XXX	<root dir>\dists\venus\apps\removerel.bat X.X.X-XXX
Operating system	<root dir>/dists/venus/platform/removerel.sh X.X.X-XXX	<root dir>\dists\venus\platform\removerel.bat X.X.X-XXX

- 2 Follow the onscreen instructions for removing the software version.

Update Software from the RealPresence Touch Web Interface

Using the web interface, you can update the RealPresence Touch software from the Polycom server or your own server.

To update RealPresence Touch software using the web interface:

- 1 Open a supported browser.
- 2 Configure the browser to allow cookies.
- 3 In the browser address line, enter the IP address of the RealPresence Touch using the format `http://IPAddress` (for example, `http://10.11.12.13`).
- 4 If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password, if one is set. The default password is the RealPresence Touch serial number.


The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.

- 5 On the Home Page, click **Software Update**.
- 6 Enter the server address for the update. The default server address, `polycom`, is the address for the Polycom public soft-update repository and has the latest released software version available.
- 7 Click **Save** to save these changes.
- 8 Click **Check for Software Updates**.
- 9 Click **Download and Install Software**.
Download progress is displayed during installation.

Update Software from the RealPresence Touch Local Interface

Using the RealPresence Touch interface, you can update the RealPresence Touch software from the Polycom server or your own server.

To update software using the RealPresence Touch interface:

- 1 From the Home screen, touch  **Administration** and then touch **Software Update**.
- 2 Enter the path and address of the update site where you posted the RealPresence Touch software in the in the Server Address field. To use the Polycom server, enter `polycom`.
- 3 Touch **Check for Software Updates**.
- 4 Touch **Download and Install Software**.

Updating RealPresence Touch Software from a USB Storage Device

If you cannot update your RealPresence Touch device using a server or with RealPresence Resource Manager, you can load the software onto a USB storage device and use that to update the device. Another benefit of using a USB device is that you can choose to perform both a factory restore and update your device software simultaneously.

The following attributes ensure that your USB device supports the software update procedure:

- Use USB 2.0 devices (some USB 3.0 devices might not work with the RealPresence Touch).
- Format the primary partition as FAT32.

Make sure to put all software update data in the root directory of the primary partition.

Update the RealPresence Touch With a USB Storage Device

You can use a USB storage device to update RealPresence Touch software and the RealPresence Touch factory restore partition.

To update RealPresence Touch software and the factory restore partition:

- 1 Open a browser and navigate to support.polycom.com.

- 2 Under **Documents and Downloads**, select **Telepresence and Video**.
- 3 Navigate to the page for the version of the system that you use with the RealPresence Touch.
- 4 Save the RealPresence Touch operating system software package (.tar) file from the Polycom website to the root directory of the USB device.
- 5 Disconnect the Ethernet power cable from the RealPresence Touch.
- 6 Connect the USB device to the side of the RealPresence Touch.
- 7 Press and hold the RealPresence Touch factory restore button with a bent paper clip for ten seconds and simultaneously reconnect the Ethernet power cable to the RealPresence Touch. For more information about RealPresence Touch factory restore refer to the *Polycom RealPresence Group Series Administrator Guide* available at support.polycom.com
- 8 Follow the on-screen instructions of the setup wizard to complete the update. The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the factory restore button.

Update RealPresence Touch Software from a USB Storage Device

You can update the RealPresence Touch quickly using a USB storage device without updating the RealPresence Touch factory restore partition.

To update RealPresence Touch software from a USB device:

- 1 Open a browser and navigate to support.polycom.com.
- 2 Under **Documents and Downloads**, select **Telepresence and Video**.
- 3 Navigate to the page for the RealPresence Group system that you use with the RealPresence Touch.
- 4 Save the RealPresence Touch operating system software package (.tar) file from the Polycom website to the root directory of the USB device.
- 5 Ensure the RealPresence Touch Ethernet cord is connected and the RealPresence Touch is powered on.
- 6 Connect the USB device to the side of the RealPresence Touch.
- 7 An automatic prompt asks you if you want to update the platform software. Touch **Yes**.

Update Polycom Touch Control Software Manually

You can manually update Polycom Touch Control software from the Polycom server or your own server.

Polycom recommends that you set the maintenance window times so that the Polycom Touch Control is updated about an hour after the last RealPresence Group system update has completed.

To manually install updates from the web interface:

- 1 Open a supported browser.
- 2 Configure the browser to allow cookies.
- 3 In the browser address line, enter the IP address of the Polycom Touch Control using the format `http://IPaddress` (for example, `http://10.11.12.13`).

- 4 If necessary, enter the Admin ID as the user name (default is admin), and then enter the Admin remote access password, if one is set. The default password is 456.

The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.

- 5 On the Home Page, under Touch Control details, click **Software Update**.
- 6 Enter the server address for the update, then click **Save**. The default server address, `polycom`, is the address for the Polycom public soft-update repository and has the latest released software version available.
- 7 Click **Check for Software Updates** to find the latest build on the server.
The Polycom Touch Control Operating system and panel software versions are listed.
- 8 Click **Download and Install Software**.
Download progress is displayed during installation.
- 9 Follow the on-screen instructions to complete the update.

Update Polycom Touch Control Software Automatically in the Web Interface

You can automatically update the Polycom Touch Control software from the Polycom server or your own server. The Polycom Touch Control automatically performs a software update when one of the following conditions are true:

- Auto Update is enabled (with **Download and Install Software** selected), and the scheduled time occurs for a software update. (Example: Scheduled time is set for 3 p.m., so the software update begins at 3 p.m.)
- Auto Update is enabled (with **Download and Install Software** selected), and the paired Group Series system finishes its software update (which triggers a Polycom Touch Control software update).

To automatically install updates in the web interface:

- 1 Open a supported browser. For a list of supported browsers, refer to the *Polycom RealPresence Group Series Release Notes*.
- 2 Configure the browser to allow cookies.
- 3 In the browser address line, enter the IP address of the RealPresence Group system using the format `http://IPaddress` (for example, `http://10.11.12.13`).
- 4 If necessary, enter the Admin ID as the user name (default is admin), and then enter the Admin remote access password, if one is set.
The first time you open the web interface each day, you might need to enter a user name and password after you select any of the interface options.
- 5 On the Home Page, under Touch Control details, click **Update Software**.
- 6 Enter the server address for the update, then click **Save**. The default server address, `polycom`, is the address for the Polycom public soft-update repository and has the latest released software version available.
- 7 To make automatic updates and update your software to the latest build on the server, select **Automatically Check for Software Updates**.
- 8 When the Export Restrictions notice appears, touch **Accept Agreement**.

- 9 Specify the automatic update options:
 - a Touch **Hour**, **Minute**, and **AM/PM** to specify the beginning of the time window within which the Polycom Touch Control checks for updates.
 - b Touch **Duration** to select the length of the time within which the Polycom Touch Control can check for updates.


After the Start Time and Duration settings are configured, the Polycom Touch Control calculates a random time within the defined update window at which to check for updates. It then checks for updates at this time on a daily basis as long as the Start Time and Duration values do not change. If the Start Time or Duration values change, a new random time within the new time window is calculated.
 - c Touch **Action for Available Software Updates** and select whether to be notified of available status updates only or to download and install software when updates are available.
- 10 Follow the on-screen instructions to complete the update.

Update Polycom Touch Control Software Automatically in the Local Interface

Using the Polycom Touch Control interface, you can automatically update the software from the Polycom server or your own server.

Polycom recommends that you set the maintenance window times so that the Polycom Touch Control is updated about an hour after the last RealPresence Group system update has completed.

To automatically install updates:


- 1 From the Home screen, touch  **Administration** and then touch **Updates**.
- 2 Enter the path and address of the update site where you posted the Polycom Touch Control software in the **Server Address** field. To use the Polycom server, enter `polycom`.
- 3 Enable **Automatically Check for Software Updates**.
- 4 When the Export Restrictions notice appears, touch **Accept Agreement**.
- 5 Specify the automatic update options:
 - a Touch **Hour**, **Minute**, and **AM/PM** to specify the beginning of the time window within which the Polycom Touch Control checks for updates.
 - b Touch **Duration** to select the length of the time within which the Polycom Touch Control can check for updates.

After the **Start Time** and **Duration** settings are configured, the Polycom Touch Control calculates a random time within the defined update window at which to check for updates. It then checks for updates at this time on a daily basis as long as the **Start Time** and **Duration** values do not change. If the **Start Time** or **Duration** values change, a new random time within the new time window is calculated.
 - c Touch **Action for Available Software Updates** and select whether to be notified of available status updates only or to download and install software when updates are available.

Manually Update Polycom Touch Control Software in the Local Interface

You can manually update the Polycom Touch Control Software using the Polycom Touch Control interface.

To manually install updates:

- 1 From the Home screen, touch  **Administration** and then touch **Updates**.
- 2 Enter the path and address of the update site where you posted the Polycom Touch Control software in the in the **Server Address** field. To use the Polycom server, enter `polycom`.
- 3 Touch **Check for Software Updates**.
- 4 Select only the updates that you want to install.
- 5 Touch **Download and Install Software**.
- 6 When the Export Restrictions notice appears, touch **Accept Agreement**. Follow the on-screen instructions to complete the update.


Update Polycom Touch Control Software from a USB Storage Device

You can use a USB storage device to either update or downgrade Polycom Touch Control software versions.

The following device attributes ensure that your USB device successfully supports the procedure:

- Use USB 2.0 devices (some USB 3.0 devices might not work with the RealPresence Group systems).
- Format the primary partition as FAT32.
- Put all software update data in the root directory of the primary partition.

To update Polycom Touch Control software using a USB device:

- 1 Open a browser and navigate to support.polycom.com.
- 2 Under **Documents and Downloads**, select **Telepresence and Video**.
- 3 Navigate to the page for the Polycom RealPresence Group system that you use with the Polycom Touch Control.
- 4 Download the latest version of these .zip distribution package files to your hard drive:
 - Polycom Touch Control Operating System
 - Polycom Touch Control Panel Software
- 5 Extract all contents of the files you downloaded to the root directory of the USB device.
When extracting multiple distribution packages, a pop up message might appear asking if you want to overwrite certain files that already exist. Select **Yes to All**.
- 6 Connect the USB device to the side of the Polycom Touch Control.
- 7 From the Home screen, touch  **Administration** and then touch **Updates**.
- 8 Touch **Check for Software Updates**.
- 9 Select only the updates that you want to install.
- 10 Touch **Download and Install Software**.
- 11 When the Export Restrictions notice appears, touch **Accept Agreement**. Follow the on-screen instructions of the setup wizard to complete the update. The setup wizard is available during initial setup, after a system reset with system settings deleted, or after using the factory restore button.

Troubleshooting for Software Upgrade Issues

If you are having trouble upgrading your system or device, these troubleshooting tips might help.

Test the Download URL

If your system or Polycom touch device is not updating properly, and you entered `polycom` as the Server Address, the system resolves `downloads.polycom.com` to an IP address. The system then checks for a software update using `http`.

To test the default download URL:

- 1 Open a browser.
- 2 Try to access the appropriate URL for your system or device.

System or Device	Test URL
Polycom Touch Control	<code>http://downloads.polycom.com/video/venus_group_series/dists/venus/info.txt</code>
Polycom RealPresence Touch	<code>http://downloads.polycom.com/video/rp_touch/vega/info.txt</code>
RealPresence Group Series	<code>http://downloads.polycom.com/video/group_series/rseries/info.txt</code>

- 3 If the computer returns `platform`, or `apps` and `platform`, you can reach the Polycom software server from your location and the URL is working.

Polycom Touch Devices

The following topics provide information on how to enable and set up Polycom touch devices:

- [Positioning the RealPresence Touch Device](#)
- [Positioning the Polycom Touch Control](#)
- [Powering On the Polycom Touch Control](#)
- [Polycom Touch Control Indicator Light](#)
- [Pairing the RealPresence Touch with a RealPresence Group System](#)
- [Power Off the RealPresence Touch](#)
- [Wake the RealPresence Touch](#)
- [Remote Management of the RealPresence Touch](#)
- [Customize the RealPresence Touch Home Screen](#)
- [Change the Home Screen Background Image on the RealPresence Touch](#)
- [Troubleshooting the RealPresence Touch Device](#)
- [Set Up the Polycom Touch Control](#)
- [Pairing States for the Polycom Touch Control Device](#)
- [Pair the Polycom Touch Control and a RealPresence Group System](#)
- [Unpair the Polycom Touch Control and a RealPresence Group System](#)
- [Power Off the Polycom Touch Control](#)
- [Wake the Polycom Touch Control](#)
- [Configuring the Polycom Touch Control Software](#)
- [Managing the Polycom Touch Control Remotely](#)
- [Troubleshooting on the Polycom Touch Control Device](#)

Positioning the RealPresence Touch Device

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 system monitor displays. The RealPresence Touch device can be positioned horizontally at either a 30 degree or 65 degree viewing angle.

Positioning the Polycom Touch Control

Before you use your touch device for the first time, ensure that it is placed properly in the meeting room.


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 Polycom Touch Control is conveniently located for use during a meeting.

Powering On the Polycom Touch Control

For instructions on how to power on the RealPresence Touch, refer to [Set Up the RealPresence Touch Device](#).

For instructions on how to power on the Polycom Touch Control, refer to [Set Up the Polycom Touch Control](#).

Polycom Touch Control Indicator Light

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

Enable the RealPresence Touch

Before your users can control the system with the RealPresence Touch device, you must enable the device on the system's web interface. Once the device is enabled, you can pair it to the system.

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

To enable RealPresence Touch:

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

Enable the Polycom Touch Control

You must enable the Polycom Touch Control device on the web interface before users can use the device to control a video room system.

To enable the Polycom Touch Control device:

- 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 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.

For details on setting up the Polycom Touch Control, see [Set Up the Polycom Touch Control](#).

Set Up the RealPresence Touch Device

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

To set up the RealPresence Touch device:

- 1 Ensure that you have completed the setup wizard on the system.
- 2 Connect the Ethernet cable to the RealPresence Touch.
- 3 Plug the Ethernet cable into the wall outlet:
 - If your room provides Power Over Ethernet, you can connect the Ethernet cable directly to a LAN outlet.
 - If your room does not provide Power Over Ethernet, you must connect the Ethernet cable to the power supply adapter. Then connect the power supply adapter to a LAN outlet and power outlet.

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

- 4 Choose your language and follow the onscreen instructions.
- 5 After the RealPresence Touch connects to the network, enter the system IP address at **Device Address**, then enter the **Admin ID** and **Password**.
- 6 Tap **Pair**.

If the system is configured to allow pairing and you entered the IP address, admin ID and password for the system correctly, the RealPresence Touch device pairs with the system. When pairing is successful, the RealPresence Touch splash screen is displayed, followed by the home screen.

Pairing the RealPresence Touch with a RealPresence Group System

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

After you have completed RealPresence Touch setup, you can pair to a different system using RealPresence Touch settings.

RealPresence Touch Pairing and Connection States

The following table describes the pairing and connection states:

State	Description
Unpaired	The RealPresence Touch is not associated with a room system.

State	Description
Paired and Connected	The RealPresence Touch is associated with a system through the pairing process, and is connected to a room system. This is normal operating mode. A RealPresence Touch can be connected to only one RealPresence Group system at a time.
Paired and Disconnected	The RealPresence Touch is associated with a room system, but communication is disrupted, usually because of a system power off or LAN issue. Communication is automatically restored when a system and the touch device are successfully connected to the LAN.

Pair the RealPresence Touch and a System For the First Time

To pair your RealPresence Touch with a system that has not been paired before, you must enter the system's credentials before connection can be established.

To manually pair for the first time to a 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 room system.
- 4 Tap **Pair**.

The pairing connection begins, and the Home screen displays when the pairing is successful.

Pair a Previously Paired System to a RealPresence Touch

If you have paired with a 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.

To pair a 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 system that you want to pair with.

The pairing connection begins, and the Home screen displays when the pairing is successful.

If you unpair from the system, any current calls on the system are still active. To hang up the calls, repair to the room system and select **More Options**, then **Participants**, **More Options**, and **Remove** or **Remove All**.



Note: 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 room system. An administrator can determine which device is paired and can unpair the device using the room system web interface. In the 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 room system and the RealPresence Touch are paired, the system web interface and the RealPresence Touch interface display information about each other and about their connection status.

Unpair the RealPresence Touch and a System

You can unpair the RealPresence Touch and a RealPresence Group system.

To unpair the RealPresence Touch and a system:

- 1 In the system web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
- 2 Clear the check box next to **Enable Polycom Touch Device**.
- 3 Click **Save**.

The system cannot pair with any touch device while the **Enable Polycom Touch Device** check box is cleared.

Remove a System from the Paired System List

You can remove a system from the device's paired system list.


To remove a room system from the paired system list:

- 1 In the web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
- 2 Click **Forget this Device**.
- 3 Click **Save**.

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 the RealPresence Touch

The RealPresence Touch goes to sleep after two minutes of inactivity. To wake it, you can touch the screen.

To wake the RealPresence Touch:

- » Touch the screen.

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

Remote Management of the RealPresence Touch

You can remotely manage certain features of your RealPresence Touch. For a list of supported browsers, refer to the *Polycom RealPresence Group Series Release Notes*.

You can manage the following features remotely:

- **Download Logs:** Downloads the RealPresence Touch logs to the location specified in the device.
- **Network Settings:** Specifies whether the system acquires an IP address automatically or manually. With the manual method, the other settings that are available from the RealPresence Touch become available on the web.
- **Pair:** Pairs and unpairs from room systems. Before you can connect to or pair with a device, you must know the device's IP Address and the User Name and password used to connect.
- **Security:** Changes the admin ID and password of the RealPresence Touch.
- **Software Updates:** Updates the RealPresence Touch software. You can update from the default Polycom server or your own server by entering the appropriate IP address.
- **View RealPresence Touch Screens:** Shows the screen currently being displayed on the RealPresence Touch. You can click **Refresh** at any time to see if the screen has changed.

Open a Remote Management Window for the RealPresence Touch

You can open a remote management window for your RealPresence Touch in a web browser.

To open a remote management window:

- 1 In a web browser, enter the IP address of the RealPresence Touch device.
- 2 In the login window, enter the **ID** and **Password** you use to access the administrative features of the RealPresence Touch.

You can access the remote management features by using the Navigation menu or the Dashboard. To return to the **Dashboard**, click the Home icon.

Download Logs Using the RealPresence Touch

You can download RealPresence Group system logs using the RealPresence Touch.

To download logs using the RealPresence Touch:

- 1 In the RealPresence Touch web interface, click **Download Logs**.
- 2 A .tar file is downloaded to your local computer.

You can extract the file and open it to review the log information.

Pair the RealPresence Touch and a System on the Web Interface

To pair your RealPresence Touch with a RealPresence Group system, you must enter the system's credentials before connection can be established.

To manually pair the RealPresence Touch to a system:

- 1 In the RealPresence Touch web interface, click **Pairing**.
- 2 At **Device**, select **RealPresence Group Series**.

- 3 Enter the **IP Address or Host Name**, **User Name**, and **Password** for the system.
- 4 Click **Pair**.

The pairing connection begins, and the Home screen displays when the pairing is successful.

Use the RealPresence Touch to Unpair a System on the Web Interface

You can unpair the RealPresence Touch and a RealPresence Group system.

To unpair a system from the RealPresence Touch:

- 1 In the RealPresence Touch web interface, click **Pairing**.
- 2 Click **Unpair**.

Change the User Name and Password for the RealPresence Touch

You can change the security credentials for the RealPresence Touch device.

To change security credentials for the RealPresence Touch:

- 1 In the RealPresence Touch web interface, click **Security**.
- 2 At **Admin ID**, enter your admin ID.
- 3 At **Current Password**, enter the current password.
- 4 At **Password**, enter the new password.
- 5 At **Confirm Password**, reenter the new password.
- 6 Click **Save**.

Customize the RealPresence Touch Home Screen

You can use the system web interface to configure how information is displayed on the Home screen of the RealPresence Touch device. These settings are included in the System settings profile, and included in bundled provisioning when using RealPresence Resource Manager.

To configure the RealPresence Touch Home Screen:

- 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 screen that are described in the following sections.



Note: To enable the Recent Calls and Speed Dial icons, do the following:

- Recent Calls: In the web interface, go to **Admin Settings > General Settings > System Settings > Recent Calls**. Select the **Enable Recent Calls** checkbox.
- Speed Dial: In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > Speed Dial**. Select the **Enable Speed Dial** checkbox.

Choose Icon Buttons to 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 selections display on the screen. You can customize one of the icon buttons to be the default. All of the other **Place a Call** icon buttons continue to display at the top of the screen.

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 Place a Call screen.

To revert back to the default icons, at **Configure Home Screen**, select **Default Configuration**, and click **Save**.

Change the Home Screen Background Image on the RealPresence Touch

The RealPresence Touch device allows you to upload a custom background image that is separate from the system monitor background. If a custom image is not loaded, the image from the primary system screen displays as the RealPresence Touch device background when it is paired with the system (default behavior). To create a custom background on the RealPresence Touch, you must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format that is less than 5 MB.

To upload a background monitor image:

- 1 In the web interface, go to **Admin Settings > General Settings > Home Screen Settings > RealPresence Touch Background**.
- 2 Browse to the desired image file and click **Choose File > Upload**.

The custom image displays paired RealPresence Touch Home screen.

Troubleshooting the RealPresence Touch Device


For information on troubleshooting the RealPresence Touch, see the following topics:

- [View System Details and Connection Status on the RealPresence Touch](#)
- [View Call Statistics on the RealPresence Touch](#)
- [Transfer RealPresence Touch Logs to a USB Storage Device](#)
- [Perform a Factory Restore on the RealPresence Touch](#)
- [Perform a RealPresence Touch Factory Restore Using a USB Storage Device](#)

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 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**.

Transfer RealPresence Touch Logs to a USB Storage Device

You might find log files useful when troubleshooting. You can transfer RealPresence Touch logs to a USB storage device.

- 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: The USB storage device must be in FAT32 format.

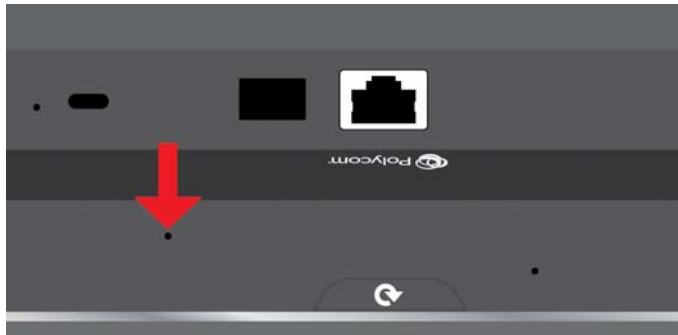
Perform a Factory Restore on the RealPresence Touch

If the RealPresence Touch device is not functioning correctly or you have forgotten the Administration password, you can use the factory restore button to reset the device. This operation completely erases the RealPresence Touch device's settings and reinstalls the default platform and applications.



Note: Do not power off the device during the factory restore process.

The restore button pinhole is on the back of the RealPresence Touch, as shown in the following figure.



To reset the RealPresence Touch device:

- 1 Disconnect the ethernet cable to power off the device.
- 2 Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
- 3 Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
- 4 Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
- 5 Follow the instructions on the setup wizard.

When the process is complete, the device displays the splash screen and then the home screen.

Perform a RealPresence Touch Factory Restore Using a USB Storage Device

If you want to install a particular software build on the RealPresence Touch, you can perform a a factory restore using a USB storage device. Do not power off the device during the factory restore process.

To perform a factory restore on the RealPresence Touch using a USB Storage Device:

- 1 Copy a build package (.tgz file) to the root directory of a USB storage device.
- 2 Disconnect the ethernet cable to power off the device.
- 3 Insert the USB storage device into the side USB port of the device.
- 4 Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
- 5 Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
- 6 Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
- 7 Follow the instructions on the setup wizard.

When the process is complete, the device displays the splash screen and then the home screen.

Set Up the Polycom Touch Control

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

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.
- 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](#).

Pairing States for the Polycom Touch Control Device

When you configure the Polycom Touch Control to pair with a particular 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.

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 screen.

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 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 RealPresence Group systems.

The following table describes the pairing states:

State	Description
Paired	The Polycom Touch Control is successfully connected to the RealPresence Group system through the pairing process, including providing the RealPresence Group admin ID and password. A single Polycom Touch Control can be paired to multiple 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 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 .
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 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 a 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

You can pair the Polycom Touch Control and a RealPresence Group system using the web interface.


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: 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.

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 a RealPresence Group system:


- 1 On the system web interface, 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.

Power Off the Polycom Touch Control

You can 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 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.

Configuring the Polycom Touch Control Software

Before you use the Polycom Touch Control, you must configure the LAN setting, and optionally, the regional setting.


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

- [Configure Polycom Touch Control LAN Settings](#)
- [Configure Polycom Touch Control Location and Time Settings](#)
- [Configure Admin ID and Password for the Polycom Touch Control](#)

Configure Polycom Touch Control LAN Settings

Before you can pair 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. <ul style="list-style-type: none"> • 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 Polycom 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 View the general settings.

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

Configure Polycom Touch Control Location and Time Settings

You can configure location settings on the Polycom Touch Control.

To configure the Polycom Touch Control location 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: <ul style="list-style-type: none"> • 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 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 <code>admin</code> .
Admin Password	Specifies the password for administrator access when logging in to the Touch Control. The default password is <code>456</code> . When this password is set, you must enter it to configure the Touch Control Admin Settings. The password must not contain spaces.

Managing the Polycom Touch Control Remotely

You can remotely manage certain features of your Polycom Touch Control from within your enterprise environment.

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 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.

Open the Remote Management Window for the Polycom Touch Control

You can open the Polycom Touch Control in a browser window to perform remote management functions.

To open the remote management window:

- 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.

Troubleshooting on the Polycom Touch Control Device

For information on troubleshooting the Polycom Touch Control, see the following topics:

- [View Call Statistics for an Active Point-to-Point Call on the Polycom Touch Control](#)
- [View Call Statistics for an Active Multipoint Call on the Polycom Touch Control](#)
- [Transfer RealPresence Touch Logs to a USB Storage Device](#)
- [View Polycom Touch Control System Details](#)
- [Factory Restore on the Polycom Touch Control](#)
- [Perform a Factory Restore on a Polycom Touch Control](#)
- [Perform a Factory Restore on a Polycom Touch Control Using a USB Storage Device](#)

View Call Statistics for an Active Point-to-Point Call on the Polycom 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 **i**. 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 on the Polycom Touch Control

During a multipoint call, you can view call statistics about any of the call participants or about an active stream.

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 **i**.
 - The participants' active streams are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and touch **i**. From an individual stream view you can select **Next Stream** to view the next stream in the stream list.

To quickly access a list of all active audio, video, and content streams within the call, navigate to **Active Streams**. This setting is available in SVC calls only. Select the desired stream and touch **i**.

Transfer Polycom Touch Control Logs to a USB Storage Device

You might find log files useful when troubleshooting. 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.

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.

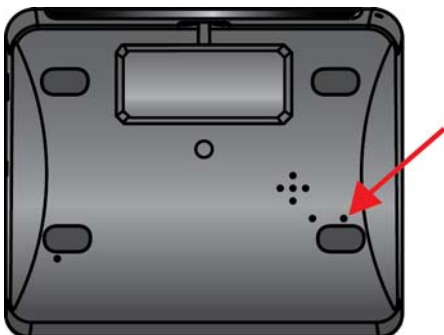
To view your Polycom Touch Control system details:

- 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.

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.



Perform a Factory Restore on a Polycom Touch Control

If the Polycom Touch Control 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 device's settings and reinstalls the default platform and applications. Do not power off the device during the factory restore process.

To reset the Polycom Touch Control using the factory 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 a Polycom Touch Control Using a USB Storage Device

If you want to install a particular software build on the Polycom Touch Control, 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 on the Polycom Touch Control using 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 device.
- 4 Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
- 5 Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
- 6 Wait for the Polycom Touch Control 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.

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.

VisualBoard Application

To learn how to configure the VisualBoard application and to install the application for use with touch or standard monitors on RealPresence Group systems, refer to the following topics.

- [VisualBoard Application Support](#)
- [Touch Monitor Support](#)
- [Enable the VisualBoard Application](#)
- [Prerequisites to Install a Second Monitor for Use with the VisualBoard Application](#)
- [Install a Second Monitor for Use With the VisualBoard Application](#)
- [Configure Monitor 1 as the Content Monitor](#)
- [Configure Monitor 2 as the Content Monitor](#)
- [Polycom® UC Board](#)

VisualBoard Application Support

The VisualBoard application is an integrated application that is supported on RealPresence Group systems. The application works with the following system models:

- Polycom RealPresence Group 300 system
- Polycom RealPresence Group 310 system
- Polycom RealPresence Group 500 system
- Polycom RealPresence Group 700 system

The VisualBoard application works with the following software versions:

- Polycom RealPresence Group system software version 4.1.3 and later
- Polycom RealPresence Immersive Studio software version 4.2.0 and later

The VisualBoard application can also be launched from the following Polycom touch devices:

- RealPresence Touch
- Polycom Touch Control

Prerequisites for the VisualBoard Application

Before you can begin using the VisualBoard application, ensure that you have done the following:

- Installed and configured one of the following: USB mouse, 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/RDP setting 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.

Touch Monitor Support

The VisualBoard application supports several different touch monitors for use with Polycom systems. For a list of supported monitors, refer to the *Polycom RealPresence Group Series Release Notes* at support.polycom.com. To enable the touch monitor interface on RealPresence Group 300 and RealPresence Group 310 systems, you must activate the dual monitor option key in the system's web interface. For information on the activation procedure, refer to [Software and System Option Keys](#).

Enable the VisualBoard Application

You must enable the VisualBoard application before you can use it with the RealPresence Group system.

To enable the VisualBoard application:

- 1 From the room system web interface, go to **Admin Settings > General Settings > System Settings > VisualBoard/RDP**.
- 2 Select **Enable**, and then select **Save**.

Prerequisites to Install a Second Monitor for Use with the VisualBoard Application

Before you can use a touch or standard monitor as the second monitor with a RealPresence Group system, you must do the following:

- 1 Enable the VisualBoard application.
- 2 Configure and connect at least monitor 1 and monitor 2 to the system.

You need the following components to connect a second monitor to a RealPresence Group system:

- USB cable
- USB storage device (optional)
- HDMI cable
- DVI-HDMI adaptor (optional)

For RealPresence Group 500 and 700 systems, the VisualBoard application works only as monitor 2, so the monitor must be connected to monitor 2 HDMI monitor output.

Install a Second Monitor for Use With the VisualBoard Application

To install a touch or standard monitor as a second monitor, follow the steps in this section. For RealPresence Group 310 systems, you must have a dual option key installed to use a second monitor with the system. Polycom recommends the use of digital output for content (DVI-D or HDMI) instead of analog (VGA or YPbPr) when using the VisualBoard application. Digital content produces the optimum results with alignment of the VisualBoard application. For information on configuring a touch monitor, refer to [Configure Secondary Monitors for Content in a Multiple Touch Monitor Environment](#).

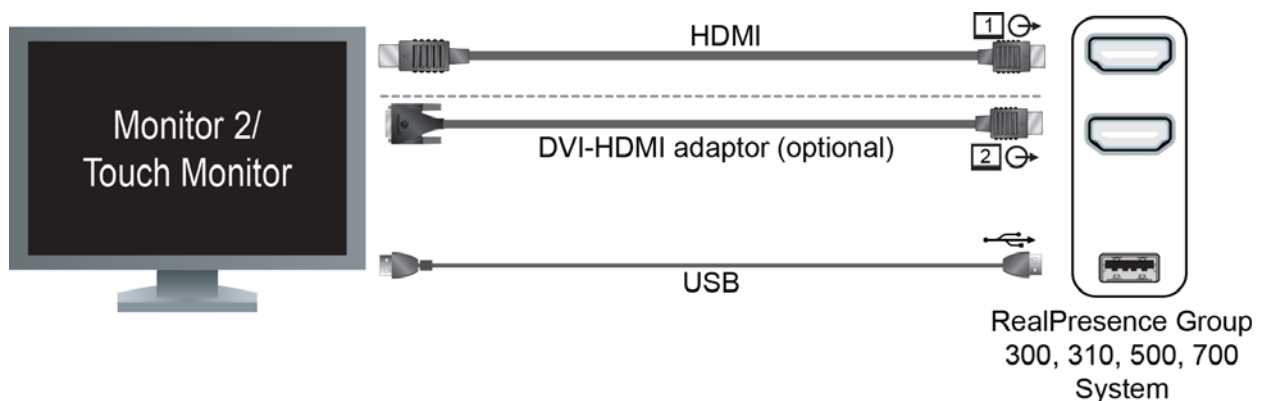
To install a monitor as a second monitor:

- 1 Connect the video cable by doing one of the following:
 - Connect one end of an HDMI cable to the HDMI Input port on the monitor. Connect the other end of the HDMI cable to the Monitor 2 HDMI Output port on the RealPresence Group system.
 - If your monitor has only a DVI input port, use a DVI-HDMI adaptor to connect it to the HDMI output port of the RealPresence Group system.
- 2 Connect the touch monitor to the system.

If you are using a Polycom UC Board sensor with your current content monitor, the sensor is connected to the RealPresence Group system.

 - a Connect one end of a USB cable to the USB port on the touch monitor.
 - b Connect the other end of the USB cable to the USB port on the RealPresence Group system.

A USB storage device can also be installed in the second USB port on the RealPresence Group system for importing and exporting slides, images, or photos.
- 3 To connect cables from the monitor 2 or the touch monitor to the RealPresence Group system, refer to the next figure.



Configure Monitor 1 as the Content Monitor

To use the VisualBoard application on your system's Monitor 1, you must configure monitor settings on the web interface. If you are using a touch monitor as Monitor 1, you can run the VisualBoard application on the monitor and touch the screen to interact with the application.

Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use **Game Mode**, if that setting is available.

To configure monitor 1 to show content and the VisualBoard application:

- 1 In the web interface, go to **Admin Settings > Audio/Video > Monitors**.
- 2 Under Monitor 1 for the **Enable** setting, select **Manual**.
- 3 For the Monitor Profile setting, select **Content, then Far, then Near** or **Content, then Far**.

Configure Monitor 2 as the Content Monitor

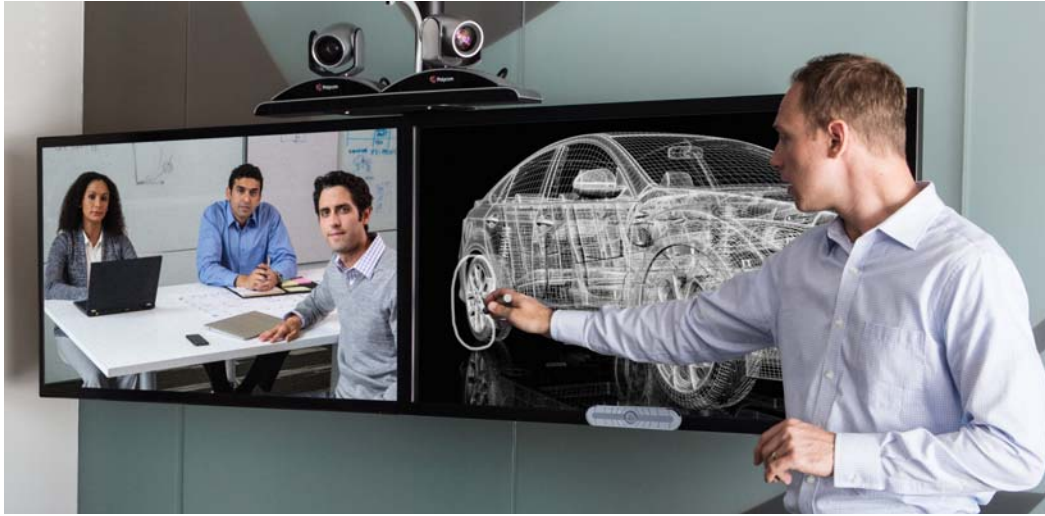
The VisualBoard application runs on Monitor 2 by default, but you might want to make configuration changes to the monitor settings. Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use **Game Mode**, if that setting is available.

To configure monitor 2 to show content:

- 1 In the system web interface, go to **Admin Settings > Audio/Video > Monitors**.
- 2 To configure monitor 1, go to **System > Admin Settings > Monitors**. At **Enable**, select either **Auto** or **Manual**. If you chose **Manual**, select any of the available profiles, except **Content, then Far, then Near** or **Content, then Far**.
- 3 To configure monitor 2, at **Monitor Profile**, enable one of the content profiles, such as **Content, then Far, then Near**, **Content, then Far**, **Content, then Near**, or the **Content Only** profile.

Polycom® UC Board

With the Polycom® UC Board, you can show and annotate content in real-time from 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. For flat, cold surfaces such as white boards with projectors, Polycom suggests that you use the Polycom UC Board.



Two monitors are required to use the Polycom UC Board. The second monitor can be either a projector used with a whiteboard, or a monitor.

Polycom recommends the following installation tips:

- Use LED backlit, LCD displays instead of CFL LCD displays.
- Do not use plasma backlit displays.
- The UC Board hardware sensor and pen are designed for cold surfaces, such as white boards with projectors.
- Mount the hardware sensor on the top of the display device. Room lights can interfere with the sensor when it is mounted on the bottom of the display.

The UC Board sensor supports one stylus at a time. It does not support using two styluses simultaneously.

For more information on setting up and using the UC Board, refer to the *Polycom UC Board Quick Start Guide*, available with the UC Board hardware and at support.polycom.com.

Configure the Polycom UC Board

You can configure the Polycom UC Board to show content.

To set up two monitors and configure to show content:

- 1 To configure monitor 1, go to **System > Admin Settings > Monitors**. At **Enable**, select either **Auto** or **Manual**. If you chose **Manual**, select any of the available profiles, except **Content, then Far, then Near** or **Content, then Far**.
- 2 To configure monitor 2, at **Monitor Profile**, enable one of the content profiles, such as **Content, then Far, then Near, Content, then Far**, or the **Content Only** profile.

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

Troubleshooting

To learn more about troubleshooting your system or device, refer to the following topics:

[General Troubleshooting](#)

[Placing a Test Call](#)

[Viewing System Details on the Local Interface](#)

[Audio Meters](#)

[View Call Statistics for an Active Point-to-Point Call With the Remote Control](#)

[View Call Statistics for an Active Multipoint Call with the Remote Control](#)

[System Reset](#)

[Factory Restore on the RealPresence Group System](#)

[Perform a Factory Restore on the Polycom EagleEye Director](#)

[Perform a Factory Restore on the EagleEye Producer](#)

[Before You Contact Polycom Technical Support](#)

[Contacting Technical Support](#)

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, might be paired to the room system.	Only one device can be paired at a time. To use the remote control, unpair the touch control device.
Picture is blank on the main monitor.	The room system is sleeping. This is normal after a period of inactivity.	Pick up the remote control to wake up the system.

Symptom	Problem	Solution
The monitor remains blank after you pick up the remote control.	The monitor is powered off.	Power on the monitor.
	The monitor's power cord is not plugged in.	Connect the monitor's power cord and the power on the monitor.
	The monitor is not correctly connected to the room system.	Verify that the monitor is connected correctly according to the set up sheet that you received with the system.
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 . Configure the other Monitor 2 settings. For details, refer to Configure Secondary Monitors for Content in a Multiple Touch Monitor Environment .
You lost the administration password for your system or device.	You cannot access the administration settings without a valid password.	Refer to the factory restore topics to learn how to reset your system.
The system is experiencing video issues during calls, such as packet loss.	You have not configured the Network Quality settings in the web interface.	For possible solutions, see Lost Packet Recovery and Dynamic Bandwidth Settings .

Placing a Test Call

Polycom support is available to assist you when you encounter difficulties. First though, If you are having problems making a call, try the troubleshooting tips and then call our test numbers. When you finish configuring the 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 RealPresence Group system at www.polycom.com/videtest.

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.

Viewing 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. You can also review information about calls, network usage, and performance on the various room system screens in 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 based on how your administrator configured the system. Therefore, this section might describe settings that you cannot access on your system. To find out more about these settings, please talk to your administrator.

Access the Information Screen

You can access system status screen in the local interface.

To access the Information screen:

» Go to  > **System Information** > **Information** to view the following system details.

Diagnostic Screen	Description
System Detail	Displays the following system information: <ul style="list-style-type: none"> • System Name • Model • Hardware Version • System Software • Serial Number • MAC Address • IP Address
Network	Displays the following network information: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Time in Last Call • Total Time in Calls • Total Number of Calls • System Up Time

Access the Status Screen

You can access system status screen in the local interface.

To access the Status screen:

- » Go to  > **System Information** > **Status**.

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for the out of a call status:

Status Screen	Description
Active Alerts	Displays the status of any device or service listed within the Status screens that has a current status indicator of red. Alerts are listed in the order they occurred. When a system device or service encounters a problem, you see an alert next to the Settings button on the menu.
Call Control	Displays the status of the Auto-Answer Point-to-Point Video and Meeting Password settings.
Audio	Displays the connection status of audio devices such as the microphones and SoundStation IP.
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	<ul style="list-style-type: none"> • 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.

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for in a call status:

- If the 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 in the Local Interface

You can access system diagnostics in the local interface.

To access information about your system diagnostics:

- » Select **Settings > System Information > Diagnostics**.

This screen includes the following system diagnostic details:

Diagnostic Screen	Description
Near End Loop	Tests the internal audio encoders and decoders, the external microphones and speakers, the internal video encoders and decoders, audio hardware, and the external microphones, speakers, cameras, and monitors. Monitor 1 displays the video and plays the audio that would be sent to the far site in a call. This test is not available when you are in a call.
Ping	Tests whether the system can establish contact with a far-site IP address that you specify. PING returns abbreviated Internet Control Message Protocol results. It returns H.323 information only if the far site is configured for H.323. It returns SIP information only if the far site is configured for SIP. If the test is successful, the 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 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. Meters function only when the associated input is enabled. Note: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the system. For details on configuring this setting, refer to Audio Meters .

Diagnostic Screen	Description
Camera Tracking	<p>Provides diagnostics specific to the EagleEye Director, if this camera is connected to the system.</p> <p>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.</p> <p>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.</p> <p>After you verify microphone functionality, calibrate the camera again.</p> <p>Video</p> <ul style="list-style-type: none"> • 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	<p>Displays the following information about each session connected to the system:</p> <ul style="list-style-type: none"> • 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	<p>Note: Do not use this setting unless your administrator tells you to do so.</p> <p>If a password is set, you must enter it to reset the system.</p> <p>Returns the system to its default settings. When you select this setting using the remote control, you can do the following:</p> <ul style="list-style-type: none"> • 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). <p>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.</p>

Audio Meters

Audio meters indicate the strength of the audio input and output of your microphones, far-site audio, and any device connected to the audio ports. To avoid or fix audio distortion, you can configure the Audio Meter setting in the local or web interface. The meters allow you to identify the left and right audio channels on the RealPresence Group system.

Set Audio Meter Levels

You can set audio meter levels for your system so that normal and loud audio peaks are within an acceptable audio range.

To set audio meter levels:

- 1 Do one of the following:
 - In the web interface, go to **Diagnostics > Audio and Video Tests > Audio Meter**.
 - In the local interface, go to **Settings > System Information > Diagnostics > Audio Meter**.
- 2 To test the audio, do one of the following:
 - To check the microphones for the near-site, speak into the microphones.
 - To check far-site audio, ask a participant at the far site to speak, or call a phone in the far-site room to hear it ring.
- 3 For normal speech and program material, set the audio signal levels so that you see peaks between +3 dB and +7 dB.

Occasional peaks of +12 dB to +16 dB with loud transient noises are acceptable. If you see +20 on the audio meter, the audio signal is 0 dBFS and the audio might be distorted. A meter reading of +20dB corresponds to 0dBFS in the room system audio. A signal at this level is likely clipping the audio system.

View Call Statistics for an Active Point-to-Point Call With the Remote Control

You might need to view call statistics on the local interface to do some troubleshooting for users. You can only view call statistics during a call. During a point-to-point call, you can view call statistics about a call participant or about an active stream. As a shortcut during a call, press the **Back** button on your remote control for two or more seconds to display the Call Statistics screen.

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**.

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 [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 > System Status** in the web interface. If a severe error occurs during startup, the system does not start up. Contact Polycom technical support.

System Reset

If the RealPresence Group 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 for the following:

- Current software version
- Remote control channel ID setting
- Directory entries
- CDR data and logs

Reset a System

You can reset a system in the web interface. For details about what is deleted from the system, see [System Reset](#).

To reset the room 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.

Factory Restore on the 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.

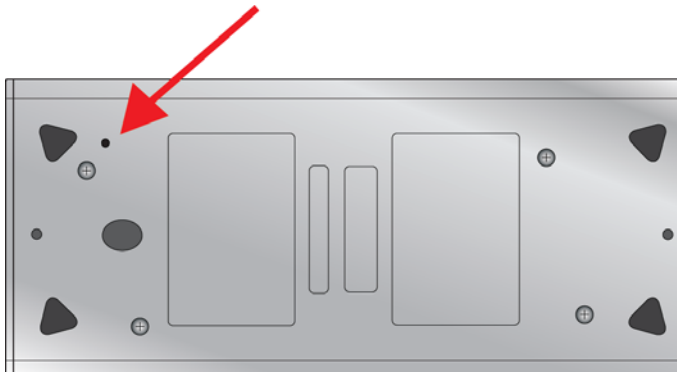
The following items are *not* saved:

- 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.

Perform a Factory Restore of a System

The restore button pinhole is on the bottom of the Polycom RealPresence Group 300, 310, and 500 systems, as shown in the following figure.



The restore button pinhole is on the front of the Polycom RealPresence Group 700 system, as shown in the following figure.



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.

Perform a Factory Restore to Install a Specific Software Version

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 perform a factory restore using a USB storage device to install a specific software version:

- 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 off 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 Data and Configuration System Files

You can remove sensitive data and configuration information from the room system for security purposes.

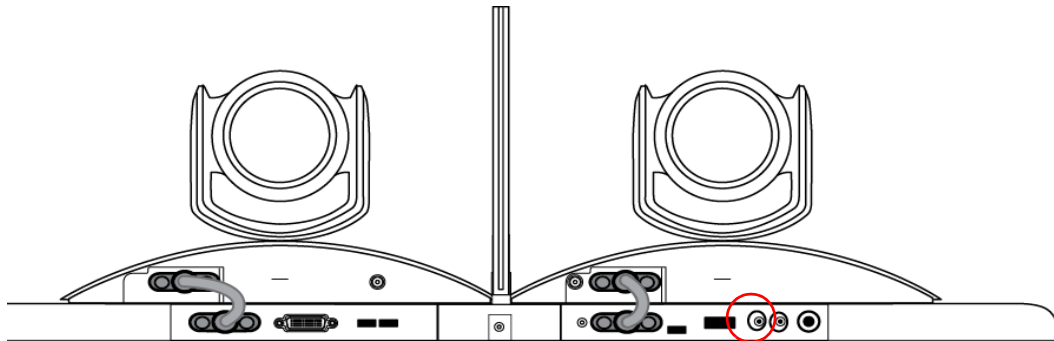
To perform a logical delete of system files:

- 1 Power off the RealPresence Group 300, 310, 500, or 700 system 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 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.



To reset the Polycom EagleEye Director using the restore button:

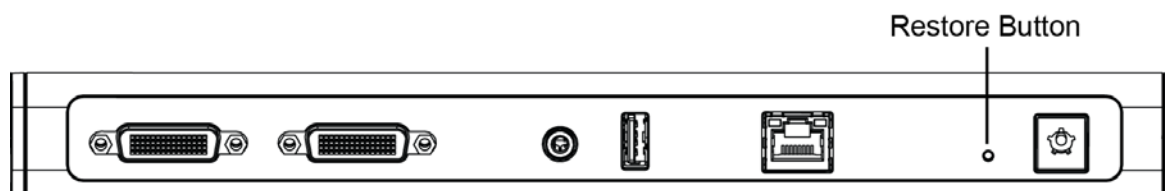
- 1 Press and hold the restore button on the back of the EagleEye Director for 2-3 seconds while the power light cycles.
When normal video content is displayed on the monitor instead of a blue screen, the EagleEye Director has been successfully restored.

- 2 Release the restore button.

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

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.



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 of the EagleEye Director](#).

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

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 room video 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 **Settings > System Information > Information > System Detail** or locate the number on the back of the system.

Locate the Software Version

You can view the software version on the local interface of the RealPresence Group system.

- » To locate the software version, go to **Settings > System Information > Information > System Detail**.

Locate Active Alert Messages

You can view the active alert messages on the local interface of the RealPresence Group system.

- » To locate the active alert messages, go to **Settings > System Information > Status > Active Alerts** for messages generated by your system.

Locate the IP Address and H.323 Extension Settings

You can view IP Address and H.323 extension settings on the local interface of the RealPresence Group system.

- » To locate the IP Address and H.323 Extension settings, go to **Settings > System Information > Information > Network**.

Locate the LAN Status

You can view the LAN status on the local interface of the RealPresence Group system.

- » To locate LAN status, go to **Settings > System Information > Status > LAN**.

Locate Diagnostics

You can view diagnostics on the local interface of the RealPresence Group system.

To locate Diagnostics, go to **Settings > System Information > Diagnostics**.

Contacting 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 screen.

Knowledge Base

For more troubleshooting information, you can search the Knowledge Base at support.polycom.com.

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 integrations. For additional information and details please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

System Panel Views

The following topics provide information on the system panel views:

[Polycom RealPresence Group 300 System](#)

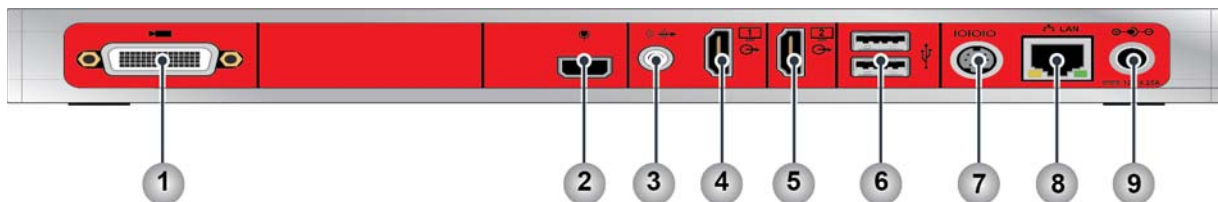
[Polycom RealPresence Group 310 System](#)

[Polycom RealPresence Group 500 System](#)

[Polycom RealPresence Group 700 System](#)

Polycom RealPresence Group 300 System

The following figure and table shows how the web interface settings relate to hardware input and outputs on the back of the RealPresence Group 300 system.

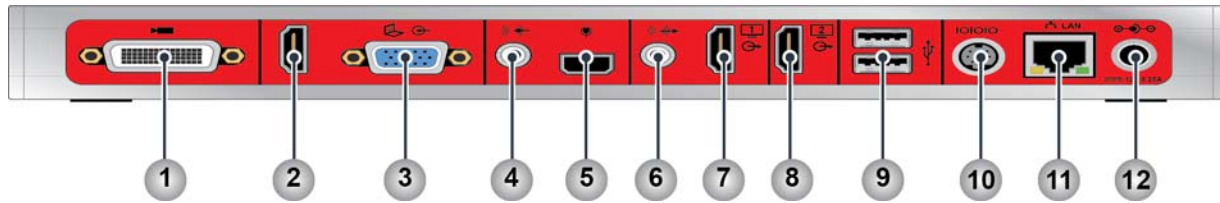


Ref. Number	Location in Web Interface: Admin Settings >	Input/Output	Supported Formats	Description
1	Audio/Video > Video Inputs > Input 1	Video Input	HDCI	Input for the camera
2	N/A	Microphone Input	Polycom Microphone	Audio input for up to two Polycom microphone arrays or a SoundStation IP 7000 speaker 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 +

Ref. Number	Location in Web Interface: Admin Settings >	Input/Output	Supported Formats	Description
4	Audio/Video > Monitors > Monitor 1	Video Output 1	<ul style="list-style-type: none"> HDMI version 1.3 with embedded audio DVI-D 	Output for Monitor 1
5	Audio/Video > Monitors > Monitor 2	Video Output 2	<ul style="list-style-type: none"> HDMI version 1.3 DVI-D 	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
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

The following figure and table shows how the web interface settings relate to hardware input and outputs on the back of the 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 version 1.3	Auxiliary video and audio input
3	Audio/Video > Video Inputs > Input 2	Video Input 2	VGA	Video input for Content

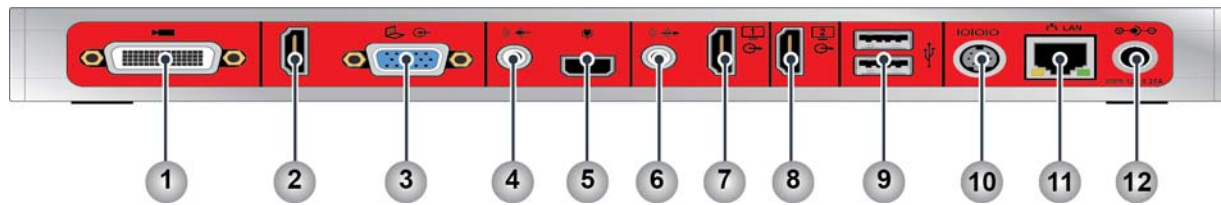
Note: Use either the HDMI or VGA video input, but not both.

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

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
7	Audio/Video > Monitors > Monitor 1	Video Output 1	<ul style="list-style-type: none"> HDMI version 1.3 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	<ul style="list-style-type: none"> HDMI version 1.3 DVI-D 	Output for Monitor 2; does not include 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

The following figure and table shows how the web interface settings relate to hardware input and outputs on the back of the 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 version 1.3	Auxiliary video and audio input
3	Audio/Video > Video Inputs > Input 2	Video Input 2	VGA	Video input for Content

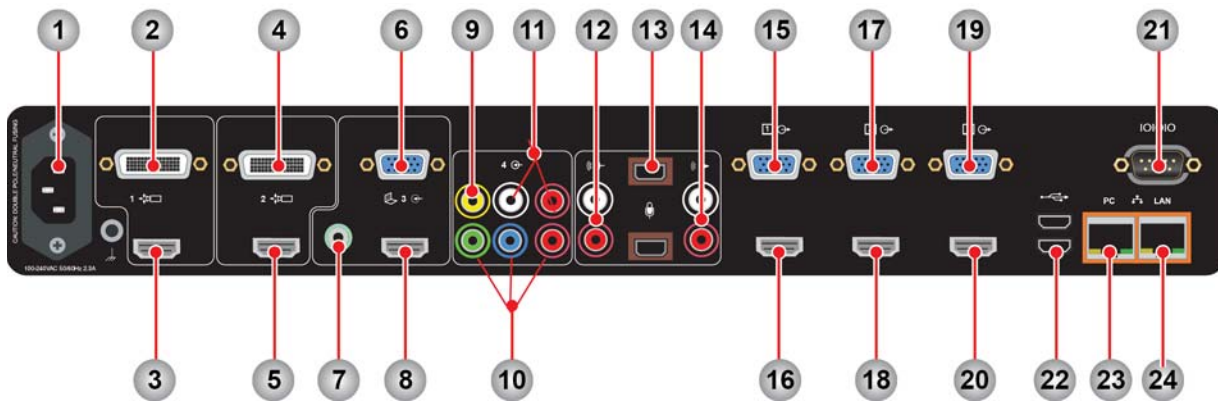
Note: Use either the HDMI or VGA video input, but not both.

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

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
7	Audio/Video > Monitors > Monitor 1	Video Output 1	<ul style="list-style-type: none"> HDMI version 1.3 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 version 1.3 DVI-D	Output for Monitor 2; does not include audio
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 700 System

This topic shows how the web interface settings relate to hardware input and outputs on the back of the 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 version 1.4	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 version 1.4	Input for Camera 2

Note: Use either the HDCI or HDMI for video inputs 1 and 2, but not both.

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 version 1.4	Video and audio input

Note: Use either the HDMI or VGA for video input 3, but not both.

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
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
16	Audio/Video > Monitors > Monitor 1	Video Output 1 Audio Output 1	HDMI version 1.3	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 version 1.3	Output for Monitor 2

Ref. Number	Location in Web Interface: Admin Settings >	Input/ Output	Supported Formats	Description
19	Audio/Video > Monitors > Monitor 3	Video Output 3	VGA	Output for Monitor 3
20	Audio/Video > Monitors > Monitor 3	Video Output 3 Audio Output 3	HDMI version 1.3	Video and audio output for Monitor 3. Audio output (near-end + far-end + content) when set for recording
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

Refer to the following topics about port usage information, which is useful when you configure your network equipment for video conferencing:

[Connections to RealPresence Group Systems](#)

[Connections from RealPresence Group Systems](#)

Connections to RealPresence Group Systems

The following table shows IP port usage 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 Device > 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 RealPresence Touch over HTTP	Yes	Admin Settings > Security > Global Security > Access > Enable Web Access - Disables HTTP and HTTPS port Admin Settings > Security > Global Security > Access > Restrict to HTTPS - Disables HTTP port	Admin Settings > Security > Global Security > Access > Web Access Port (http)

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 RealPresence Touch over HTTPS	Yes	Admin Settings > Security > Global Security > Access > Enable Web Access	No
1719	Static	UDP	H.225.0 RAS	No	Admin Settings > Network > IP Network > H.323 > Use Gatekeeper	No
1720	Static	TCP	H.225.0 Call Signaling	Yes	Admin Settings > Network > IP Network > H.323 > Enable IP H.323	No
5001	Static	TCP	People+Content™ IP client application for content sharing. Used by the RealPresence Group systems and the RealPresence Touch device	Yes	Admin Settings > Audio / Video > Video Input > General Camera Settings > Enable People+Content IP	No
5060	Static	TCP UDP	SIP (Protocol depends on Transport Protocol setting)	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP Admin Settings > Network > IP Network > SIP > Transport Protocol	No
5061	Static	TLS	SIP	Yes	Admin Settings > Network > IP Network > SIP > Enable SIP Admin Settings > Network > IP Network > SIP > Transport Protocol	No

Inbound 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 > 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

The following table shows IP port usage 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 for RealPresence Group system software installation and for the RealPresence Touch device	Yes	Uncheck "Register" checkbox during the setup wizard	No
123	Static	UDP	NTP	Yes	Admin Settings > General Settings > Date and Time > System Time > Time Server	No

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
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
443	Static	TLS	Microsoft Skype Address Book	No	Admin Settings > Servers > Directory Servers > Server Type	No
514	Static	UDP	SYSLOG	No	Diagnostics > System > System Log Settings > Enable Remote Logging Diagnostics > System > System Log Settings > Remote Log Server Transport Protocol = UDP	Yes - outgoing port can be specified in the Remote Log Server Address field.

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
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
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)

Outbound Port	Type	Protocol	Function	Configuration		
				On By Default? (Low Security Profile)	Enable/Disable?	Configurable Port Number
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
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 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?
Place a Call			
Contacts	Search Box	No value	Yes
Speed Dial			
Edit	Search Box	No value	Yes
Manual Dial			
	Entry box	No value	Yes
	Video Audio	Video	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
		Auto 128 256 384 512 768 1024 1472 1920 2048 3072 3840 4096 6144	Auto	Yes
		Auto H.323 SIP	Auto	Yes
General Settings				
System Settings				
Call Settings				
	Auto Answer Point to Point Video	Yes No Do Not Disturb	No	Yes
	Auto Answer Multipoint Video	Yes No Do Not Disturb	No	Yes
Recent Calls				
	Call Detail Report	Checkbox	Enabled	Yes
	Enable Recent Calls	Checkbox	Disabled	Yes
Home Screen Settings				
	Speed Dial	Checkbox	Disabled	Yes
	Calendar	Checkbox	Disabled	Yes
	Background	Choose image file	No file selected	Yes
	Startup Background	Choose image file	No file selected	Yes
	Kiosk Mode	Checkbox	Disabled	Yes
	Home Screen Icons	Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			
Enable Polycom Touch Device Note: Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
SmartPairing	Disabled	Disabled	Read-only
Serial Ports			
Mode			
RS-2 32 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

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Transport Protocol	Auto TLS TCP UDP	TLS	Yes
Dialing Preference			
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP H.323 SIP	IP H.323	Yes
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	SIP	Yes
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	H.323	Yes
Audio/Video			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Enabled	Read-only

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Video Inputs				
General Camera Settings				
	Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
	Enable People+Content IP	Checkbox	Disabled	Yes
	Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Audio				
	Polycom StereoSurround	Checkbox	Disabled	Yes
Security				
Global Security				
Security Profile				
	Security Profile	Maximum High Medium Low	Maximum	Yes
Authentication				
	Enable Active Directory External 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?
Allow Access to User Settings	Checkbox	Disabled	Yes
Restrict to HTTPS	Checkbox	Enabled	Read-only
Web access port (http) Note: You cannot select this setting if the Restrict to HTTPS setting is enabled.	16-bit integer	Grayed out (80)	Read-only
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
Maximum Number of Active Sessions	10,15,20,25,30,35,40,45,50	25	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
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
Login Credentials				
	Use Room Password for Remote Access	Checkbox	Enabled	Read-only
	Require User Login for System Access	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
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 Letters	Off,1,2,All	2	Yes
	Require Uppercase Letters	Off,1,2,All	2	Yes
	Require Numbers	Off,1,2,All	2	Yes
	Require Special Characters	Off,1,2,All	2	Yes
	Maximum Consecutive Repeated Characters	1-4	2	Yes
	Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
User (Room), Admin (Room)			
Minimum Length	8-16,32	9	Yes
Require Lowercase Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Maximum Consecutive Repeated Characters	1-4	2	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
Meeting			
Minimum Length	Off,1-20,32	Off	Yes
Require Lowercase Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Reject Previous Passwords	8-16	10	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes	
Maximum Consecutive Repeated Characters	1-4	2	Yes	
SNMP Note: SNMP passwords are applicable only when the system uses SNMP v3.				
Minimum Length	8-16,32	12	Yes	
Require Lowercase Letters	Off,1,2,All	1	Yes	
Require Uppercase Letters	Off,1,2,All	1	Yes	
Require Numbers	Off,1,2,All	1	Yes	
Require Special Characters	Off,1,2,All	1	Yes	
Reject Previous Passwords	8-16	10	Yes	
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes	
Maximum Consecutive Repeated Characters	1-4	2	Yes	
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only	
Security Banner				
Enable Security Banner	Checkbox	Enabled	Yes	
Banner Text	DoD Custom	DoD	Yes	

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Local System Banner Text		Unicode characters, 2048 bytes max	DoD Banner Text	Yes
Remote System Banner Text		Unicode characters, 2048 bytes max	DoD Banner Text	Yes
Certificates				
Certificate Options				
Always Validate Peer Certificates from Browser		Checkbox	Enabled	Yes
Always Validate Peer Certificates from Server		Checkbox	Enabled	Yes
Revocation				
Revocation Method		OCSP CRL	OCSP	Yes
Allow Incomplete Revocation Checks		Checkbox	Enabled	Yes
Servers				
Directory Servers				
Server Type		Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status		N/A	Disabled	Read only
SNMP				
Version1		Checkbox	Disabled	Yes
Version2c		Checkbox	Disabled	Yes
Version3		Checkbox	Enabled	Yes
Provisioning Service		Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service	Checkbox	Disabled	Yes
	Domain Name User Name Password Server Address		

Diagnostics Area	Maximum		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	TLS	Read only

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		Maximum		
		Range	Default Value	Configurable?
Place a Call				
Contacts		Search Box	No value	Yes
Speed Dial				
Edit		Search Box	No value	Yes
Manual Dial				
		Entry box	No value	Yes
		Video Audio	Video	Yes
		Auto 128 256 384 512 768 1024 1472 1920 2048 3072 3840 4096 6144	Auto	Yes
		Auto H.323 SIP	Auto	Yes
General Settings				
System Settings				
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

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Disabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	Yes
Background	Choose image file	No file selected	Yes
Startup Background	Choose image file	No file selected	Yes
Kiosk Mode	Checkbox	Disabled	Yes
Home Screen Icons	Checkbox	Disabled	Yes
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			
Enable Polycom Touch Device Note: Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
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

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Login Mode	None, Admin password only, Username/Password	Admin password only	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto TLS TCP UDP	TLS	Yes
Dialing Preference			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	AVC Only	Yes
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP H.323 SIP	IP H.323	Yes
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	SIP	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)	IP H.323 SIP	H.323	Yes
Audio/Video			
Sleep			
Enable Mic Mute in Sleep Mode	Checkbox	Disabled	Yes
Video Inputs			
General Camera Settings			
Allow Other Participants In a Call to Control Your Camera	Checkbox	Disabled	Yes
Enable People+Content IP	Checkbox	Disabled	Yes
Enable Camera Preset Snapshot Icons	Checkbox	Disabled	Yes
Audio			
Polycom StereoSurround	Checkbox	Disabled	Yes
Security			
Global Security			
Security Profile			
Security Profile	Maximum High Medium Low	High	Yes
Authentication			
Enable Active Directory External Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
	Enable Web Access	Checkbox	Enabled	Yes
	Allow Access to User Settings	Checkbox	Disabled	Yes
	Restrict to HTTPS	Checkbox	Enabled	Read-only
	Web access port (http) Note: You cannot select this setting if the Restrict to HTTPS setting is enabled.	16-bit integer	Grayed out (80)	Read-only
	Enable Telnet Access	Checkbox	Disabled	Read-only
	Enable SSH Access	Checkbox	Enabled	Yes
	Enable SNMP Access	Checkbox	Disabled	Yes
	Lock Port after Failed Logins	Off,2-10	Off	Yes
	Port Lock Duration	1,2,3,5,10,20,30 minutes, 1,2,4,8 hours	1 minute	Yes
	Reset Port Lock Counter After	Off,[1..24] hours	Off	Yes
	Enable Whitelist	Checkbox	Disabled	Yes
	Idle Session Timeout in Minutes	1,3,5,10,15,20,30,45,60,120,240,480	10	Yes
	Maximum Number of Active Sessions	10,15,20,25,30,35,40,45,50	25	Yes
Encryption				
	Require AES Encryption for Calls	Off When Available Required for Video Calls Only Required for All Video Calls	Required for Video Calls Only	Yes
	Require FIPS 140 Cryptography	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
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 Failed Logins	Off,[1..24] hours	Off	Yes
	Lock User Account After Failed Logins	2-10	3	Yes
	User Account Lock Duration	1,3,5,10,15,20,30 minutes, 1,2,4,8 hours	1 minute	Yes
	Reset User Account Lock Counter After Failed Logins	Off,[1..24] hours	Off	Yes
Login Credentials				
	Use Room Password for Remote Access	Checkbox	Enabled	Yes
	Require User Login for System Access	Checkbox	Enabled	Yes
Password Requirements				
Admin (Room, Remote), User (Room, Remote)				
	Reject Previous Passwords	Off,1-16	10	Yes
	Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes
	Maximum Password Age in Days	Off,30,60,90,100, 110,120,130,140, 150,160,170,180	90	Yes
	Minimum Changed Characters	1-4	4	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Password Expiration Warning	1-7	4	Yes
Remote Access (Admin Remote, User Remote)			
Minimum Length	1-16,32	6	Yes
Require Lowercase Letters	Off, 1,2,All	Off	Yes
Require Uppercase Letters	Off, 1,2,All	Off	Yes
Require Numbers	Off, 1,2,All	Off	Yes
Require Special Characters	Off, 1,2,All	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
User (Room), Admin (Room)			
Minimum Length	8-16,32	6	Yes
Require Lowercase Letters	Off, 1,2,All	Off	Yes
Require Uppercase Letters	Off, 1,2,All	Off	Yes
Require Numbers	Off, 1,2,All	Off	Yes
Require Special Characters	Off, 1,2,All	Off	Yes
Maximum Consecutive Repeated Characters	Off, 1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Read-only
Meeting			
Minimum Length	Off, 1-20,32	Off	Yes
Require Lowercase Letters	Off, 1,2,All	Off	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Reject Previous Passwords	Off,1-16	10	Yes
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
SNMP			
Note: SNMP passwords are applicable only when the system uses SNMP v3.			
Minimum Length	8-16,32	8	Yes
Require Lowercase Letters	Off,1,2,All	1	Yes
Require Uppercase Letters	Off,1,2,All	1	Yes
Require Numbers	Off,1,2,All	1	Yes
Require Special Characters	Off,1,2,All	1	Yes
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	Maximum		
	Range	Default Value	Configurable?
Certificates			
Certificate Options			
Always Validate Peer Certificates from Browser	Checkbox	Enabled	Yes
Always Validate Peer Certificates from Server	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			
Server Type	Off Microsoft LDAP Polycom GDS	Off	Yes
Registration Status	N/A	Disabled	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Provisioning Service	Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service	Checkbox	Disabled	Yes
	Domain Name User Name Password Server Address		

Diagnostics Area	High		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Yes

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		Maximum		
		Range	Default Value	Configurable?
Place a Call				
Contacts		Search Box	No value	Yes
Speed Dial				
Edit		Search Box	No value	Yes
Manual Dial				
		Entry box	No value	Yes
		Video Audio	Video	Yes
		Auto 128 256 384 512 768 1024 1472 1920 2048 3072 3840 4096 6144	Auto	Yes
		Auto H.323 SIP	Auto	Yes
General Settings				
System Settings				
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

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Enabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar	Checkbox	Disabled	Yes
Background	Choose image file	No file selected	Yes
Startup Background	Choose image file	No file selected	Yes
Kiosk Mode	Checkbox	Disabled	Yes
Home Screen Icons	Checkbox	Disabled	Yes
Address Bar	None IP Address SIP Address H.323 Extension Pairing Code	None	Yes, for both the left and right elements
RealPresence Touch Background	Choose image file	No file selected	Yes
Skype Mode	Checkbox	Disabled	Yes
Pairing			
Enable Polycom Touch Device Note: Disabling this setting closes the SSH port.	Checkbox	Disabled	Yes
SmartPairing Mode	Disabled Automatic Manual	Disabled	Yes
Serial Ports			
Mode			
RS-232 Mode Note: Some RealPresence Group systems support only a subset of listed modes.	Off Control Camera Control Closed Caption Pass Thru	Off	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Login Mode	Range: None, Admin password only, Username/Password	Admin password only	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	Auto TLS TCP UDP	TLS	Yes
Dialing Preference			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Dialing Options			
Scalable Video Coding Preference (H.264)	SVC then AVC AVC Only	SVC then AVC	Yes
Enable H.239	Checkbox	Disabled	Yes
Enable Audio-Only Calls	Checkbox	Disabled	Yes
TIP	Checkbox	Disabled	Yes
Call Type Order	Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video	Yes
Video Dialing Order	IP H.323 SIP	IP H.323	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)		IP H.323 SIP	SIP	Yes
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)		IP H.323 SIP	H.323	Yes
Audio/Video				
Video Inputs				
Sleep				
Enable Mic Mute in Sleep Mode		Checkbox	Disabled	Yes
General Camera Settings				
Allow Other Participants In a Call to Control Your Camera		Checkbox	Disabled	Yes
Enable People+Content IP		Checkbox	Enabled	Yes
Enable Camera Preset Snapshot Icons		Checkbox	Enabled	Yes
Audio				
Polycom StereoSurround		Checkbox	Disabled	Yes
Security				
Global Security				
Security Profile				
Security Profile		Maximum High Medium Low	Medium	Yes
Authentication				
Enable Active Directory External Authentication		Checkbox	Disabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
	Access			
	Enable Network Intrusion Detection System (NIDS)	Checkbox	Enabled	Yes
	Enable Web Access	Checkbox	Enabled	Yes
	Allow Access to User Settings	Checkbox	Disabled	Yes
	Restrict to HTTPS	Checkbox	Enabled	Yes
	Web access port (http) Note: You cannot select this setting if the Restrict to HTTPS setting is enabled.	16-bit integer	Grayed out (80)	Read only
	Enable Telnet Access	Checkbox	Disabled	Yes
	Enable SSH Access	Checkbox	Enabled	Yes
	Enable SNMP Access	Checkbox	Disabled	Yes
	Lock Port after Failed Logins	Off,2-10	Off	Yes
	Port Lock Duration	1,2,3,5,10,20,30 minutes, 1,2,4,8 hours	1 minute	Yes
	Reset Port Lock Counter After	Off,[1..24] hours	Off	Yes
	Enable Whitelist	Checkbox	Disabled	Yes
	Idle Session Timeout in Minutes	1,3,5,10,15,20,30,45,60,120,240,480	10,15,20,25,30,35,40,45,50	Yes
	Maximum Number of Active Sessions	10,15,20,25,30,35,40,45,50	25	Yes

Admin Settings Area		Maximum		
		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	Disabled	Yes
	Require User Login for System Access	Checkbox	Disabled	Yes
Password Requirements				
Admin (Room, Remote), User (Room, Remote)				
	Reject Previous Passwords	Off,1-16	Off	Yes
	Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes

Admin Settings Area	Maximum		
	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 Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
User (Room), Admin (Room)			
Minimum Length	8-16,32	8	Yes
Require Lowercase Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Meeting			
Minimum Length	Off,1-20,32	Off	Yes
Require Lowercase Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Reject Previous Passwords	Off,1-16	Off	Yes
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
SNMP			
Note: SNMP passwords are applicable only when the system uses SNMP v3.			
Minimum Length	8-16,32	3	Yes
Require Lowercase Letters	Off,1,2,All	Off	Yes
Require Uppercase Letters	Off,1,2,All	Off	Yes
Require Numbers	Off,1,2,All	Off	Yes
Require Special Characters	Off,1,2,All	Off	Yes
Reject Previous Passwords	Off,1-16	Off	Yes
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	Configurable?
Certificates				
Certificate Options				
Always Validate Peer Certificates from Browser		Checkbox	Disabled	Yes
Always Validate Peer Certificates from Server		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
Servers				
Directory Servers				
Server Type		Off Microsoft LDAP Polycom GDS	Off	Yes

Admin Settings Area	Maximum		
	Range	Default Value	Configurable?
Registration Status	N/A	Disabled	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service	Checkbox	Disabled	Yes
	Recording Service Domain Name User Name Password Server Address		

Diagnostics Area	Medium		
	Range	Default Value	Configurable?
System			
System Log Settings			
Enable Remote Logging	Checkbox	Disabled	Yes
Remote Log Server Transport Protocol	UDP TCP TLS	UDP	Read only

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		Maximum		
		Range	Default Value	
Place a Call				
Contacts		Search Box	No value	
Speed Dial				
Edit		Search Box	No value	
Manual Dial				
		Entry box	No value	
		Video Audio	Video	
		Auto 128 256 384 512 768 1024 1472 1920 2048 3072 3840 4096 6144	Auto	
		Auto H.323 SIP	Auto	
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

Admin Settings Area		Maximum	
		Range	Default Value
Recent Calls			
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Enabled	Yes
Home Screen Settings			
Speed Dial	Checkbox	Disabled	Yes
Calendar		Checkbox	Disabled
Background		Choose image file	No file selected
Startup Background		Choose image file	No file selected
Kiosk Mode		Checkbox	Disabled
Home Screen Icons		Checkbox	Disabled
Address Bar		None IP Address SIP Address H.323 Extension Pairing Code	None
RealPresence Touch Background		Image file not selected	Yes
Skype Mode		Checkbox	Disabled
Pairing			
Enable Polycom Touch Device Note: Disabling this setting closes the SSH port.		Checkbox	Disabled
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		Maximum	
		Range	Default Value
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
Dialing Options			
Scalable Video Coding Preference (H.264)		SVC then AVC AVC Only	SVC then AVC
Enable H.239		Checkbox	Disabled
Enable Audio-Only Calls		Checkbox	Disabled
TIP		Checkbox	Disabled
Call Type Order		Video Video Then Phone Phone Then Video VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)	Video
Video Dialing Order		IP H.323 SIP	IP H.323
Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)		IP H.323 SIP	SIP
Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)		IP H.323 SIP	H.323
Audio/Video			
Video Inputs			

Admin Settings Area		Maximum		
		Range	Default Value	
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
Audio				
	Polycom StereoSurround	Checkbox		Disabled
Security				
Global Security				
Security Profile				
	Security Profile	Maximum High Medium Low	Low	Yes
Authentication				
	Enable Active Directory External Authentication	Checkbox	Disabled	Yes
Access				
	Enable Network Intrusion Detection System (NIDS)	Checkbox	Disabled	Yes
	Enable Web Access	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	
Allow 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	
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	

Admin Settings Area		Maximum		
		Range	Default Value	
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	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	
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	Disabled	Yes	
Require User Login for System Access	Checkbox	Disabled	Yes	

Admin Settings Area		Maximum		
		Range	Default Value	
Password Requirements				
Admin (Room, Remote), User (Room, Remote)				
	Reject Previous Passwords	Off,1-16	Off	Yes
	Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes
	Maximum Password Age in Days	Off,30,60,90,100,110,120,130,140,150,160,170,180	Off	Yes
	Minimum Changed Characters	Off,1-4,All	Off	Yes
	Password Expiration Warning	Off,1-7	Off	Yes
Remote Access (Admin Remote, User Remote)				
	Minimum Length	Off,1-16,32	Off	Yes
	Require Lowercase Letters	Off,1,2,All	Off	Yes
	Require Uppercase Letters	Off,1,2,All	Off	Yes
	Require Numbers	Off,1,2,All	Off	Yes
	Require Special Characters	Off,1,2,All	Off	Yes
	Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
	Can contain ID or Its Reverse Form	Checkbox	Enabled	Yes

Admin Settings Area		Maximum		
		Range	Default Value	
User (Room), Admin (Room)				
Minimum Length	Off,1-16,32	Off	Yes	
Require Lowercase Letters	Off,1,2,All	Off	Yes	
Require Uppercase Letters	Off,1,2,All	Off	Yes	
Require Numbers	Off,1,2,All	Off	Yes	
Require Special Characters	Off,1,2,All	Off	Yes	
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes	
Can contain ID or Its Reverse Form	Checkbox	Enabled	Yes	
Meeting				
Minimum Length	Off,1-20,32	Off	Yes	
Require Lowercase Letters	Off,1,2,All	Off	Yes	
Require Uppercase Letters	Off,1,2,All	Off	Yes	
Require Numbers	Off,1,2,All	Off	Yes	
Require Special Characters	Off,1,2,All	Off	Yes	
Reject Previous Passwords	Off,1-16	Off	Yes	

Admin Settings Area		Maximum		
		Range	Default Value	
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes	
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes	
SNMP				
Note: SNMP passwords are applicable only when the system uses SNMP v3.				
Minimum Length	8-16,32	8	Yes	
Require Lowercase Letters	Off,1,2,All	Off	Yes	
Require Uppercase Letters	Off,1,2,All	Off	Yes	
Require Numbers	Off,1,2,All	Off	Yes	
Require Special Characters	Off,1,2,All	Off	Yes	
Reject Previous Passwords	Off,1-16	Off	Yes	
Minimum Password Age in Days	Off,1,5,10,15,20,30	Off	Yes	
Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes	
Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes	

Admin Settings Area		Maximum		
		Range	Default Value	
Certificates				
Certificate Options				
Always Validate Peer Certificates from Browser	Checkbox	Disabled	Yes	
Always Validate Peer Certificates from Server	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	
Servers				
Directory Servers				
Server Type		Off Microsoft LDAP Polycom GDS	Off	

Admin Settings Area		Maximum	
		Range	Default Value
Registration Status		N/A	Read only
SNMP			
Version1	Checkbox	Disabled	Yes
Version2c	Checkbox	Disabled	Yes
Version3	Checkbox	Enabled	Yes
Provisioning Service	Checkbox	Checkbox	Disabled
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes
Recording Service			
Enable Recording Service		Checkbox - Disabled	Yes
		Recording Service Domain Name User Name Password Server Address	

Diagnostics Area		Low	
		Range	Default Value
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:

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.

Number of Sites in Call	Max Speed for Each Site	Max Speed for Each Site (ICE Enabled, Skype for Business 2015)	Max Speed for Each Site (CCCP Skype for Business 2015 with A/V MCU)
3	3072 kbps	1024 kbps	664 kbps
4	2048 kbps	512 kbps	664 kbps
5	1536 kbps	384 kbps	664 kbps
6	1152 kbps	256 kbps	664 kbps

Number of Sites in Call	Max Speed for Each Site	Max Speed for Each Site (ICE Enabled, Skype for Business 2015)	Max Speed for Each Site (CCCP Skype for Business 2015 with A/V MCU)
7 (RealPresence Group 700 only)	1024 kbps	128 kbps	664 kbps
8 (RealPresence Group 700 only)	832 kbps	128 kbps	664 kbps

These values do not apply when the Microsoft Skype Interoperability option is enabled, whether it is in a Skype for Business 2015 environment. When this option key is enabled, all calls are CCCP calls and are capped at 1920 kbps due to ICE restrictions.

The values in the Max Speed for Each Site (ICE Enabled, Skype for Business 2015) column are applicable only when both of the following criteria are met:

- The Skype Interoperability option key is disabled, so that calls are negotiated with H.263 using Skype for Business 2015 clients.
- The ICE calls go across the firewall boundary.

High-Profile Call Speeds and Resolutions

This section includes the H.264 high-profile resolutions and frame rates sent in calls between two RealPresence Group systems. Resolutions and frame rates are based on both the call speed and the **Optimized for** setting of your Camera input.

Due to the complexities of the systems and their capabilities, it is not possible to include tables of the resolutions and frame rates for calls between a RealPresence Group system and a different type of endpoint or a multipoint resource. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

The values for sharpness and motion are the same from 2 MB to 6 MB for systems that support higher call speeds. The difference between NTSC and PAL cameras is how frame rates are calculated:

- NTSC 60 fps equals PAL 50 fps
- NTSC 30 fps equals PAL 25 fps

The following table shows the resolutions for People video on systems with NTSC cameras in H.264 high-profile calls. The actual resolutions and frame rates might vary and depend upon the call types and call scenarios in your environment.

Call Speeds and Resolutions in High-Profile Calls

Call Speed (kbps)	Motion/ Sharpness	Camera Source			
		HD (1280x720x60)		HD (1920x1080x60)	
		Resolution	Max Frame Rate (fps)	Resolution	Max Frame Rate (fps)
<160	Motion	512x288	60	512x288	60
160-511	Motion	640x368	60	640x368	60
512-831	Motion	848x480	60	848x480	60

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)
832-895	Motion	1024x576	60	720x832	60
896-1727	Motion	1280x720	60	1280x720	60
>=1728	Motion	1280x720	60	1920x1080	60
<128	Sharpness	640x368	30	640x368	30
128-511	Sharpness	1024x576	30	1024x576	30
512-1023	Sharpness	1280x720	30	1280x720	30
>=1024	Sharpness	1280x720	30	1920x1080	30

The following table shows the resolutions for People video on systems with NTSC EagleEye Acoustic cameras in H.264 high-profile calls.

Call Speeds and Resolutions in High-Profile Calls for EagleEye Acoustic

		Camera Source	
		HD (1920x1080x30)	
Call Speed (kbps)	Motion/ Sharpness	Resolution	Max Frame Rate (fps)
<128	Motion/Sharpness	640x368	30
128-511	Motion/Sharpness	1024x576	30
512-1023	Motion/Sharpness	1280x720	30
>=1024	Motion/Sharpness	1920x1080	30

Multipoint Resolutions for High Definition Video

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. Note that changing from discussion to speaker does not alter the transmit of 960x540 from an endpoint and the receive of 1080p from the endpoints.

RealPresence 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 support one endpoint as a host system and up to 7 other endpoints in an 8-way multipoint conference.

Number of Endpoints in the Video Conference	Maximum Transmitting Resolutions	Maximum Receiving Resolutions
2-4 endpoints	1080p, 30fps	960x540p, 30fps
5-8 endpoints	720p, 30fps	640x368p, 30fps

Resolution and Frame Rates for Content Video

The high frame rates with high resolution apply only to point-to-point calls above 832 kbps. In addition, you must set **Optimized for** value of your Camera input to **Sharpness**. Low frame rates apply if your call does not meet these requirements.

For multipoint calls, the maximum resolution and frame rate for content is 720p @ 30 fps.

Resolution	Encode Resolution	Sharpness	Motion
800 x 600	800 x 600	30	60
1024 x 768	1024 x 768	30	60
1280 x 720	1280 x 720	30	60
1280 x 768	1280 x 720	30	60
1280 x 1024	1280 x 1024	30	60
1600 x 1200	1280 x 1024	30	60
1680 x 1050	1280 x 720	30	60
1920 x 1080	1920 x 1080	30	60*

*Available only when the **Quality Preference** setting on your RealPresence Group 310 or RealPresence Group 500 system is set to **Content** in **Admin Settings > Network > IP Network > Network Quality**.