Contents

Before You Begin..............................................................................................................................12
  Getting Help........................................................................................................................................ 12
  Polycom and Partner Resources........................................................................................................ 12
  The Polycom Community.................................................................................................................... 12

Getting Started.................................................................................................................................. 13
  High Definition Video Conferencing.................................................................................................. 13
  User Interface Customization.............................................................................................................. 13
  Security Setting Management............................................................................................................ 14
  Call Setting Configuration................................................................................................................... 14
  Powering the System On and Off........................................................................................................ 15
    Power On the RealPresence Centro System....................................................................................... 15
    Automatic Wake With Motion Sensors............................................................................................ 15
  Navigating the System........................................................................................................................ 15
    Access the System Web Interface................................................................................................... 15
    Changing a Password....................................................................................................................... 16
    Search the Web Interface................................................................................................................ 16

Setting Up System Hardware............................................................................................................. 17
  Positioning the RealPresence Centro System.................................................................................... 17

Running the Setup Wizard................................................................................................................. 18
  Run the Setup Wizard Locally............................................................................................................... 18
  Run the Setup Wizard from a Remote Location................................................................................... 18

Configuring General System Settings............................................................................................. 19
  Name the System............................................................................................................................... 19
  Enter Contact Information.................................................................................................................. 19
  Set the Location............................................................................................................................... 20
  Set the Language............................................................................................................................... 21
  Set the Date and Time......................................................................................................................... 21
  Displaying Participant Names Continuously in a Call......................................................................... 22
    Configure Participant Name Display............................................................................................... 22

Using a Provisioning Service.............................................................................................................. 24
  Enable a Provisioning Service............................................................................................................ 24
<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a Provisioning Service</td>
<td>25</td>
</tr>
<tr>
<td>Disable a Provisioning Service</td>
<td>26</td>
</tr>
<tr>
<td>ZTP Web Service Solution</td>
<td>26</td>
</tr>
<tr>
<td>Certificates and Security Profiles within a Provisioned System</td>
<td>26</td>
</tr>
<tr>
<td>Set Up Multitiered Directory Navigation</td>
<td>27</td>
</tr>
<tr>
<td>Activating System Options</td>
<td>28</td>
</tr>
<tr>
<td>System Software Options</td>
<td>28</td>
</tr>
<tr>
<td>View System Software Options</td>
<td>28</td>
</tr>
<tr>
<td>Obtain Software or System Option Keys</td>
<td>28</td>
</tr>
<tr>
<td>Create a Single Key File to Update Multiple Systems</td>
<td>29</td>
</tr>
<tr>
<td>Key File Formats</td>
<td>29</td>
</tr>
<tr>
<td>Activate System Options</td>
<td>30</td>
</tr>
<tr>
<td>Registering with a Calendaring Service</td>
<td>31</td>
</tr>
<tr>
<td>Enable the Calendaring Service</td>
<td>31</td>
</tr>
<tr>
<td>Join Scheduled Meetings</td>
<td>33</td>
</tr>
<tr>
<td>Configuring Network Settings</td>
<td>34</td>
</tr>
<tr>
<td>Connecting to a LAN</td>
<td>34</td>
</tr>
<tr>
<td>Configure LAN Properties</td>
<td>34</td>
</tr>
<tr>
<td>Configure IP Address (IPv4) Settings</td>
<td>37</td>
</tr>
<tr>
<td>Configure IP Address (IPv6) Settings</td>
<td>38</td>
</tr>
<tr>
<td>Configure DNS Server Settings</td>
<td>39</td>
</tr>
<tr>
<td>LLDP and LLDP-MED Support</td>
<td>39</td>
</tr>
<tr>
<td>LLMP-MED Information Discovery</td>
<td>40</td>
</tr>
<tr>
<td>Behavior When LLDP is Enabled</td>
<td>40</td>
</tr>
<tr>
<td>Enable LLDP Using a USB Storage Device</td>
<td>40</td>
</tr>
<tr>
<td>Enable LLDP in the Web Interface</td>
<td>41</td>
</tr>
<tr>
<td>IP Network Settings</td>
<td>41</td>
</tr>
<tr>
<td>Configure H.323 Settings</td>
<td>41</td>
</tr>
<tr>
<td>Configure the System to Use a Gatekeeper</td>
<td>42</td>
</tr>
<tr>
<td>SIP Settings</td>
<td>43</td>
</tr>
<tr>
<td>RTV and Skype-Hosted Conference Support</td>
<td>46</td>
</tr>
<tr>
<td>Multilevel Precedence and Preemption (MLPP)</td>
<td>46</td>
</tr>
<tr>
<td>Define MLPP Network Domains</td>
<td>47</td>
</tr>
<tr>
<td>Add an MLPP Network Domain</td>
<td>47</td>
</tr>
<tr>
<td>Alternative Network Address Type (ANAT)</td>
<td>48</td>
</tr>
<tr>
<td>Multipoint Conference On a RealPresence Collaboration Server</td>
<td>48</td>
</tr>
<tr>
<td>Enable Call Escalation of Point-to-Point Calls</td>
<td>48</td>
</tr>
</tbody>
</table>
Securing the System........................................................................................................... 56
Configure Security Profiles................................................................................................. 56
  Maximum Security Profile Requires Default Value Changes........................................... 57
Managing System Access.................................................................................................... 57
  Enable External Authentication....................................................................................... 58
  Configure Local Access................................................................................................. 59
  Configure Remote Access.............................................................................................. 60
  Local Accounts................................................................................................................ 61
Detecting Intrusions........................................................................................................... 65
View Connections to Your System in a Sessions List....................................................... 66
Secure API Access............................................................................................................. 66
  Enable Secure API Access............................................................................................ 66
  Disable Secure API Access......................................................................................... 67
  Access the API with SSH.............................................................................................. 67
Port Lockout...................................................................................................................... 67
  Configure Port Lockout Settings.................................................................................. 68
Whitelisting......................................................................................................................... 69
  Enable a Whitelist......................................................................................................... 69
  Add IP Addresses to a Whitelist................................................................................... 69
  IPv4 Address Formats.................................................................................................. 70
  IPv6 Address Formats.................................................................................................. 70
Encryption......................................................................................................................... 70
  Configure Encryption.................................................................................................... 70
  Configuring Encryption Settings for SVC Calls.......................................................... 71
  Set the Transport Protocol for SVC Calls................................................................... 71
  Set Up AES Encryption for SVC Calls.......................................................................... 72
  Verify H.323 Media Encryption................................................................................... 72
Configuring Call Settings........................................................................................................ 89
Configure Call Settings........................................................................................................ 89
Setting Call Preferences for SVC.......................................................................................... 91
 Configure SVC Dialing Options.......................................................................................... 91
 Enable SVC Preference (H.264) for Calls............................................................................ 92
 Enable Automatic Answering of SVC Point-to-Point Calls................................................. 93
 Set Preferred Call Speeds.................................................................................................... 93
 Configure the Recent Calls List........................................................................................ 94
 Set Call Answering Mode..................................................................................................... 94
 Set the Maximum Call Length............................................................................................ 95
 Set a Multipoint Viewing Mode......................................................................................... 95
 Enable Flashing Incoming Call Alerts............................................................................... 96
 Turn Off Flashing Alerts..................................................................................................... 96
 Displaying Participant Names Continuously in a Call....................................................... 96
 Configure Participant Name Display............................................................................... 96
 Configure System Display Name During Call...................................................................... 97

Registering with a Directory.................................................................................................98
Enable H.323....................................................................................................................... 98
Configure the Polycom GDS.............................................................................................. 99
Configure the LDAP Directory Server.............................................................................. 99
## Configuring a Camera or Camera Control System

- Integrating RealPresence Group Series with Polycom EagleEye Cube HDCI .................................................... 120
- Position the EagleEye Cube HDCI Camera ........................................................................................................ 121
- LED Indicators .................................................................................................................................................... 121
- Configure Camera Settings ................................................................................................................................ 121
- Camera Tracking .................................................................................................................................................. 121
- Participant Count CDR Details .......................................................................................................................... 123
- EagleEye Cube HDCI Camera Software Updates ............................................................................................... 123
- Factory Restore the EagleEye Cube HDCI ........................................................................................................... 124

Setting Up a Polycom EagleEye IV Camera ........................................................................................................ 124
- EagleEye IV Camera Orientation .......................................................................................................................... 124
- Replace the EagleEye IV Camera ........................................................................................................................ 125

Improve Camera Tracking Performance ................................................................................................................ 125

Polycom EagleEye Director II Camera System ..................................................................................................... 125
- Position the EagleEye Director II Camera System ............................................................................................... 127
- Indicator Lights .................................................................................................................................................... 129
- View System Status for EagleEye Director II Camera System ........................................................................... 130
- EagleEye Director II Camera System Diagnostics ............................................................................................ 131
- Perform a Factory Restore .................................................................................................................................. 132

Setting Up a Polycom EagleEye Producer System ............................................................................................... 133
- Calibration ............................................................................................................................................................ 133
- Camera Tracking .................................................................................................................................................. 134

Set Up the Polycom EagleEye Director ................................................................................................................ 138
- Indicator Lights .................................................................................................................................................... 138
- Adjust the Room View ......................................................................................................................................... 139
- Camera Tracking in the Local Interface .............................................................................................................. 139
- Camera Presets .................................................................................................................................................... 140
- Transfer EagleEye Director Logs ......................................................................................................................... 141
- EagleEye Director Software Updates .................................................................................................................. 141
- Perform a Factory Restore for the EagleEye Director .......................................................................................... 141
- Troubleshooting EagleEye Director Camera Calibration .................................................................................... 142
- Troubleshooting EagleEye Director Camera Tracking ....................................................................................... 142

Setting Up Polycom EagleEye Acoustic Camera ................................................................................................. 142

## Configuring Remote Control Behavior

- Configure Remote Control Behavior .................................................................................................................. 144
- Programming the Remote Control ....................................................................................................................... 145
- Set the Remote Control Channel ID ................................................................................................................... 145
- Set the Remote Control Channel ID for a Specific System ............................................................................... 146
- Confirm the Channel ID ...................................................................................................................................... 146
Setting Up a Polycom RealPresence Touch Device

Positioning the RealPresence Touch Device
Run the RealPresence Touch Device Setup Wizard (OOB)
Power Off the RealPresence Touch
Wake the RealPresence Touch
Enable the RealPresence Touch Device
Pairing the Device
Pairing States
Pair For the First Time
Pair to a Previously Paired System
Unpair a RealPresence Touch
Remove a System from the Paired System List
Managing the RealPresence Touch Device
Open a Remote Management Window
Pair Using RealPresence Touch Web Interface
Unpair Using the RealPresence Touch Web Interface
Change the RealPresence Touch User Name and Password
Configure Network Settings
Enable Recent Calls and Speed Dial
Customize the RealPresence Touch Screens
Choose the Home Screen Icons
Choose the Place a Call Screen Icons
Change the Background Image
Setting Up and Configuring Directory Servers for the RealPresence Touch
Set Up Directory Servers for the RealPresence Touch
Enable Skype for Business Mode
Disable Skype for Business Mode
Updating Software
Dynamic Polycom Touch Device Software Updates
Managing Polycom Touch Device Software on Your Server
Update Software from the Web Interface
Update Software from the Local Interface
Update RealPresence Touch Software from a USB Storage Device
Update the Software and the Factory Restore Partition From a USB Storage Device
## System Maintenance

Managing System Profiles................................................................. 184
- Store a Setting Profile................................................................. 184
- Upload a Profile............................................................................. 184

Resetting and Restoring a RealPresence Centro System........... 185
- Reset a RealPresence Centro System........................................ 185
- Perform a Factory Restore on the RealPresence Centro System... 185
- Perform a Factory Restore Using a USB Storage Device.......... 186

Delete Data and Configuration System Files.......................... 187
- View Log File Status................................................................. 187
- Configure System Log Management.......................................... 188
- Configure System Log Level and Remote Logging.................. 188

Retrieving Log Files................................................................. 190
- Download System Log Files...................................................... 190
- Transfer System Log Files....................................................... 190
- SNMP Reporting....................................................................... 190

Upgrading RealPresence Centro System Software.................. 193
- Serial and License Numbers..................................................... 194
- Software or System Option Keys............................................. 195
- Update System Software from a USB Storage Device............ 195
- Update System Software from a .tar File............................... 195

Downgrading System Software.................................................... 196
- Determine the Software Version............................................. 196
- Delete System Settings............................................................ 196

## Troubleshooting

General Troubleshooting................................................................. 197
- View Remote Sessions on the System...................................... 198
- Placing a Test Call................................................................. 198
Contents

Other Restrictions When Using the Maximum Security Profile ........................................... 245
High Security Profile Default Settings ........................................................................... 246
Changing High Security Profile Default Values .......................................................... 257
Medium Security Profile Default Settings .................................................................... 258
Changing Medium Security Profile Default Values ..................................................... 269
Low Security Profile Default Settings .......................................................................... 269

Call Speeds and Resolutions ....................................................................................... 280
Point-to-Point Call Speeds .......................................................................................... 280
Multipoint Call Speeds for RealPresence Centro Systems ............................................ 280
High-Profile Call Speeds and Resolutions .................................................................. 280
Multipoint Resolutions for High Definition Video for RealPresence Centro Systems .... 281
Resolution and Frame Rates for Content Video ......................................................... 282
Before You Begin

Topics:

• Getting Help

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

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

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

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

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

System Serial Number: ____________________________________________
Option Key: ____________________________________________________

Getting Help

For more information about installing, configuring, and administering Polycom products, refer to the Polycom Documentation Library or Documents & Software at Polycom Support.

Polycom and Partner Resources

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

The Polycom Community

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

Topics:

- High Definition Video Conferencing
- User Interface Customization
- Security Setting Management
- Call Setting Configuration
- Powering the System On and Off
- Navigating the System

High Definition Video Conferencing

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

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

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

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

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

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

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

User Interface Customization

You can use the RealPresence Centro system web interface to configure how information is displayed for end users on the Home screen of the system local interface.
Home Screen Icons appear in the lower center of the system local interface, three at a time. By default, users see the icons shown in the following table in this location.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>📸</td>
<td>Camera</td>
</tr>
<tr>
<td></td>
<td>Opens the Camera Control screen.</td>
</tr>
<tr>
<td>📞</td>
<td>Place a Call</td>
</tr>
<tr>
<td></td>
<td>Opens the Place a Call screen, where you can manually dial a call, or can select a contact name from a list.</td>
</tr>
<tr>
<td>⚙️</td>
<td>Content</td>
</tr>
<tr>
<td></td>
<td>Appears only when a content source is detected.</td>
</tr>
</tbody>
</table>

**Security Setting Management**

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

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

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

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

**Call Setting Configuration**

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

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

Power On the RealPresence Centro System

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

Procedure

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

Automatic Wake With Motion Sensors

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

Procedure

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

Navigating the System

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

Access the System Web Interface

You can use the system web interface to perform many of the same calling and configuration tasks you can perform on the local interface.

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

• Use a supported browser.
• Configure your browser to allow cookies.

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

The system web interface supports the most commonly used web browsers. For a list of supported browsers, refer to the Polycom RealPresence Centro Release Notes at Polycom Support.
For security purposes, Polycom recommends that you follow best practices when logging into the Polycom® RealPresence Centro™ system web interface. Use an updated browser version and do not browse the internet while logged in to the system.

### Procedure

1. Enter the system IP address in a browser.
2. Enter the user name (the default is admin).
3. Enter the password, if one is set.

### Changing a Password

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

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

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

### Search the Web Interface

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

**Procedure**

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

Topics:

• Positioning the RealPresence Centro System

Positioning the RealPresence Centro System

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

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

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

Topics:

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

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

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

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

Run the Setup Wizard Locally

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

Procedure

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

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

Run the Setup Wizard from a Remote Location

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

Procedure

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

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

Topics:

• Name the System
• Enter Contact Information
• Set the Location
• Set the Language
• Set the Date and Time
• Displaying Participant Names Continuously in a Call

Name the System

The RealPresence Centro system name displays on the screens of far-end sites during a call.

The system interface supports the 16 language fonts listed in the following figure. Other languages might not display correctly. It is recommended that the first character of a system name must be a letter or a number. The system supports double-byte characters.

![Language Chart]

Procedure

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

Enter Contact Information

Enter contact information for your system so that users know whom to call when they need assistance.

Procedure

1. In the system web interface, go to Admin Settings > General Settings > My Information > Contact Information.
2. Configure the following settings.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Person</td>
<td>Specifies the name of the system administrator.</td>
</tr>
<tr>
<td>Contact Number</td>
<td>Specifies the phone number for the system administrator.</td>
</tr>
<tr>
<td>Contact Email</td>
<td>Specifies the email address for the system administrator.</td>
</tr>
<tr>
<td>Contact Fax</td>
<td>Specifies the fax number for the system administrator.</td>
</tr>
<tr>
<td>Tech Support</td>
<td>Specifies the name of the person who provides technical support.</td>
</tr>
<tr>
<td>City</td>
<td>Specifies the city where the system administrator is located.</td>
</tr>
<tr>
<td>State/Province</td>
<td>Specifies the state or province where the system administrator is located.</td>
</tr>
<tr>
<td>Country</td>
<td>Specifies the country where the system administrator is located.</td>
</tr>
<tr>
<td>Help Desk Number</td>
<td>Specifies the phone number of the help desk, displayed on the RealPresence Touch device only. Users can tap Call Help Desk to place an audio-only call to the help desk.</td>
</tr>
</tbody>
</table>

### Set the Location

Specify the country and country code where the system is located.

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Specifies the country where the system is located.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Displays the country code associated with the system location.</td>
</tr>
</tbody>
</table>
Set the Language

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

Procedure

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

Set the Date and Time

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Format</td>
<td>Specifies how the date is displayed in the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This a web-only setting.</td>
</tr>
<tr>
<td>Time Format</td>
<td>Specifies how the time is displayed in the interface.</td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving Time</td>
<td>Specifies the daylight saving time setting. When you enable this setting, the system clock automatically changes for daylight saving time.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This a web-only setting.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Specifies the time difference between GMT (Greenwich Mean Time) and your location.</td>
</tr>
<tr>
<td>Time Server</td>
<td>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.</td>
</tr>
<tr>
<td>Primary Time Server Address</td>
<td>Specifies the address of the primary time server to use when Time Server is set to Manual.</td>
</tr>
<tr>
<td>Secondary Time Server Address</td>
<td>Specifies the address of the time server to use when the Primary Time Server Address does not respond. This is an elective field.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Current Date and Current Time</td>
<td>• If the Time Server is set to Manual or Auto, these settings are not displayed.</td>
</tr>
<tr>
<td></td>
<td>• If the Time Server is set to Off, these settings are configurable.</td>
</tr>
</tbody>
</table>

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

4. Configure these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Time in Call</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Elapsed Time: Amount of time in the call.</td>
</tr>
<tr>
<td></td>
<td>• System Time: Current time set on the system.</td>
</tr>
<tr>
<td></td>
<td>• Off: Time doesn’t display.</td>
</tr>
<tr>
<td>When to Show</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Start of the call only</td>
</tr>
<tr>
<td></td>
<td>• Entire call</td>
</tr>
<tr>
<td></td>
<td>• Once per hour: At the beginning of the hour for one minute.</td>
</tr>
<tr>
<td></td>
<td>• Twice per hour: At the beginning of the hour and halfway through the hour for one minute.</td>
</tr>
<tr>
<td>Show Countdown Before Next Meeting</td>
<td>When enabled, a timer displays and counts down to the next scheduled meeting 10 minutes before it starts. (If another timer is already showing, the countdown replaces it.)</td>
</tr>
<tr>
<td></td>
<td>The countdown displays only when you enable the calendaring service.</td>
</tr>
</tbody>
</table>

### Displaying Participant Names Continuously in a Call

Administrators can configure a system to display participant names throughout a conference call.

#### Configure Participant Name Display

You can allow participants in a multipoint call to see participant names throughout the call.

**Procedure**

1. In the system web interface, go to **Admin Settings > General Settings > System Settings > Call Settings**.
2. At **Display Participant Names in Multipoint Video**, select one of the following:
   • **Auto**: After participants join a call, their names are displayed for 10 seconds (default).
• **Always**: Participant names are displayed throughout a call.

3. Select **Save**.
Using a Provisioning Service

Topics:

• Enable a Provisioning Service
• Configure a Provisioning Service
• Disable a Provisioning Service
• ZTP Web Service Solution
• Certificates and Security Profiles within a Provisioned System
• Set Up Multitiered Directory Navigation

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

• Polycom systems are registered to a standards-based presence service, so presence states are shared with Contacts.
• Polycom systems have access to a corporate directory that supports LDAP access.
• The Domain, User Name, Password, and Server Address fields are populated on the Provisioning Service screen.
• Provisioned settings are read-only in the system web interface. Settings that are dependent on provisioned values are read-only or unavailable.
• The system automatically checks for and runs software updates every time it restarts and at an interval set by the service.
• You can upload a provisioned bundle from an already configured system. When systems request provisioning, the bundle and automatic settings are downloaded.
• With administrative permissions, you can change a system’s settings after a bundle is applied (a new bundle also overwrites manual settings).
• If a registered system fails to detect the service when it restarts or checks for updates, an alert displays on System Status.
• If the system loses registration with the service, it continues to use the most recent configuration it received.

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

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

Enable a Provisioning Service

You can register your system with a provisioning service in one of the following ways:

• Running the setup wizard, which indicates if your system detects a provisioning service on the network.
The setup wizard is available during initial setup, after a system reset when you delete system settings, or when you factory reset the system. For information about configuring the RealPresence Resource Manager system so that Polycom systems detect and register with it, see the Polycom RealPresence Resource Manager System Operations Guide.

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

Procedure

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

Configure a Provisioning Service

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Specifies the type of provisioning server. Select RPRM, DMS, or CLOUD.</td>
</tr>
<tr>
<td></td>
<td>• RPRM is the RealPresence Resource Manager.</td>
</tr>
<tr>
<td></td>
<td>• DMS is the Broadsoft BroadWorks Device Management System.</td>
</tr>
<tr>
<td></td>
<td>• CLOUD is the RP Cloud server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Domain for registering with the provisioning service.</td>
</tr>
<tr>
<td>User Name</td>
<td>System user name for registering to the provisioning service.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for registering with the provisioning service.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Address of the system running the provisioning service.</td>
</tr>
</tbody>
</table>

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.

It might take a minute or two for the status to change.
Disable a Provisioning Service

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

Procedure

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

ZTP Web Service Solution

The ZTP solution is a cloud-based web service designed to simplify the deployment of Polycom devices. The Polycom ZTP console is a web interface that you can use to create and manage profiles and device associations. The ZTP solution is intended as a one-time step at initial deployment. Usually, end customers require a supplier or skilled installer to deploy devices out-of-the-box. The ZTP web console enables you to create provisioning profiles so that you can associate with one or more devices. These profiles enable end customers to install the devices themselves. The profiles also provide a central provisioning server address that automatically redirects multiple customer devices to your provisioning server. In addition to setting the provisioning server address, you can use the solution to provision RealPresence Group systems that are running version 5.0 software or later.

For information about deploying the solution, refer to the Polycom Zero Touch Provisioning Guide at Polycom Support.

Certificates and Security Profiles within a Provisioned System

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

- To use the Maximum Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using Maximum Security Mode.
  - You must manually assign the Maximum Security Profile to the system during installation using the setup wizard, or afterwards using the system web interface.
  - You must use full PKI and observe the following procedures before you enable provisioning on the system:
    1. You must install a signed client certificate on the system to enable the provisioning connection to be authenticated by the RealPresence Resource Manager system.
    2. Decide whether to automatically validate web clients by enabling the Always Validate Peer Certificates from Browsers setting. If you do enable the setting, you'll need to install a signed server certificate and all of the CA certificates needed to validate browser certificates for all web clients. Then configure the certificate revocation method.
    3. Decide whether to validate servers by enabling the Always Validate Peer Certificates from Servers setting. If you do enable the setting, you must install of the CA certificates needed to validate server certificates from all remote servers. Then
adjust the certificate revocation method accordingly. For example, you might need to load additional CRLs if you use the CRL revocation method).

- To use the Medium or High Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using commercial mode.
  - You must manually assign the Medium or High Security Profile to the system during installation using the setup wizard, or afterwards using the system web interface.
  - Configure PKI according to your company’s guidelines.

- To use the Low Security Profile with provisioning:
  - The RealPresence Resource Manager system must be using commercial mode.
  - You can enable provisioning in the setup wizard. All provisionable settings are taken from the RealPresence Resource Manager system.

Set Up Multitiered Directory Navigation

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

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

The following limitations apply to this feature:

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

Procedure

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

Topics:
  • System Software Options

System Software Options
System software options unlock certain features available for your system model. These options provide additional functionality, such as multipoint video conferencing, Skype for Business interoperability, and 1080p video.

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

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

View System Software Options
You can view options supported on your RealPresence Centro system in the system web interface.

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

Obtain Software or System Option Keys
A key is a number that unlocks certain features or gives you the ability to update your system.

To activate features or update software, you must obtain a key that’s valid only with your system. You can obtain software or option keys for a single system or for multiple systems. If you don’t have a support agreement, contact an authorized Polycom dealer to get a key.

The following types of keys are available:
  • Software keys are valid for the software updates you are installing as well as for any point, maintenance, or patch releases that may later become available.
  • Option keys activate software options and are valid across all software releases.

Procedure
  1. Go to Polycom Support.
  2. Go to Licensing & Product Registration > Activation/Upgrade at Polycom Support.
  3. Do one of the following:
    • Log in with your email address and password.
    • Register as a new user.
  4. Do one of the following:
• To update one system, select **Site & Single Activation/Upgrade**. Follow the onscreen instructions to enter your system serial number and license. Go to the **Upgrade** tab to confirm the version upgrade key code.

• To update multiple systems that are covered by a software service agreement, select **Batch Upgrade** and choose your product. Follow the onscreen instructions to upload the text file that contains your system license and serial numbers (or serial numbers only).

• To activate features for multiple systems covered by a software service agreement, select **Batch Activation**. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers (or serial numbers only). You are sent a text file containing the requested keys for each system.

Create a Single Key File to Update Multiple Systems

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

**Procedure**

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

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

**Key File Formats**

Most key files use this format:

<table>
<thead>
<tr>
<th>License Number</th>
<th>Serial Number</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1059-3131-6042-3609</td>
<td>8213190FFAE7D5</td>
<td>U8FB-0D4E-6E30-0000-0009</td>
</tr>
</tbody>
</table>

The following example shows a software update key file:

<table>
<thead>
<tr>
<th>License Number</th>
<th>Serial Number</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1000-0000-0000-0000-0003</td>
<td>82041003E070B0</td>
<td>U8FB-0D4E-6E30-0000-0009</td>
</tr>
<tr>
<td>U1000-0000-0000-0000-0004</td>
<td>820327024193AK</td>
<td>U982-4507-5D80-0000-0009</td>
</tr>
</tbody>
</table>

The following example shows an option key file:

<table>
<thead>
<tr>
<th>License Number</th>
<th>Serial Number</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>K1000-0000-0000-0000-0001</td>
<td>82041003F082B1</td>
<td>K15B-DC2D-E120-0000-0009</td>
</tr>
<tr>
<td>K1000-0000-0000-0000-0002</td>
<td>82041503E093B0</td>
<td>K27E-30F9-2D20-0000-0009</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>License Number</th>
<th>Serial Number</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>82041003F082B1</td>
<td>U7B6-698E-1640-0000-02C1</td>
</tr>
<tr>
<td>U</td>
<td>82041503E093B0</td>
<td>UCC1-C9A6-FE60-0000-02C1</td>
</tr>
</tbody>
</table>
Activate System Options

To activate certain features on your RealPresence Centro system, you must use the system's web interface to enter an option key. 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 the appropriate option key.

Procedure

1. Open the system web interface.
2. Navigate to Admin Settings > General Settings > Options.
3. In the Key field, enter the option key and click Save.
Registering with a Calendaring Service

Topics:
- Enable the Calendaring Service
- Join Scheduled Meetings

Your RealPresence Centro system can display calendar details linked to a Microsoft Outlook or Office 365 account. The system retrieves this information from Microsoft Exchange Server with credentials you provide or through automatic discovery using an associated email or SIP server address.

Your system performs the following actions when you configure it to use a calendaring service:
- Displays the day’s scheduled meetings, including details about each
- Lets users join a meeting with one click or touch
- Hides details about meetings marked private (depending on how you configure the system)
- Displays a meeting reminder and plays a reminder tone before the next scheduled meeting

Enable the Calendaring Service

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

When verifying your configuration for interoperability with Zoom, ensure that the value for the Microsoft Exchange Server is interop.zoom.us.

Procedure
1. In the system web interface, go to Admin Settings > Servers > Calendaring Service.
2. Select the Enable Calendaring Service check box.
3. Configure the following options;

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Specifies the email address used when scheduling the system for a meeting (for instance, you can use your system as a mechanism to reserve a meeting space). This email address must match the Primary SMTP Address for the account on Microsoft Exchange Server, which displays as the value of the mail attribute in the account properties.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain</strong></td>
<td>Specifies the domain to register to the Microsoft Exchange Server in NETBIOS or DNS notation (for example, company.local or COMPANY). If you are using the Auto Discover Using setting in the system web interface, don’t provide a value here.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Specifies the user name to register to the Microsoft Exchange Server. This can be the name of the system or an individual (for example, <a href="mailto:username@company.com">username@company.com</a>). If you want to use the calendar associated with an Office 365 account, enter the user name for that account here.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Specifies the system password to register to the Microsoft Exchange Server. This can be the system's or an individual's password. If you want to use the calendar associated with an Office 365 account, enter the password for that account here.</td>
</tr>
<tr>
<td><strong>Auto Discover Using</strong></td>
<td>Specifies how the system obtains the Microsoft Exchange Server address. If you select Email Address, the system uses the value provided in the Email field. If you select SIP Server, the system uses the registered SIP server domain name configured for the system. With either option, you must complete the Email, User Name, and Password fields that correspond to the account you want the system to use for the calendaring service. The system may prompt you to confirm the password. If after configuring the calendaring service a message displays that the system is unable to discover the service, verify that the information you provided is correct. You can also use an API command to automatically discover the Microsoft Exchange Server address. For more information, go to Polycom Support.</td>
</tr>
<tr>
<td><strong>Microsoft Exchange Server</strong></td>
<td>Specifies the FQDN of the Microsoft Exchange Client Access server. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server’s virtual IP address. If required, you can use an IP address instead of an FQDN, but Polycom recommends using the same FQDN for Outlook clients. Provide a value here only if you want to manually provide connection information to the Microsoft Exchange Server. Otherwise, use the Auto Discover Using setting to automatically populate this field.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure Connection Protocol</td>
<td>Specifies the connection protocol to connect to the Microsoft Exchange Server/Skype for Business Server. Select <strong>Automatic</strong> or <strong>TLS 1.0</strong>.</td>
</tr>
<tr>
<td>Meeting Reminder Time in Minutes</td>
<td>Specifies the number of minutes before the meeting that a reminder displays on the system.</td>
</tr>
<tr>
<td>Play Reminder Tone When Not in a Call</td>
<td>Specifies whether to play a sound along with the text reminder (when the system is not in a call).</td>
</tr>
<tr>
<td>Show Information for Meetings Set to Private</td>
<td>Specifies whether to display details about meetings marked private.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

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

## Join Scheduled Meetings

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

**Procedure**

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

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

Topics:
- Connecting to a LAN
- LLDP and LLDP-MED Support
- IP Network Settings
- Multilevel Precedence and Preemption (MLPP)
- Multipoint Conference On a RealPresence Collaboration Server
- Web Proxy Auto-Discovery Protocol
- Configure Network Quality Settings
- Simplified ISDN Dialing
- Support for Location-Based Routing in Skype for Business Hosted Calls

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.

Note: Running the scanning tools is not recommended during business hours as this might result in the performance degradation on RealPresence Centro.

Connecting to a LAN
You must connect the RealPresence Centro system to a LAN to do any of the following with your system:
- Make H.323 or SIP calls
- Use a Global Directory Server
- Register with a management system
- Access the system web interface
- Use Polycom People+Content IP
- Connect to a RealPresence Touch device

Configure LAN Properties
You can configure LAN properties for your system in the local interface or the system web interface.

Procedure
1. In the system web interface, go to Admin Settings > Network > LAN Properties.
2. Configure the following LAN Options settings in the system web interface at Admin Settings > Network > LAN Properties > LAN Options.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Name</strong></td>
<td>Indicates your system name. If the system discovers a valid name during setup or a software update, the system automatically creates the hostname. However, if an invalid name is found, such as a name with a space, the system creates a hostname using the following format: <code>SystemType-xxxxxx</code>, where <code>xxxxxx</code> is a set of random alphanumeric characters.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td><strong>IPv4 networks</strong>: The system sends the host name to the DHCP server to attempt to register the name with the local DNS server or look up the domain where the system is registered (if supported).</td>
</tr>
<tr>
<td></td>
<td><strong>IPv6 networks</strong>: You can leave this field blank since the system doesn’t support this function. However, Polycom recommends configuring the field to contain the registered host name.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Identifies the domain your system belongs to.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td>If the system doesn’t automatically obtain a domain name, optionally enter one here.</td>
</tr>
<tr>
<td><strong>Autonegotiation</strong></td>
<td>Specifies whether the system should automatically negotiate the LAN speed and duplex mode per IEEE 802.3 autonegotiation procedures. If you enable this setting, the system sets <strong>LAN Speed</strong> and <strong>Duplex Mode</strong> to read-only.</td>
</tr>
<tr>
<td>(under General Settings in the local interface)</td>
<td>Polycom recommends that you use autonegotiation to avoid network issues.</td>
</tr>
<tr>
<td><strong>LAN Speed</strong></td>
<td>Specifies whether to use 10 Mbps, 100 Mbps, or 1000 Mbps for the LAN speed. Note that the switch must support the speed you choose. If you enable the <strong>Autonegotiation</strong> setting, this setting is read-only.</td>
</tr>
<tr>
<td>(under General Settings in the local interface)</td>
<td></td>
</tr>
<tr>
<td><strong>Duplex Mode</strong></td>
<td>Specifies the duplex mode to use. Note that the switch must support the speed you choose. If you enable the <strong>Autonegotiation</strong> setting, this setting is read-only.</td>
</tr>
<tr>
<td>(under General Settings in the local interface)</td>
<td></td>
</tr>
<tr>
<td><strong>Ignore Redirect Messages</strong></td>
<td>Enables the system to ignore ICMP redirect messages.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td>Polycom recommends that you enable this setting in most circumstances.</td>
</tr>
<tr>
<td><strong>ICMP Transmission Rate Limit (millisec)</strong></td>
<td>Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 means the system sends 1 packet per second. If you enter 0, the system enables the transmission rate limit.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td>This setting applies only to “error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Generate Destination Unreachable Messages</strong></td>
<td>Generates an ICMP Destination Unreachable message if the system can’t deliver a packet to its destination for reasons other than network congestion.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td></td>
</tr>
<tr>
<td><strong>Respond to Broadcast and Multicast Echo Requests</strong></td>
<td>When enabled, your system sends an ICMP Echo Reply message in response to a broadcast or multicast Echo Request that isn’t specifically addressed to the system.</td>
</tr>
<tr>
<td>(system web interface only)</td>
<td></td>
</tr>
</tbody>
</table>
| **IPv6 DAD Transmit Count**                  | 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. |
| (system web interface only)                  |                                                                                                                                              |
| **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**                              | Specifies if you want the system to advertise itself on the network using the Link Layer Discovery Protocol (LLDP). Enable if you want your system to operate on a virtual LAN (VLAN). |
| (under **General Settings** in the local interface) |                                                                                                                                               |
| **Enable EAP/802.1X**                        | Enables EAP/802.1X network access. The system supports the following authentication protocols:  
• EAP-MD5  
• EAP-PEAPv0 (MSCHAPv2)  
• EAP-TTLS  
• EAP-TLS |
| (under **EAP 802.1X** in the local interface) |                                                                                                                                               |
| **EAP/802.1X Identity**                      | Specifies the identity the system uses for 802.1X authentication. This setting is available only when you enable EAP/802.1X. You can’t leave this field blank. |
| (under **EAP 802.1X** in the local interface) |                                                                                                                                               |
| **EAP/802.1X Password**                      | Specifies the password the system uses for 802.1X authentication. This setting is required when you use EAP-MD5, EAP-PEAPv0, or EAP-TTLS. |
| (under **EAP 802.1X** in the local interface) |                                                                                                                                               |
| **Enable 802.1p/Q**                          | Enable if you want to configure your system with a virtual LAN (VLAN) and set link layer priorities. |
| (under **802.1p/Q** in the local interface)  |                                                                                                                                               |
| **VLAN ID**                                  | Identifies the VLAN you want your system to operate on. This setting is available only when you enable 802.1p/Q. You can use values from 1 to 4094. |
|                                             |                                                                                                                                               |
Setting | Description
--- | ---
**Video Priority** | Sets the link layer priority of video traffic on the wired LAN. Video traffic is RTP traffic consisting of video data and associated RTCP traffic. This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Poly recommends not using 6 and 7.

**Audio Priority** | Sets the link layer priority of audio traffic on the wired LAN. Audio traffic is RTP traffic consisting of audio data and associated RTCP traffic. This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Poly recommends not using 6 and 7.

**Control Priority** | Sets the link layer priority of control traffic on the wired LAN. Control traffic consists of control information associated with a call:
- **H.323**: H.225.0 Call Signaling, H.225.0 RAS, H.245, Far-End Camera Control (FECC)
- **SIP**: SIP Signaling, FECC, Binary Floor Control Protocol (BFCP)

This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Poly recommends not using 6 and 7.

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

### Configure IP Address (IPv4) Settings

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

**Procedure**

1. In the system web interface, go to **Admin Settings > Network > LAN Properties**.
2. Configure the following IPv4 settings on the LAN Properties screen.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>Specifies how the system obtains an IP address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Obtain IP address automatically</strong>—Select if the system gets an IP address from a DHCP server on the LAN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enter IP address manually</strong>—Select if the IP address will not be assigned automatically.</td>
</tr>
</tbody>
</table>
### Configure IP Address (IPv6) Settings

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable IPv6</strong></td>
<td>Enables the IPv6 network stack and makes the IPv6 settings available.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Specifies how the system obtains an IP address.</td>
</tr>
<tr>
<td>- Obtain IP address automatically—Select if the system gets an IP address from a SLAAC or a DHCP server on the LAN.</td>
<td></td>
</tr>
<tr>
<td>- Enter IP address manually—Select if the IP address will not be assigned automatically.</td>
<td></td>
</tr>
<tr>
<td><strong>Enable SLAAC</strong></td>
<td>Specifies whether to use stateless address autoconfiguration (SLAAC) instead of DHCP to automatically obtain an IP address.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Link-Local</strong></td>
<td>Displays the IPv6 address used for local communication within a subnet.</td>
</tr>
<tr>
<td></td>
<td>This setting is configurable only when Enter IP Address Manually is selected.</td>
</tr>
</tbody>
</table>
### Configuring Network Settings

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNS Servers</strong></td>
<td>Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, you can enter one here.</td>
</tr>
<tr>
<td><strong>Server 1 Address</strong></td>
<td>If the system does not automatically obtain a DNS server address, you can enter one here. Up to four DNS server addresses are allowed.</td>
</tr>
<tr>
<td><strong>Server 2 Address</strong></td>
<td>If the system does not automatically obtain a DNS server address, you can enter one here. Up to four DNS server addresses are allowed.</td>
</tr>
<tr>
<td><strong>Server 3 Address</strong></td>
<td>If the system does not automatically obtain a DNS server address, you can enter one here. Up to four DNS server addresses are allowed.</td>
</tr>
<tr>
<td><strong>Server 4 Address</strong></td>
<td>If the system does not automatically obtain a DNS server address, you can enter one here. Up to four DNS server addresses are allowed.</td>
</tr>
</tbody>
</table>

#### LLDP and LLDP-MED Support

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

Examples of applications that use information discovered by LLDP include:

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

**LLMP-MED Information Discovery**

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

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

**Behavior When LLDP is Enabled**

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

- Video Conferencing VLAN
- Voice VLAN
- Voice Signaling VLAN

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

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

**Enable LLDP Using a USB Storage Device**

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

**Procedure**

1. Create a `usbprovisioning.properties` file with the following text string:
   
   ```
   lldpenable=true
   ```

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

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

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

Procedure
1. In the system web interface, go to Admin Settings > Network > LAN Properties.
2. Select the check box at Enable LLDP and click Save.

IP Network Settings

You can configure the following IP network protocols in the RealPresence Centro system web interface.
- H.323
- SIP

Configure H.323 Settings

If your network uses an H.323 gatekeeper, the system can automatically register its H.323 name and extension. Others can then call the system using its H.323 name or extension instead of its IP address.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP H.323</td>
<td>Enables the system to display H.323 settings and configuration options.</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Read-only setting shows if your system is registered with an H.323 gatekeeper.</td>
</tr>
<tr>
<td>H.323 Name</td>
<td>How gatekeepers and gateways identify your system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The <strong>H.323 Name</strong> is the same as the device name unless you change it. Your organization’s dial plan might define the name you can use.</td>
</tr>
<tr>
<td>H.323 Extension (E.164)</td>
<td>You can place point-to-point calls using this extension if both systems are registered with a gatekeeper. Gatekeepers and gateways also use the extension to identify your system. Your organization’s dial plan might define the extensions you can use.</td>
</tr>
</tbody>
</table>
Configure the System to Use a Gatekeeper

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Gatekeeper</strong></td>
<td>Specifies if you want to use a gatekeeper for H.323 services.</td>
</tr>
<tr>
<td></td>
<td>• Off: Calls don’t use a gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>• Auto: System tries to automatically find an available gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>• Specify: Calls use the specified gatekeeper. You must select this setting to enable H.235 Annex D Authentication.</td>
</tr>
<tr>
<td></td>
<td>If you don’t configure this setting to <strong>Off</strong>, a registration status displays.</td>
</tr>
<tr>
<td><strong>Require Authentication</strong></td>
<td>Enables support for H.235 Annex D Authentication.</td>
</tr>
<tr>
<td></td>
<td>When you enable H.235 Annex D Authentication, the H.323 gatekeeper ensures that only trusted H.323 endpoints can access the gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>This setting is available when you set <strong>Use Gatekeeper</strong> to Specify.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>When authentication is required, specifies the user name for authentication with H.235 Annex D.</td>
</tr>
<tr>
<td><strong>Enter Password</strong></td>
<td>When authentication is required, specifies the password for authentication with H.235 Annex D.</td>
</tr>
<tr>
<td><strong>Current Gatekeeper IP Address</strong></td>
<td>Displays the IP address that the gatekeeper is using.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Off</strong> for the <strong>Use Gatekeeper</strong> field, the <strong>Current Gatekeeper IP Address</strong> field doesn’t display.</td>
</tr>
</tbody>
</table>
### Primary Gatekeeper IP Address Table

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Primary Gatekeeper IP Address| The gatekeeper IPv4 address the system registers with. As part of the registration process, the gatekeeper might return alternate gatekeepers. If your system loses communication with the primary gatekeeper, your system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system re-establishes communication with the primary gatekeeper, it unregisters from the alternate gatekeeper.  
  • If you set the Use Gatekeeper field to Off, the Primary Gatekeeper IP Address field doesn’t display.  
  • If you use an automatically selected gatekeeper, this area displays the gatekeeper’s IP address.  
  • If you specify a gatekeeper, enter the gatekeeper IP address or name (for example, 10.11.12.13 or gatekeeper.companyname.usa.com). |

### SIP Settings
If your network supports SIP, you can use it to connect calls on your system.

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Enables the system to make and receive SIP calls.</td>
</tr>
<tr>
<td>Enable AS-SIP</td>
<td>Enables the system to display the AS-SIP settings configuration options.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Read-only setting shows if your system is registered to a SIP server.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Specifies whether to automatically or manually set the SIP server’s IP address. If you select <strong>Auto</strong>, you can’t edit the <strong>Transport Protocol</strong>, <strong>Registrar Server</strong>, and <strong>Proxy Server</strong> settings. If you select <strong>Specify</strong>, you can edit these settings.</td>
</tr>
</tbody>
</table>
| Transport Protocol      | Sets the protocol your system uses for SIP signaling (your SIP network determines which protocol is required).  
  - **Auto**: Enables automatic negotiation of protocols in the following order: TLS, TCP, and UDP. Polycom recommends this setting for most environments.  
  - **TCP**: Provides reliable transport via TCP.  
  - **UDP**: Provides best-effort transport via UDP.  
  - **TLS**: Provides secure SIP signaling. TLS is available only when you register your system with a SIP server that supports it. If you set this option, your system ignores TCP/UDP port 5060. Select TLS if you want to encrypt SVC calls. |
<p>| Force Connection Reuse  | Disabled by default (recommended). When disabled, the system uses an ephemeral source port for outgoing SIP messages. When enabled, the system uses the active SIP listening port as the source port (5060 or 5061, depending on the negotiated SIP transport protocol in use). You can use this setting to establish correct operation with remote SIP peer devices, which require that the source port match the contact port in SIP messages. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **BFCP Transport Preference** | Controls content sharing negotiation behavior. When you use the Binary Floor Control Protocol (BFCP), a relationship is established between the floor control server and its clients. What you set here determines how network traffic flows between the server and clients.  
Note: TCP is typically slightly slower but more reliable than UDP. Some deployments don’t support it, such as with session border controllers (SBCs).  
• **Prefer UDP**: (Default) Starts resource sharing using UDP but falls back to TCP if needed.  
• **Prefer TCP**: Starts resource sharing using TCP but falls back to UDP if needed.  
• **UDP Only**: Shares resources only using UDP. If UDP is unavailable, your system can’t share content in a separate video stream.  
• **TCP Only**: Shares resources only through TCP. If TCP is unavailable, your system can’t share content in a separate video stream. |
| **Sign-in Address**           | The SIP address or name of the system (for example, mary.smith@department.company.com). If you leave this blank, the system IP address is used for authentication. |
| **User Name**                 | The user name for authenticating your system with a SIP registrar server (for example, marySmith). If the SIP proxy requires authentication, you can’t leave the user name and password blank. |
| **Password**                  | The password associated with the user name for authenticating your system with a SIP registrar server.                                       |
| **Registrar Server**          | The IP address or FQDN of the SIP registrar server. If you register a remote system with an edge server, use that server’s FQDN.  
By default, the system sends SIP signaling to ports 5060 (TCP) and 5061 (TLS) on the registrar server.  
Enter the address and port using the following format:  
<IP_Address>:<Port>.  
The <IP_Address> can be an IPv4 or IPv6 address or an FQDN (for example, servername.company.com:6050). |
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Server</strong></td>
<td>The IP address or FQDN of the SIP proxy server. If you leave this field blank, the system uses the registrar server address. If you also leave the SIP registrar server field blank, there is no SIP proxy server to configure. By default, the system sends SIP signaling to ports 5060 (TCP) and 5061 (TLS) on the proxy server. The syntax for this setting is the same as the registrar server.</td>
</tr>
</tbody>
</table>

| **Registrar Server Type** | Specifies the type of SIP registrar server you’re using.                                                                                                                                           |

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

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

### RTV and Skype-Hosted Conference Support

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

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

### Multilevel Precedence and Preemption (MLPP)

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

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

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

- Answer directly
- Join into conference
Define MLPP Network Domains

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

Procedure

1. To edit a domain, click ![edit_icon].
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence Level</td>
<td>The name associated with the precedence level. You can click <strong>Add Precedence Level</strong> to create a level and you can click <strong>x</strong> to remove a level.</td>
</tr>
<tr>
<td>Dial Digit</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Priority Header</td>
<td>Represents the value in the SIP Resource Priority Header used to signal the precedence level. This field accepts a single UTF-8 character.</td>
</tr>
<tr>
<td>Audio DSCP</td>
<td>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.</td>
</tr>
<tr>
<td>Video DSCP</td>
<td>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.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

Add an MLPP Network Domain

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

Procedure

1. To add a network domain, click ![add_icon] and then configure the same settings for the new network domain in the define MLPP network domains task above.
2. Click **Save** when you are finished configuring the settings to save your changes.
**Alternative Network Address Type (ANAT)**

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

RealPresence Centro

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

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

**Multipoint Conference On a RealPresence Collaboration Server**

You can enable users to create an impromptu conference call during an active SIP call. To do this, you must configure RealPresence Group Series systems to escalate new calls to an RMX conference call.

Polycom recommends that you disable adhoc call escalation to make calls through an internal MCU.

For information on configuring a SIP conference factory on a DMA system or locating the conference factory ID, see the *RealPresence DMA System v9.0.0 Operations Guide*.

**Enable Call Escalation of Point-to-Point Calls**

You can enable point-to-point call escalation on your system.

**Procedure**

1. In the system web interface, navigate to **Admin Settings > Network > IP Network > Adhoc Call Escalation**.
2. Select **Enable automatic call escalation of point-to-point to an external MCU**.
3. For the **Conference Factory ID**, enter the ID associated with the SIP conference factory on your RealPresence DMA system.

**Note:** The conference factory ID must come from the same RealPresence DMA system your video conferencing system uses for SIP registration. Calls don’t escalate if your RealPresence DMA system doesn’t recognize the ID you provide.

4. Select **Save**.

Calls converted through a RealPresence DMA system gateway (H.323 to SIP or vice versa) don’t join an impromptu conference call.
Web Proxy Auto-Discovery Protocol

The Web Proxy Auto-Discovery Protocol (WPAD) allows RealPresence Centro systems to route network traffic outside enterprise networks.

When your RealPresence Centro system uses Web Proxy, inbound HTTP and HTTPS traffic (ports 80 and 443) is directed to the configured proxy or proxies.

The Proxy auto-config (PAC) file is a configuration file executed by the system to determine the proxy for a specified URL.

Your system can authenticate with a proxy using the following methods:

- Digest authentication (with either MD-5 or SHA-256 digest)
- NTLM authentication (only NTLMv2 is supported)
- Basic authentication (this insecure method is disabled by default)
- No authentication (or null authentication, meaning the proxy server doesn’t require credentials)

By default, the Basic authentication is disabled. You can enable Basic authentication in RealPresence Centro system web interface.

Your system supports the following services when configured to use a web proxy:

- Directory servers
- Provisioning service
- Calendaring service
- Recording service
- Software updates
- Uploading logs

Sample PAC file

This section shows an example of a sample PAC file.

```javascript
function FindProxyForURL(url, host)
{
    if ( url.substring (0, 5) == "http:" )
    {
        return "PROXY 10.221.77.3:8080; PROXY 10.221.76.7:8080;DIRECT";
    }
    else if ( url.substring (0, 6) == "https:" )
    {
        return "PROXY 10.221.77.3:8080; PROXY 10.221.76.7:8080;DIRECT";
    }
    else
    {
        return "DIRECT";
    }
}
```

The Function “function FindProxyForURL(url, host)” returns a string with one or more access method specifications. These specifications cause RealPresence Group Series system to use a particular proxy server or connect directly.

This function instructs RealPresence Group Series system to retrieve information for http / https protocols using the first proxy i.e. “PROXY 10.221.77.3:8080”.

If “PROXY 10.221.77.3:8080” is unreachable/unresponsive, then RealPresence Group series system tries the second proxy i.e. “PROXY 10.221.76.7:8080”.

Polycom, Inc.
For more examples on PAC syntax, refer to [FindProxyForURL](https://en.wikipedia.org/wiki/FindProxyForURL).

**Note:** If the first specified proxy is reachable and the authentication is unsuccessful, RealPresence Group Series system will not roll over to try a different proxy path.

---

**Enable Web Proxy**

Web Proxy is disabled in RealPresence Centro system by default.

To enable Web Proxy settings for the RealPresence Centro system:

**Procedure**

1. In the RealPresence Centro system web interface, go to `Admin Settings > Network > Web Proxy Settings`.
2. Select `Enable Web Proxy` check box.

**Configure Web Proxy Settings**

To allow RealPresence Centro system to use the Web Proxy protocol.

**Procedure**

1. In the system web interface, go to `Admin Settings > Network > Web Proxy Settings`.
2. Do one of the following:
   - If `Use SFB Credentials for Proxy` is checked, the system automatically takes the SIP user credentials defined in the RealPresence Centro web interface.
   - Select `Auto configuration` checkbox and uncheck the `Enable WPAD` checkbox. Enter the `Proxy Username` and `Proxy Password`, and enter the `PAC URL`.
   - Select `Auto configuration` and `Enable WPAD` checkbox. Enter the `Proxy Username` and `Proxy Password`. Providing the Proxy Username and Proxy Password is not mandatory.
   - Uncheck `Auto configuration` checkbox. Enter the `Proxy Username`, `Proxy Password`, `Proxy Address`, and `Proxy Port`. Providing the Proxy Username and Proxy Password is not mandatory.
3. Click `Save`.

**Update Proxy auto-config (PAC) File**

When the PAC file is updated on the server, do the following to make the changes effective on RealPresence Centro system:

**Procedure**

1. In the system web interface, go to `Admin Settings > Network > Web Proxy Settings`.
2. Click `UPDATE PAC FILE`.

**Verify Proxy auto-config (PAC) File**

To verify the PAC file configured on the RealPresence Centro system:
**Procedure**

1. In the system web interface, go to Admin Settings > Network > Web Proxy Settings.
2. Click on DOWNLOAD PAC FILE link to download the PAC file.

   The Proxy auto-config (PAC) file is a configuration file executed by the system to determine the proxy for a specified URL.

**Verify Proxy auto-config (PAC) File Status**

To verify the PAC file status on the RealPresence Centro system:

**Procedure**

 » In the system web interface, go to Admin Settings > Network > Web Proxy Settings.

   Following are the various status for the PAC File:
   - **Success**
     The PAC File is successfully downloaded.
   - **In Progress**
     The PAC File download is in progress.
   - **WPAD Failed**
     The DHCP 252 protocol has not successfully fetched the PAC URL.
   - **Download Failed**
     The PAC File download is failed.
   - **Expired**
     The PAC File is expired.

**Limitations**

RealPresence Centro system configured with Web Proxy has the following limitations:

- Polycom recommends using “realm” authentication along with the username for Digest and NTLM authentication mechanisms. For e.g “realm\username” is applicable for both Digest and NTLM mechanisms.
- When configuring Auto Configuration with Web Proxy Enabled, the PAC file will be downloaded only if RealPresence Centro system receives the corresponding DHCP option field from the DHCP server.
- There is no RPRM provisioning support when RealPresence Centro system is configured with Web Proxy.
- There is no option available to verify Web Proxy authentication status.
- The System Status information is not available in RealPresence Centro system web interface, when Web Proxy is enabled for RealPresence Centro system.
- The admin can configure and change the Web Proxy settings only through RealPresence Centro web interface.
- RealPresence Centro Web Proxy does not support media on 443 port.
Configure Network Quality Settings

You can specify how your system responds to network quality issues by controlling how your network handles packets during video calls.

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically Adjust People/Content Bandwidth</strong></td>
<td>Specifies whether the system automatically adjusts bandwidth for the people or content stream depending on the relative complexity of the people video, content video, or both. If you enable this setting, the <strong>Quality Preference</strong> setting is not available.</td>
</tr>
<tr>
<td><strong>Quality Preference</strong></td>
<td>Specifies which video stream has precedence when attempting to compensate for network loss:</td>
</tr>
<tr>
<td>• Both people and content streams</td>
<td>The stream option you select experiences less quality degradation during network loss compensation than the other. Choosing Both means each stream experiences roughly equal degradation.</td>
</tr>
<tr>
<td>• People streams</td>
<td>This setting is not available if you enable <strong>Automatically Adjust People/Content Bandwidth</strong>.</td>
</tr>
<tr>
<td>• Content streams</td>
<td></td>
</tr>
<tr>
<td><strong>Type of Service</strong></td>
<td>Specifies the type of service (ToS), which lets you prioritize packets sent to your system for video, audio, Far End Camera Control (FECC), and OA&amp;M:</td>
</tr>
<tr>
<td>• IP Precedence</td>
<td><strong>Note</strong>: If you enable AS-SIP and you select <strong>DiffServ</strong>, the DSCP values for audio and video defined for the negotiated call precedence level in the default network domain for outbound calls override the <strong>Video</strong> and <strong>Audio</strong> settings on this page. If you don’t enable AS-SIP, the system uses the <strong>Video</strong> and <strong>Audio</strong> values defined here.</td>
</tr>
<tr>
<td>• DiffServ</td>
<td></td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>Specifies the <strong>IP Precedence</strong> or <strong>DiffServ</strong> priority level for video RTP and associated RTCP traffic.</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>Specifies the <strong>IP Precedence</strong> or <strong>DiffServ</strong> priority level for audio RTP and associated RTCP traffic.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Specifies the IP Precedence or DiffServ priority level for control traffic on the following channels:</td>
</tr>
</tbody>
</table>
|                                        | • **H.323**: H.225.0 Call Signaling, H.225.0 RAS, H.245, and FECC  
|                                        | • **SIP**: SIP Signaling, FECC, and Binary Floor Control Protocol (BFCP)  
|                                        | (The system enables FECC by **Allow Other Participants in a Call to Control Your Camera**.)                                               |
| **OA&M**                               | Specifies the IP Precedence or DiffServ value for traffic unrelated to video, audio, or FECC.                                             |
| **Maximum Transmission Unit Size**     | Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or let you select it.                                   |
| **Maximum Transmission Unit Size Bytes** | Specifies the MTU size (in bytes) used in calls.                                                                                          |
|                                        | • If video quality is poor or you experience network errors, 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**        | If you enable this setting, the system uses the Lost Packet Recovery (LPR) protocol to help compensate for packet loss if it occurs.         |
| **Enable RSVP**                        | If you enable this setting, the system can use the Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. (To use this feature, the near and far site must support RSVP.) |
| **Dynamic Bandwidth**                  | Enable this setting if you want the system to automatically determine the optimal call rate.                                              |
| **MRC Bandwidth Allocation**           | Adjusts media bit stream bandwidth, reducing packet loss. This setting is specifically designed for SVC-based calls.                         |
| **Maximum Transmit Bandwidth**         | Specifies the maximum transmit call rate between 64 kbps and the system’s maximum line rate.                                               |
|                                        | Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.          |
Maximum Receive Bandwidth

Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate.

Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.

Lost Packet Recovery and Dynamic Bandwidth Settings

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

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

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

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

Simplified ISDN Dialing

The Simplified ISDN dialing feature provides seamless ISDN Gateway call dialing support on RealPresence Group Series systems through Polycom ISDN Gateway. You can now make calls by entering the ISDN number without entering a prefix of the ISDN Gateway IP address.

Configure Gateway Call Type Settings

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Gateway</td>
<td>Allows the ISDN Gateway settings to display and to be configured.</td>
</tr>
<tr>
<td>Gateway Number Type</td>
<td>Indicates the Gateway number type for ISDN Gateway dialing.</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• E.164</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gateway Number</td>
<td>Specify the number based upon the <strong>Gateway Number Type</strong> you select.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong>: Specify the IP address for the ISDN Gateway.</td>
</tr>
<tr>
<td></td>
<td>• <strong>E.164</strong>: Specify the H.323 extension (E.164 number) for the ISDN Gateway. Your organization’s dial plan might define the extensions you can use.</td>
</tr>
</tbody>
</table>

3. Select **Save**.

**Support for Location-Based Routing in Skype for Business Hosted Calls**

The RealPresence Centro system now supports location-based routing (LBR) for Skype for Business calls. Location-Based Routing make it possible to restrict the routing of calls between VoIP endpoints and PSTN endpoints based on the location of the parties in the call.

**Note:** This feature is supported in Skype for Business VoIP calls in an IPv4 environment only.

The LBR feature introduces a new set of rules to prevent toll bypass by restricting the routing of an outgoing call to a national or an international PSTN number as per the call authorization rules. You must enable this feature on the Skype for Business server.
Securing the System

Topics:

• Configure Security Profiles
• Managing System Access
• Detecting Intrusions
• View Connections to Your System in a Sessions List
• Secure API Access
• Port Lockout
• Whitelisting
• Encryption
• Firewall/NAT Traversal
• Security Certificates
• Set Up a Security Banner
• Set a Meeting Password
• Visual Security Classification
• Enable Room and Call Monitoring

Configure Security Profiles

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 Admin Settings in the system web interface. The default values and ability to change some settings are affected by which security profile your system uses.

Consider each security profile as a set of default values for all configuration settings that affect product security and that achieves some level of base product security. You can choose from four profiles—Maximum, High, Medium, and Low. Each profile provides a basic security posture, ranging from the most secure to the least secure, which enables 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 choose, 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-security profiles, however, you can’t change some settings at all or they have restricted ranges of values.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>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.</td>
</tr>
<tr>
<td>High</td>
<td>Configures the system with most security controls enabled, but doesn’t mandate the use of some controls that are mandated in the Maximum profile. You can’t change some configuration settings in this profile; other settings have restricted ranges of values. This profile is most appropriate for enterprise deployments that demand high security.</td>
</tr>
<tr>
<td>Medium</td>
<td>Configures the system with some of the basic security controls enabled, but not all. You can change most settings in this profile.</td>
</tr>
<tr>
<td>Low</td>
<td>Configures the system with no mandated security controls, although you can enable all controls as needed. This is the default profile.</td>
</tr>
</tbody>
</table>

3. To change the profile setting, select the **Security Profile** you want to use.
   
   You can increase or decrease the level of security.

4. Follow the prompts in the Security Profile Change wizard.

### Maximum Security Profile Requires Default Value Changes

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

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

### Managing System Access

You can control how users and administrators access the system.

You can set up local and external authentication for the following system interfaces:

- Local interface
- System web interface
- Command-line API (external authentication is available only when accessing the API using SSH)
Enable External Authentication

You can set up external authentication through Active Directory for your system. The system can map only one Active Directory group to a given role.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Active Directory External Authentication</td>
<td>Specifies whether to authenticate users with the Active Directory server. When you enable Active Directory authentication, users can log in to the system with their network credentials using this format: domain\user. With this format, users can have accounts on multiple domains.</td>
</tr>
<tr>
<td>Active Directory Server Address</td>
<td>Specifies the Active Directory server’s FQDN or IP address. If you are using subdomains, append port number 3268 as follows: ad.domain.com:3268. You can alternatively use RealPresence Resource Manager as an Active Directory server and enter its address here.</td>
</tr>
<tr>
<td></td>
<td>If you enable Always Validate Peer Certificates from Server on the Certificates page, make sure this value matches what is in the Active Directory server certificate. For example, if you enter the Active Directory server IP address here, but the certificate only has the server’s FQDN, external authentication fails.</td>
</tr>
<tr>
<td>Active Directory Admin Group</td>
<td>Specifies the Active Directory group whose members should have administrator access to the system. This name must exactly match the name in the Active Directory server for successful authentication.</td>
</tr>
<tr>
<td>Active Directory User Group</td>
<td>Specifies the Active Directory group whose members should have user access to the system. This name must exactly match the name in the Active Directory server for successful authentication.</td>
</tr>
</tbody>
</table>

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

Use the local system administrator credentials to pair the system with a touch device, such as the RealPresence Touch.
Configure Local Access

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

Passwords for logging in to the system are case sensitive and can’t contain more than 40 characters.

Procedure

1. In the system web interface, go to Admin Settings > Security > Local Accounts > Login Credentials.
2. Configure the following settings. The order in which the settings are displayed differs between the interfaces.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin ID</td>
<td>The local administrator account name (default is admin). It is not case sensitive.</td>
</tr>
<tr>
<td>Admin Room Password</td>
<td>If you set this option, you must enter this password to change administrator settings in the local interface. The default password is the serial number listed in System Details and on the back of the device.</td>
</tr>
<tr>
<td>Use Room Password for Remote Access</td>
<td>Specifies if the administrator or user Room Password used to log in locally is also used for remote logins. This setting is enabled by default.</td>
</tr>
<tr>
<td>Admin Remote Access Password</td>
<td>If you set this option, you must enter this password to access the system through the system web interface or command-line API (SSH or telnet). This password lets you perform device management tasks, such as updating the system's software.</td>
</tr>
<tr>
<td>Require User Login for System Access</td>
<td>If you set this option, you must log in to use the local interface (including when the system comes out of sleep mode or completes its startup process). This setting is not supported on Polycom touch devices.</td>
</tr>
<tr>
<td>User ID</td>
<td>The user account name (default is user). It is not case sensitive.</td>
</tr>
<tr>
<td>User Room Password</td>
<td>If you set this option, you must enter this password to log in to the local interface.</td>
</tr>
<tr>
<td>User Remote Access Password</td>
<td>If you set this option, you must enter this password to log in through the system web interface or API (SSH or telnet). This password gives you limited functionality in the system web interface and access to only a subset of the API commands.</td>
</tr>
</tbody>
</table>
Configure Remote Access

You can remotely configure, manage, and monitor your system from its system web interface or using the API. (You can also perform these actions with RealPresence Resource Manager or SNMP [monitoring only].)

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

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

**Procedure**

1. In the system web interface, select **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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Network Intrusion Detection System (NIDS)</strong></td>
<td>When you enable this setting, the system creates security log entries when it detects a possible network intrusion. (This setting is enabled or disabled by default based on the security profile, but you can change it.)</td>
</tr>
<tr>
<td><strong>Enable Web Access</strong></td>
<td>Specifies whether you can access the system using the system web interface.</td>
</tr>
<tr>
<td><strong>Allow Access to User Settings</strong></td>
<td>Specifies whether users can access the <strong>User Settings</strong> screen through the local interface.</td>
</tr>
<tr>
<td><strong>Restrict to HTTPS</strong></td>
<td>Specifies that you can access the system web interface only over port 443. Enabling this setting closes access through port 80 (HTTP).</td>
</tr>
<tr>
<td><strong>Web Access Port (HTTP)</strong></td>
<td>Specifies the port to use when accessing the system web interface over HTTP. If you change the default (port 80), specify port 1025 or higher and make sure it is not already in use. You must include the port number with the IP address when you use the system web interface to access the system. (This setting is unavailable if <strong>Restrict to HTTPS</strong> is enabled.)</td>
</tr>
<tr>
<td><strong>Enable Telnet Access</strong></td>
<td>Specifies whether you can access the system using telnet.</td>
</tr>
</tbody>
</table>
## Setting | Description
--- | ---
**API Port** | Specifies whether to use port 23 or 24 for API access. If you select port 23, the diagnostics port changes to port 24.
**Enable SSH Access** | Specifies whether you can access the system using SSH.
**Enable Diagnostics Port Idle Session Timeout** | Specifies whether to allow the diagnostics port to time out at the configured time interval or not. You set the timeout at **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. You set the timeout at **Idle Session Timeout in Minutes**.
**Enable SNMP Access** | Specifies whether to allow SNMP access.
**Allow Video Display on Web** (local interface only) | Specifies whether you can use the system web interface to view the room where the system is located, or video of calls in which the system participates.
**Note:** This feature activates both near site and far site video displays in Web Director.
**Lock Port after Failed Logins** | Temporarily locks the login port after a configurable number of unsuccessful login attempts have been made.
**Enable Whitelist** | Specifies whether to enable a whitelist.
**Idle Session Timeout in Minutes** | Specifies the number of minutes a session can be idle before it times out.
**Maximum Number of Active Sessions** (system web interface only) | Specifies the maximum number of users logged in through the system web interface or command-line API (SSH or telnet).

## Local Accounts
There are two types of local accounts for accessing the RealPresence Centro system: one for the user (by default named **user**) and another for the administrator (by default named **admin**). Administrators can configure the system and also perform user activities, such as placing calls.

The system stores local account IDs and passwords.

### Configure Password Policy Settings
You can specify requirements for administrator, user, meeting, remote access, and SNMP passwords for your system.

Polycom strongly recommends that you create an administrator password for your system.
## Procedure

1. In the system web interface, go to **Admin Settings > Security > Local Accounts > Password Requirements**.
2. Configure the following settings for **Admin Room, User Room, Meeting, Remote Access**, or **SNMP** passwords.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>The minimum number of characters required for a valid password.</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>The minimum number of lowercase letters required for a valid password.</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>The minimum number of uppercase letters required for a valid password.</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>The minimum number of numerals required for a valid password.</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>The minimum number of special characters required for a valid password. Supported characters include: @ - _ ! ; $ , / &amp; . # *</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>The number of most recent passwords that you can’t reuse. If you set this to Off, all previous passwords are valid.</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>The minimum number of days before the password can change.</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>The maximum number of days before the password must change.</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>The number of characters that must be different or change position in a new password. For example, if you set this to 3,123abc can change to 345cde but not to 234bcd.</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>The maximum number of consecutive repeated characters allowed in a password. For example, if you set this to 3,aaa123 is a valid password but aaaa123 is not.</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Specifies how many days in advance a warning displays indicating that the password expires soon (if you set a maximum password age).</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Specifies whether the associated ID or its reverse can be part of a password. If you enable this setting and the ID is admin, passwords admin and ninda are allowed.</td>
</tr>
</tbody>
</table>

3. **Click Save.**

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

**Preventing Account Unauthorized System Access**

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

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

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

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

- Local interface
- Web interface
- Telnet interface

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

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

**Scenario 1 - Admin account locked due to excessive failed logins**

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

**Scenario 2 - Successful login resets the failed login attempts counter**

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

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

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

**Configure Account Lockout**

You can specify account lockout controls to prevent unauthorized access to your system.

**Procedure**

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lock Admin/User Account after Failed Logins</strong></td>
<td>Specifies the number of failed login attempts allowed before the system locks the account. You can turn this setting <strong>Off</strong>.</td>
</tr>
<tr>
<td><strong>Admin/User Account Lock Duration</strong></td>
<td>Specifies the amount of time an account is locked because of failed login attempts. After this period expires, the system resets the failed login attempts counter to zero, and users can again log in with that account.</td>
</tr>
</tbody>
</table>
| **Reset Admin/User Account Lock Counter After** | Determines how many hours the failed login window lasts. The window is a period of time starting with the first failed login attempt and during which the system counts subsequent failed attempts against the number allowed.  

The counter resets to zero at the end of the window (if the account is not locked because of failed attempts) and after a successful login. |

**Enable Access to User Settings**

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

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

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

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

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

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

If the following conditions are met, the ability to show icons is automatically enabled and read only:
• Speed Dial is disabled in the Admin Settings > General Settings > Home Screen Settings.
• The Calendar is not displayed because the system is not connected to the Microsoft Exchange Server.
• Remote access through the web, telnet, and SNMP are disabled in Security > Global Security > Access.

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

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Packet Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY: NIDS/unknown_tcp</td>
<td>Packet that attempts to connect or probe a closed TCP port</td>
</tr>
<tr>
<td>SECURITY: NIDS/unknown_udp</td>
<td>Packet that probes a closed UDP port</td>
</tr>
<tr>
<td>SECURITY: NIDS/invalid_tcp</td>
<td>TCP packet in an invalid state</td>
</tr>
<tr>
<td>SECURITY: NIDS/invalid_icmp</td>
<td>ICMP or ICMPv6 packet in an invalid state</td>
</tr>
<tr>
<td>SECURITY: NIDS/unknown</td>
<td>Packet with an unknown protocol number in the IP header</td>
</tr>
<tr>
<td>SECURITY: NIDS/flood</td>
<td>Stream of ICMP or ICMPv6 ping requests or TCP connections to an opened TCP port</td>
</tr>
</tbody>
</table>
Following the message prefix, the security log entry includes the timestamp and the IP, TCP, UDP, ICMP, or ICMPv6 headers. For example, the following security log entry shows an “unknown_udp” intrusion:

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

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

**View Connections to Your System in a Sessions List**

You can see a list of current connections to your system. You can find the following information in the list:

- Type of connection (for example, web)
- ID associated with the session (for example, admin or user)
- Remote address (IP addresses of the hosts accessing your system)

**Procedure**

1. In the system web interface, go to **Diagnostics**.
2. Go to **System > Sessions**.

**Secure API Access**

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

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

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

**Enable Secure API Access**

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

**Procedure**

- Do one of the following
  - In the system web interface, go to **Admin Settings > Security > Global Security > Access** and enable the **Enable Legacy API Over SSH** setting.
  - In a system API session, enter `sshenable true`. 
Disable Secure API Access

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

Procedure

» Do one of the following:
  • In the system web interface of the system, select Admin Settings > Security > Global Security > Access and disable the Enable Legacy API Over SSH setting.
  • In a system API session, enter sshenable false.

Access the API with SSH

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

To access the API with SSH:

Procedure

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

Port Lockout

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

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

A system web interface is configured with these settings:

• Admin Settings > Security > Global Security > Authentication > Enable Active Directory External Authentication is enabled, a valid Active Directory Server Address is configured, as are both the Active Directory Admin Group and Active Directory User Group settings.
• Admin Settings > Security > Global Security > Access > Enable Legacy API Over SSH, Lock SSH Port after Failed Logins is set to 3, SSH Port Lock Duration is set to 1 Minute, and Reset SSH Port Lock Counter After is set to 1 Hour.
• Admin Settings > Security > Global Security > Access > Lock Port after Failed Logins is set to 4.
Scenario 1: Web interface locked due to excessive failed logins

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

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

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

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

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

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

Configure Port Lockout Settings

You can limit the number of failed login attempts to your system interface to protect against brute-force attacks.

If the number of failed login attempts during this window doesn’t reach the maximum number allowed, the system sets the failed login attempts counter to zero at the end of this window.

The telnet port is locked regardless of how you configure it. A telnet session disconnects after five failed login attempts. If a new session starts, the system allows another five.

Procedure

1. In the system web interface, select Admin Settings > Security > Global Security > Access. The SSH port settings are visible only when Enable Legacy API Over SSH is enabled.
2. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock SSH Port after Failed Logins</td>
<td>The number of failed login attempts allowed before the SSH/Telnet interface locks. You can set this to Off.</td>
</tr>
</tbody>
</table>
**Setting** | **Description**
--- | ---
SSH Port Lock Duration | Specifies the amount of time that the web interface remains locked due to failed login attempts. When this period expires, the failed login attempts counter resets and you can try to log in again.
Reset SSH Port Lock Counter After | Specifies the number of hours, starting with the first failed login attempt, during which subsequent failed login attempts are counted against the maximum number allowed (Lock SSH Port after Failed Logins). The counter resets when the set period of time expires or a user successfully logs in.
Lock Port after Failed Logins | The number of failed login attempts allowed before the web interface locks. You can set this to Off.

**Whitelisting**

Whitelisting allows access to your RealPresence Centro system web interface and SNMP ports only to IP addresses you specify.

A whitelist supports up to 30 addresses (including IPv4 and IPv6 formats) and can only be configured in the system web interface.

**Note:** If your IP addresses are dynamically assigned, make sure the whitelist is updated so those hosts can connect to your system.

**Enable a Whitelist**

Add or remove IP addresses on your system whitelist.

**Procedure**

1. In the system web interface, select **Admin Settings > Security > Global Security > Access**.
2. Select **Enable Whitelist**, then **Edit Whitelist**.

**Add IP Addresses to a Whitelist**

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

**Procedure**

1. Click the **Edit Whitelist** link.
2. Select address type IPv4 or IPv6.
3. In the address text field, enter the IP address of the system you want to allow.
   - Follow the format suggested by the address type you selected. Select **Add**.
   - Repeat this step for all the IP addresses you want to add. You can add web server and SNMP addresses.
   - If you entered an address in error, highlight the address in the list and select **Clear**.
IPv4 Address Formats
The whitelist configuration requires a single IP address, a range of addresses, or an IP and netmask. (The netmask represents the number of valid bits of the IPv4 address to use.)

Here are valid IPv4 formats for your RealPresence Centro system:
- 10.12.128.7
- 172.26.16.0/24

IPv6 Address Formats
For IPv6 addresses, you can use a Classless Inter-Domain Routing (CIDR) notation to represent a range of IP addresses.

Here are valid IPv6 formats for your RealPresence Centro system:
- ::1
- 2001:db8:abc:1024.2.3
- 2001:db8::/48
- 2001:db8:abcd:0012::/64
- 2001:0db8:85a3:0000:0000:1234:0abc:cdef

Encryption
AES is standard on RealPresence Centro systems. When enabled, your system automatically encrypts calls with other systems using AES.

A locked padlock icon displays on the connected monitor(s) when a call is encrypted. If a call is unencrypted, you see an unlocked padlock. The padlock may not accurately indicate encryption status if the call is cascaded or includes an audio-only endpoint. To avoid security ambiguity, participants can verbally communicate the state of their padlock icon at the beginning of a call.

The following AES cryptographic algorithms ensure flexibility when negotiating secure media transport:
- H.323 (per H.235.6)
  - AES-CBC-128 / DH-1024
  - AES-CBC-256 / DH-2048
- SIP (per RFCs 3711, 4568, 6188)
  - AES_CM_128_HMAC_SHA1_32
  - AES_CM_128_HMAC_SHA1_80
  - AES_CM_256_HMAC_SHA1_32
  - AES_CM_256_HMAC_SHA1_80

Configure Encryption
You can configure encryption settings on your system.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require AES Encryption for Calls</td>
<td>Specifies how to encrypt calls with other participant systems that support AES encryption.</td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>When set, the system uses only FIPS 140-2-approved cryptographic modules. Cipher suites and protocols not approved by FIPS 140-2 are disabled.</td>
</tr>
<tr>
<td>Disable TLS v1.0</td>
<td>Disables the TLS v1.0 application. By default, they system enables Disable TLS v1.0 in Maximum, High, and Medium Security Profiles, which means that TLS v1.0 is disabled. The default for the Low Security Profile is disabled, which means that the system enables TLS v1.0.</td>
</tr>
</tbody>
</table>

**Configuring Encryption Settings for SVC Calls**

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

- Set the transport protocol.
- Set AES encryption.

**Set the Transport Protocol for SVC Calls**

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

**Procedure**

1. In the system web interface, go to Admin Settings > Network > IP Network.
2. Click SIP to expand the section.
3. In the Transport Protocol list, select TLS.
4. Click Save.
Set Up AES Encryption for SVC Calls

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

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

Verify H.323 Media Encryption

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

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

Procedure
1. Establish an encrypted H.323 call between two sites.
2. At each site, locate the Call Statistics information on the Place a Call screen of the system web interface.
   The check code also displays under Diagnostics > System > Call Statistics in the Transmit column of the Call Encryption section.
3. Verbally verify that the code is the same at both sites.
4. Do one of the following:
   • If the codes match, the call is secure. Proceed with the call.
   • If the codes do not match, then there is a possibility that the key exchange is compromised. Hang up the call. Next, check the network path from the local system to the far-end system to determine if the systems are experiencing a Man in the Middle attack. This occurs when a foreign device tricks the local system into creating an encryption key using information from the imposter. Then, the imposter can decode the data sent by the local system and eavesdrop on the call.

Firewall/NAT Traversal

You can configure your system for firewall or network address translation (NAT) traversal using the H.460.18 and H.460.19 standards.

The following illustration shows how a service provider might provide H.460 firewall traversal between two physical locations. In this example, the Polycom Video Border Proxy (VBP) device is on the edge of the service provider’s network, facilitating IP calls between systems behind different firewalls.
Basic Firewall/NAT Traversal

Your RealPresence Centro system can connect to SIP-based Polycom solutions using the Acme Packet Net-Net family of session border controllers (SBCs).

A system connects to the Acme Packet Net-Net SBC as a remote enterprise endpoint, which is registered to the enterprise's SIP infrastructure and connects to an internal enterprise endpoint through the enterprise firewall.

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

Polycom systems also provide full mutual TLS support for SIP and XMPP Presence connections. Full mutual TLS support gives administrators the ability to identify and authenticate devices attempting to join conferences from outside the network.
Configure the H.460 Firewall/NAT Traversal

You can enable and configure H.460 firewall or NAT traversal on your RealPresence Centro system. Make sure you register your system with a network device that supports H.460.18 and H.460.19 standards (for example, a RealPresence Access Director system or a Polycom VBP device).

Procedure

1. Enable firewall traversal on the system.
   - In the system web interface, go to Admin Settings > Network > IP Network > Firewall.
   - Select Enable H.460 Firewall Traversal.

2. Verify the firewalls that you traverse allow your system to use outbound TCP and UDP connections.
   - Firewalls with a stricter rule set must allow the system to use at least the following outbound TCP and UDP ports: 1720 (TCP), 14085-15084 (TCP), 1719 (UDP), and 16386-25386 (UDP).
   - Firewalls must allow inbound traffic to the TCP and UDP ports used for outbound traffic.

3. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed Ports</td>
<td>Defines which TCP and UDP ports your system uses for firewall traversal. Enable this option if your firewall isn’t H.323 compatible. The system assigns a port range starting with the TCP and UDP ports you specify (port 3230 is where the range begins by default). Note: For the fixed ports you configure, you must open the corresponding ports on your firewall. For H.323, open TCP port 1720. For SIP, open UDP port 5060, TCP 5060, or TCP 5061 depending on if you’re using UDP, TCP, or TLS, respectively, as the SIP transport protocol. Disable this option if your firewall is H.323 compatible or the system isn’t behind a firewall.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>The starting value for the range of TCP and UDP ports the system uses. The system automatically configures the range based on the beginning value you set here.</td>
</tr>
<tr>
<td>UDP Ports</td>
<td>To allow H.323 traffic, you need two TCP and eight UDP ports per connection. You must also open TCP port 1720 on the firewall.</td>
</tr>
<tr>
<td></td>
<td>To allow SIP traffic, you need TCP port 5060 and eight UDP ports per connection.</td>
</tr>
<tr>
<td></td>
<td><strong>UDP port range:</strong> Because systems support ICE, the range of fixed UDP ports is 32, 62, and 82 for RealPresence Group Series 300/310, 500, and 700 systems, respectively. 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 3230-3236, the second call 3236-3242, the third call 3242-3248, and so on.</td>
</tr>
<tr>
<td></td>
<td><strong>Fixed ports range and filters:</strong> You might notice that the source port of a SIP signaling message is not in the fixed ports range. When your firewall is filtering on source ports, in the system web interface, go to the SIP page and enable <strong>Force Connection Reuse</strong>. When enabled, the system uses port 5060 and 5061 for the source and destination port (these must be open on the firewall).</td>
</tr>
<tr>
<td>NAT Configuration</td>
<td>Specifies if the system automatically determines the NAT public (WAN) address.</td>
</tr>
<tr>
<td></td>
<td>• If the system isn’t behind a NAT or is connected to the network through a VPN, set this option to <strong>Off</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the system is behind a NAT that allows HTTP traffic, set this option to <strong>Auto</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the system is behind a NAT that doesn’t allow HTTP traffic, set this option to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>NAT Public (WAN) Address</td>
<td>The address callers from outside the LAN use to call your system. If you configured the NAT manually, enter the NAT public address here.</td>
</tr>
<tr>
<td></td>
<td>You can configure this option only when you set <strong>NAT Configuration</strong> to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>NAT is H.323 Compatible</td>
<td>Identifies whether the system is behind a NAT that can translate H.323 traffic.</td>
</tr>
<tr>
<td></td>
<td>This option is available only when you set <strong>NAT Configuration</strong> to <strong>Auto</strong> or <strong>Manual</strong>.</td>
</tr>
</tbody>
</table>
Setting | Description
--- | ---
Address Displayed in Global Directory | Choose whether to display the system's public or private address in the global directory. This option is available only when you set NAT Configuration to Auto or Manual.
Enable SIP Keep-Alive Messages | Specifies whether to regularly transmit keep-alive messages on the SIP signaling channel and on RTP sessions part of SIP calls. Keep-alive messages maintain connections through firewall/NAT devices that are often used at network edges. If your system is in an Avaya SIP environment, Polycom recommends that you disable this setting to enable calls to fully connect.

Real-time media streams often use UDP for their speeds. If your system is behind a firewall that restricts access to UDP ports, however, you can configure your system for only TCP connections.

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

Security Certificates

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

Systems can use certificates to authenticate network connections to and from the system. 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. Polycom supports the following certificate file formats: .pem,.crt/.cert.

How Certificates are Used

RealPresence Centro systems can generate CSRs to send to a certificate authority (CA). (A CA is a trusted entity that officially issues, or signs, digital certificates.) Once signed by the CA, you can install the certificate on the system for its TLS connections.

Systems support, and typically require, two certificates when used in an environment with fully deployed PKI:

- Server certificate: The system's web server presents this certificate after receiving connection requests from browsers attempting to connect to the system's web interface.
- Client certificate: The system presents this to authenticate its identity while trying to connect to a 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 in an environment that does not have a fully deployed PKI, you do not need to create and install these certificates because systems automatically generate self-signed certificates to establish secure TLS connections. When a full PKI is deployed, however, self-signed certificates are not trusted and CA-signed certificates must be used. The following sections describe how to generate and use certificates by using the system web interface.

**Certificate Signing Requests**

The RealPresence Centro system lets you install one client and one server certificate so that network peers can identify the system. Each of these certificates require a CSR. Also known as an unsigned certificate, a CSR must be submitted to a CA to be signed, after which the certificate can be installed on your system.

**Certificate Signing Request Requirements**

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

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

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

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

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

**Create a Certificate Signing Request**

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

**Procedure**

1. In the system web interface, go to Admin Settings > Security > Certificates > Certificate Options.
2. Click Create for the type of CSR you want to create, Signing Request Server or Signing Request Client.
The procedure is the same for server and client CSRs.

3. Configure these settings on the Create Signing Request screen and click **Create**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hash Algorithm</strong></td>
<td>Specifies the hash algorithm for the CSR. You can select SHA-256 or keep the default SHA-1.</td>
</tr>
<tr>
<td><strong>Common Name (CN)</strong></td>
<td>Specifies the name that the system assigns to the CSR. Use the following guidelines when configuring the Common Name:</td>
</tr>
<tr>
<td></td>
<td>• For systems registered in DNS, use the FQDN of the system.</td>
</tr>
<tr>
<td></td>
<td>• For systems not registered in DNS, use the IP address of the system. Maximum Characters: 64; truncated if necessary. Default is blank</td>
</tr>
<tr>
<td><strong>Organizational Unit (OU)</strong></td>
<td>Specifies the unit of business defined by your organization. Default is blank. Maximum Characters: 64</td>
</tr>
<tr>
<td></td>
<td>Note: The system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.</td>
</tr>
<tr>
<td><strong>Organization (O)</strong></td>
<td>Specifies your organization’s name. Default is blank. Maximum Characters: 64</td>
</tr>
<tr>
<td><strong>City or Locality (L)</strong></td>
<td>Specifies the city where your organization is located. Default is blank. Maximum Characters: 128</td>
</tr>
<tr>
<td><strong>State or Province (ST)</strong></td>
<td>Specifies the state or province where your organization is located. Default is blank. Maximum Characters: 128</td>
</tr>
<tr>
<td><strong>Country (C)</strong></td>
<td>Displays the country selected in <strong>Admin Settings &gt; General Settings &gt; My Information</strong>. You can’t edit this field.</td>
</tr>
<tr>
<td><strong>SAN: FQDN</strong></td>
<td>Specifies the FQDN assigned to the system. This is the same as the <strong>Common Name (CN)</strong>, but it isn’t truncated. Default is blank. Maximum Characters: 253</td>
</tr>
<tr>
<td><strong>SAN: Additional Name</strong></td>
<td>Specifies an additional name. Default is blank. Maximum Characters: 253</td>
</tr>
<tr>
<td><strong>SAN: IPv4 Address</strong></td>
<td>Default is the IPv4 address of the system. Maximum Characters: 15</td>
</tr>
<tr>
<td><strong>SAN: IPv4 Address (DNS)</strong></td>
<td>Default is the IPv4 address of system. This field provides the IPv4 address in ASCII format, which is sometimes needed for Microsoft server interoperability. Maximum Characters: 15</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SAN: IPv6 Global Address</td>
<td>Default is the IPv6 Global Address of the system. Maximum Characters: 40</td>
</tr>
<tr>
<td>SAN: IPv6 Site Local Address</td>
<td>Default is the IPv6 Site Local Address of the system. Maximum Characters: 40</td>
</tr>
<tr>
<td>SAN: IPv6 Link Local Address</td>
<td>Default is the IPv6 Link Local Address of the system. Maximum Characters: 40</td>
</tr>
</tbody>
</table>

A message indicating that the CSR is 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 a CSR is generated, get it signed and installed on your system before creating another. For example, if you generate a client CSR and then, prior to having it signed and installed on the system, another client CSR is generated, the system discards and invalidates the previous CSR, and any attempt to install a signed version of it results in an error.

### RealPresence Server Address Configuration in PKI-enabled Environments

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

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

### Enable PKI Certificates

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

#### Procedure

1. On the system web interface, go to **Admin Settings > Network > LAN Properties > LAN Options**.
2. At **Host Name**, use the same name that the RealPresence Resource Manager uses to provision the system. This name must be the same so that certificate signing requests (CSRs) generated during certificate installation have the correct host name information.
Configure Certificate Validation Settings

Certificates are authorized externally when they are signed by the CA. The certificates can be automatically validated when they are used to establish an authenticated network connection. To perform this validation, the 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 accesses the system web interface, the system is the server and the web browser is the client application. In other situations, such as when the system connects to LDAP directory services, the system is the client and the LDAP directory server is the server.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Peer Certificate Chain Depth</td>
<td>Specifies how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host when a network connection is being established between the two systems.</td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Server</td>
<td>Controls whether the system requires a browser to present a valid certificate when it tries to connect to the system web interface.</td>
</tr>
<tr>
<td>Installed Certificates</td>
<td>Allows the administrator to either view installed certificates or to add a new certificate.</td>
</tr>
<tr>
<td>Signing Request Server</td>
<td>Allows the administrator to create a new server request certificate.</td>
</tr>
<tr>
<td>Signing Request Client</td>
<td>Allows the administrator to create a new client request certificate.</td>
</tr>
</tbody>
</table>

Install Certificates

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

Procedure

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

Your system accepts the following certificate file formats: .pem, .crt/.cert. You might be installing a client or server certificate that has been signed by a CA after having been previously generated as a CSR, or installing a CA certificate needed by the system to validate a certificate it receives from another system.
3. Click **Open**.

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

You can select a certificate in the list to view its contents. You can also remove a certificate from the list by clicking **Remove**.

4. If needed, click **Close** to close the certificate section of the screen.

5. Click **Save**.

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

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

---

**Certificate Revocation**

During certificate validation, your RealPresence Centro system checks whether certificates used for secure communications are revoked by their issuing CAs.

Your system can check certificate revocation status with one of the following standard methods:

- **Certificate Revocation List (CRL):** File containing a list of certificates revoked by their issuing CA. You must manually upload CRLs to your system.

- **Online Certificate Status Protocol (OCSP):** Your system contacts an OCSP responder, a web server that provides revocation status through a query/response exchange.

**Configure the CRL Method**

Use the CRL method for revocation checking.

**Procedure**

1. In the system web interface, go to **Admin Settings > Security > Certificates > Revocation**.
2. Configure the following settings and select **Save**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocation Method</td>
<td>To use the CRL revocation method, select <strong>CRL</strong>.</td>
</tr>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>When enabled, a certificate in the chain of trust validates without a revocation check if no corresponding CRL from the issuing CA is installed.</td>
</tr>
<tr>
<td>Add CRL</td>
<td>Browse for and select a CRL to install.</td>
</tr>
</tbody>
</table>

3. View automatically and manually downloaded CRLs on the page. Make sure to install CRLs from each CA that issued the certificates on your system.
4. Optional: To delete a CRL from the list, select **Remove**.
Remove a Certificate and CRL

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

Procedure

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

   The system restarts after deleting all installed certificates and CRLs.

Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol (SCEP) is a service that automatically requests and renews certificates for large deployments of endpoints and software clients.

The SCEP service triggers when you boot up the system, unplug and replug the LAN, or enable the service in the web user interface. The system checks the system’s certificate data to obtain digital certificates based on the following criteria:

- If the certificate doesn’t exist, the SCEP service initiates the enrollment process.
- If the certificate exists, the SCEP service verifies the renewal and expiration dates and does one of the following:

<table>
<thead>
<tr>
<th>If the current date is...</th>
<th>The service...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before the renewal date</td>
<td>Looks for a time thread and creates one if none exist.</td>
</tr>
<tr>
<td>On or after the renewal date but on or before the expiration date</td>
<td>Initiates the renewal process.</td>
</tr>
<tr>
<td>After the expiration date</td>
<td>Removes the certificate using a system module and initiates the enrollment process.</td>
</tr>
</tbody>
</table>

Note: You can configure the renewal date in the SCEP settings.

Note the following information regarding SCEP:

- When the SCEP installs a new certificate in a system, it ignores the existing manually installed SCEP certificate.
- Update the challenge password manually.
- The SCEP server communicates only through HTTP, and the system only supports one SCEP server at a time.
- The maximum key size supported for the RSA key is 2048 bit.
- You can also configure the SCEP settings on the RealPresence Centro system through RealPresence Resource Manager.

Make sure none of the values against each parameter in SCEP settings are empty while provisioning through RealPresence Resource Manager.
**Note:** When a RealPresence Touch device is paired with RealPresence Centro system, you can view the SCEP settings for RealPresence Group Series system on RealPresence Touch device. However, you cannot edit them. When the SCEP feature is enabled on a standalone RealPresence Touch device, you can edit the settings from RealPresence Touch device.

For more information on the configuration options, refer to the Polycom RealPresence Resource Manager System Operations Guide available at Polycom Support.

### Install SCEP

If you already have an SCEP certificate installed in your system, you don’t have to disable EAP/802.1x authentication before you install SCEP. Verify your system’s certificate settings before you install the service.

**Procedure**

1. Do one of the following:
   - From the RealPresence Centro system web interface, go to **Admin Settings > Network > LAN Properties > LAN Options**.
   - From the RealPresence Touch device web interface, go to **Network Settings**.
2. Clear the Enable EAP/802.1x check box.
3. Restart the system.
4. Update your system with new software that includes SCEP.
5. Verify the SCEP certificate is installed into the system.
6. Enable EAP/802.1x authentication.

### Configure SCEP Settings

You can configure the SCEP settings from the system web interface.

**Procedure**

1. Do one of the following:
   - From the RealPresence Centrosystem web interface, go to **Admin Settings > Security > Certificates**.
   - From the RealPresence Touch device web interface, go to **Security > Certificates > Certificate Options**.
2. Select View and Update.
3. Select Enable SCEP and configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCEP URL</td>
<td>The URL of the SCEP server.</td>
</tr>
<tr>
<td>SCEP Challenge Password</td>
<td>Password configured in the SCEP server to generate a certificate.</td>
</tr>
<tr>
<td>Automatic Renewal</td>
<td>The automatic renewal period before certificates expire. You can choose the period based on the number of Days or Percentage of time left on a completed certificate.</td>
</tr>
<tr>
<td>Days</td>
<td>The number of days before expiration to renew the certificate.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Percentage</td>
<td>The percentage of the certificate that the system must validly complete to renew the certificate.</td>
</tr>
<tr>
<td>Renewal Entry Attempts</td>
<td>The number of times a certificate attempts to renew.</td>
</tr>
<tr>
<td>Enrollment Retry Attempts</td>
<td>The time interval a certificate attempts to renew.</td>
</tr>
<tr>
<td>CA Profile</td>
<td>The profile in the server set by the Admin.</td>
</tr>
<tr>
<td>Common Name</td>
<td>The system takes an email as a common name.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The unit of business as defined by your organization.</td>
</tr>
<tr>
<td>Organization</td>
<td>Your organization’s name.</td>
</tr>
<tr>
<td>City or Locality</td>
<td>The city or local area where your organization is located.</td>
</tr>
<tr>
<td>State or Province</td>
<td>The state or province where your organization is located.</td>
</tr>
<tr>
<td>Country</td>
<td>The country where your organization is located.</td>
</tr>
</tbody>
</table>

4. Select Save.

**View SCEP Certificates**

You can verify the SCEP certificates from the system web interface.

**Procedure**

1. Do one of the following:
   - From the RealPresence Centro system web interface, go to **Admin Settings > Security > Certificates**.
   - In the RealPresence Touch device web interface, go to **Security > Certificates > Certificate Options**.

2. To open the certificate section, at Installed Certificates, select **View and Update**.

**Set Up a Security Banner**

The following is an example of banner text:

>This device is the property of Polycom, Inc., and must be used in accordance with the company’s acceptable use policy.

**Procedure**

1. In the system web interface, go to **Admin Settings > Security > Security Banner**.
2. Configure these settings and click **Save**.
### Setting | Description
--- | ---
Enable Security Banner | Enable or disable the ability to display a security banner when logging in to the local interface or the system web interface.
Banner Text | • **Custom**: Lets you enter any text for the banner.  
• **DoD**: Displays a default U.S. Department of Defense security banner. You can't view or change this text on the local interface, but you can in the system web interface.
Local System Banner Text | The security banner that displays on the local interface and API (SSH or telnet). 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 to force a line break. Banner for text logins (ports 22, 23, 24).
Remote Access Banner Text | The security banner that displays on the system web interface. Enter up to 2,408 single-byte or 1,024 double-byte characters. The text wraps to the next line as you type, but you can press Enter anywhere to force a line break. This is visible only in the system web interface.

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

Remember the following points about meeting passwords:

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

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

This feature helps participants remain conscious of their meeting’s security classification when in a BroadWorks-managed call on the RealPresence Centro system.

During and throughout a call, the Visual Security Classification (VSC) provides a visual indication to the system user of the call’s 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.

Remember the following:

- 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.

Visual Security Classification is disabled by default and can be enabled with a provisioning server or in the system web interface. Before enabling this feature, do the following:

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

Enable Visual Security Classification

You can enable Visual Security Classification on your system.

Procedure

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

Enable Room and Call Monitoring

Before you can use room and call monitoring, you must enable the feature in the RealPresence Centro system local interface.
Procedure
1. In the local interface, go to Settings > Administration > Security > Remote Access.
2. To allow the room or call to be viewed remotely, enable Allow Video Display on Web.

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

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

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

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

Configure the OCSP Method
Use the OCSP method for revocation checking.

Procedure
1. In the system web interface, go to Admin Settings > Security > Certificates > Revocation.
2. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocation Method</td>
<td>To use the OCSP revocation method, select OCSP.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>When enabled, your system considers a revocation check successful if there is no response or the OCSP responder indicates a certificate’s status is unknown. Regardless of how you configure this setting, the following statements apply:</td>
</tr>
<tr>
<td></td>
<td>• If the OCSP responder indicates a known revoked status, your system treats it as a revocation check failure and doesn’t allow the connection.</td>
</tr>
<tr>
<td></td>
<td>• If the OCSP responder indicates a known good status, your system treats it as a successful revocation check and allows the connection.</td>
</tr>
<tr>
<td>Global Responder Address</td>
<td>Specifies the URI of the OCSP responder (for example, <a href="http://responder.example.com/ocsp">http://responder.example.com/ocsp</a>). The responder is used when Use Responder Specified in Certificate is disabled and sometimes even when it’s enabled. Polycom recommends that you always include a URI in this field regardless of how you configure Use Responder Specified in Certificate.</td>
</tr>
<tr>
<td>Use Responder Specified in Certificate</td>
<td>Some certificates include the OCSP responder address. When you enable this setting, your system attempts to use this address (when present) instead of the Global Responder Address you specified.</td>
</tr>
<tr>
<td></td>
<td>Note: Only HTTP URLs in a certificate’s AIA field are supported.</td>
</tr>
</tbody>
</table>
Configuring Call Settings

Topics:

- Configure Call Settings
- Setting Call Preferences for SVC
- Set Preferred Call Speeds
- Configure the Recent Calls List
- Set Call Answering Mode
- Set the Maximum Call Length
- Set a Multipoint Viewing Mode
- Enable Flashing Incoming Call Alerts
- Displaying Participant Names Continuously in a Call
- Configure System Display Name During Call

Configure Call Settings

You can configure call settings in the system web interface.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Time in Call</strong></td>
<td>Sets the maximum number of hours allowed for a call. When the maximum time expires, the system prompts the user to hang up. If the user doesn’t answer within one minute, the call automatically ends. If the user chooses to stay in the call, the system doesn’t prompt the user again.</td>
</tr>
</tbody>
</table>
| **Auto Answer Point-to-Point Video** | Specifies whether the system answers an incoming call when not in a call. Choose one of the following options:  

  - **Yes**: The system automatically answers incoming point-to-point calls.  
  - **No**: Users must answer incoming calls manually.  
  - **Do Not Disturb**: The system rejects incoming calls without notification. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Auto Answer Multipoint Video** | Specifies whether the system answers an incoming call when it is already in a call (regardless if the system has multipoint call capability). Choose one of the following options:  
  • **Yes**: The system automatically answers incoming point-to-point calls.  
  • **No**: Users must answer incoming calls manually.  
  • **Do Not Disturb**: The system rejects incoming calls without notification.                                                                 |
| **Multipoint Mode**             | Specifies the multipoint viewing mode when the system hosts a multipoint call. Choose one of the following options:  
  • **Auto**  
  • **Full Screen**  
  • **Discussion**  
  • **Presentation** |
| **Display Icons in a Call**      | Specifies whether to display onscreen graphics, including icons and help text, during calls.                                                                                                               |
| **Enable Flashing Incoming Call Notification** | Specifies whether you see an incoming call notification.                                                                                                                                                      |
| **Preferred 'Place a Call' Navigation** | Specifies the default options that display on the local interface **Place a Call** screen. Choose one of the following options:  
  • **Keypad**: Displays recently-dialed numbers and a dialpad.  
  • **Contacts**: Displays a screen for searching a directory. The multitiered directory (LDAP) root entry displays at the top of the **Contacts** list, which combines your search results and favorites.  
  • **Recent Calls**: Lists previous calls in chronological order.                                                                 |
| **Automatic Self View Control** | Specifies if the **Self View** setting displays in the local interface.  
  • If you enable **Automatic Self View Control**, the **Self View** setting isn’t available. The system automatically chooses when to display the self-view window, which depends on available display space and the display mode, among other factors.  
  • If you don’t enable **Automatic Self View Control**, the user can turn **Self View** on and off from the local interface.                                                                 |
Setting Call Preferences for SVC

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

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

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

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

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

Configure SVC Dialing Options

You can specify video and audio dialing preferences for your system.

Procedure

1. In the system web interface, go to Admin Settings > Network > Dialing Preference > Dialing Options.
2. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalable Video Coding Preference (H.264)</td>
<td>Specifies whether to use scalable or advanced video coding:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SVC then AVC</strong>: Use SVC when possible; otherwise, use AVC.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AVC Only</strong>: This setting disables SVC.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AVC then SVC</strong>: This setting doesn’t apply to Skype for Business-hosted calls, since SVC is negotiated automatically by Skype for Business Server 2015 or the Skype for Business 2015 client.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable H.239</td>
<td>Enables the use of a standards-based specification for parallel video streams (people and content). Enable this setting if you know call participants support H.239.</td>
</tr>
<tr>
<td>Enable Audio-Only Calls</td>
<td>Specifies one additional outbound audio-only call from the system. This occurs when a multipoint conference call reaches the maximum number of calls allowed for the license type.</td>
</tr>
<tr>
<td>Call Type Order</td>
<td>Specifies an order preference for video or voice calls. Select either Video then Phone, or Phone then Video. This setting is read-only if the video system has no phone connections.</td>
</tr>
</tbody>
</table>
| Video Dialing Order         | Specifies how the system places video calls to directory entries with more than one type of number. Select one of the following protocols for each preference:  
  • IP H.323  
  • SIP  
  • Gateway  
  This setting also determines how the system places video calls from the Place a Call screen when your set the call protocol to Auto or if it's unavailable. For example, if a call doesn’t connect with H.323, the system tries using SIP. |
| Audio Dialing Order         | Specifies how the system places audio calls to directory entries with more than one type of number. The system might list other connected Polycom products as a dialing order choice.  
For example, if you have a SoundStation IP 7000 connected to your system, Speakerphone would be listed.  
Select one of the following protocols for each preference:  
  • IP H.323  
  • SIP  
  • Gateway |

**Enable SVC Preference (H.264) for Calls**

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

**Procedure**

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

Enable Automatic Answering of SVC Point-to-Point Calls

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

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

Procedure

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

Set Preferred Call Speeds

When your system is configured for a Zoom environment, you need to set the preferred speed to either 1024 or 1920. The maximum speed must be set to 1920.

Polycom recommends the preferred speed as 1920 when the Group Series system is configured to a Microsoft environment.

You can configure call speeds in the system web interface.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Speed for Placed Calls</td>
<td>Determines the speeds to use for IP calls from this system when either of the following statements is true:</td>
</tr>
<tr>
<td>IP Calls</td>
<td>• A user sets the call speed to Auto on the Place a Call screen.</td>
</tr>
<tr>
<td></td>
<td>• A user places a call from the directory.</td>
</tr>
<tr>
<td></td>
<td>If the far-site system doesn’t support the selected speed, the system automatically negotiates a lower speed.</td>
</tr>
<tr>
<td></td>
<td>The SIP (TIP) Calls setting is available only when the TIP setting is enabled.</td>
</tr>
<tr>
<td>Maximum Speed for Received Calls</td>
<td>Allows you to restrict the bandwidth used when receiving IP calls.</td>
</tr>
<tr>
<td>IP Calls</td>
<td>The system doesn’t receive calls at a higher rate than the speed you set here.</td>
</tr>
</tbody>
</table>
Configure the Recent Calls List

You can display recent calls on the Place a Call page in the system web interface.

The recent calls list includes the following information:

- Name or number
- If the system placed or received the call
- Date and time

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Detail Report</td>
<td>When enabled, you can view call information on the system web interface or download it as a .csv file. When disabled, the system doesn’t write call information.</td>
</tr>
<tr>
<td>Enable Recent Calls</td>
<td>Specifies whether to show recent calls on the local interface and the system web interface.</td>
</tr>
<tr>
<td>Maximum Number to Display</td>
<td>The maximum number of calls the system displays in the recent calls list.</td>
</tr>
</tbody>
</table>

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

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

Set Call Answering Mode

You can configure how users answer calls on the system.

Procedure

1. In the system web interface, go to Admin Settings > General Settings > System Settings > Call Settings.
2. Select Auto Answer Point-to-Point Video to set the answer mode for calls with one site, or select Auto Answer Multipoint Video to set the mode for calls with two or more other sites, and then select one of the following:
   - Yes: The system automatically answers incoming calls.
   - No: Users must answer incoming calls manually.
   - Do Not Disturb: Disables the system from processing incoming calls and routing them to the user.
Set the Maximum Call Length

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

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

Set a Multipoint Viewing Mode

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

Procedure
1. In the system web interface, go to 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>The view switches between continuous presence and full screen, depending on the interaction between the sites.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Multiple sites are displayed in continuous presence. The current speaker’s image is highlighted.</td>
</tr>
<tr>
<td>Presentation</td>
<td>The speaker sees continuous presence while the other sites see the speaker in full screen on the monitor.</td>
</tr>
<tr>
<td>Full Screen</td>
<td>The site that is speaking is shown in full screen to all other sites. The current speaker sees the previous speaker.</td>
</tr>
</tbody>
</table>
Enable Flashing Incoming Call Alerts

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

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

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

Turn Off Flashing Alerts

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

Procedure
1. In the system web interface, go to Admin Settings > General Settings > System Settings > Call Settings.
2. Clear the Enable Flashing Incoming Call Notification checkbox.
3. Click Save.

Displaying Participant Names Continuously in a Call

Administrators can configure a system to display participant names throughout a conference call.

Configure Participant Name Display

You can allow participants in a multipoint call to see participant names throughout the call.

Procedure
1. In the system web interface, go to Admin Settings > General Settings > System Settings > Call Settings.
2. At Display Participant Names in Multipoint Video, select one of the following:
   • Auto: After participants join a call, their names are displayed for 10 seconds (default).
   • Always: Participant names are displayed throughout a call.
3. Select Save.
Configure System Display Name During Call

You can configure to display the system name in place of SIP address in the RealPresence Centro system web interface.

Procedure

1. In the system web interface, go to **Admin Settings > System Setting > Call Settings**.
2. Select the **Display System Name Instead of SIP Address** check box.
Registering with a Directory

Topics:

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

You can register your system with a directory to call contacts in your organization.

The system supports up to 2,000 Favorites. The following are also supported:

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

Global and Favorites groups are supported. You can create up to 200 Favorites groups. 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 that display in the Favorites group.

Enable H.323

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP H.323</td>
<td>Allows the H.323 settings to be displayed and configured.</td>
</tr>
<tr>
<td>H.323 Name</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Setting Description

#### H.323 Extension (E.164)
Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system.

Your organization's dial plan might define the extensions you can use.

#### Use Gatekeeper
Turn the gatekeeper off or make it automatic.

#### Require Authentication
Require authentication for IP H.323 connections.

#### Current Gatekeeper IP Address
The IP address for the current gatekeeper.

#### Primary Gatekeeper IP Address
The IP address for the primary gatekeeper.

### Configure the Polycom GDS
You can register your system with the Polycom Global Directory Server (GDS).

Enable H.323 on your system before you register it with this directory server.

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Address</strong></td>
<td>Specifies the IP or DNS address of the Polycom GDS.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The Polycom GDS password, if one exists.</td>
</tr>
</tbody>
</table>

### Configure the LDAP Directory Server
You can register your system with an LDAP directory server.

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Address</strong></td>
<td>Specifies the address of the LDAP directory server. When provisioned, this setting is read-only.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specifies the port for connecting with the LDAP server. When provisioned, this setting is read-only.</td>
</tr>
<tr>
<td>Base DN (Distinguished Name)</td>
<td>Specifies the top level of the LDAP directory where searches begin. When provisioned, this setting is read-only.</td>
</tr>
<tr>
<td>Multitiered Directory Default Group DN</td>
<td>Specifies the top-level group of the LDAP directory required to access its hierarchical structure. When provisioned, this setting is read-only.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the protocol for authenticating with the LDAP server: <strong>NTLM, Basic, or Anonymous.</strong></td>
</tr>
<tr>
<td>Use SSL (Secure Socket Layer)</td>
<td>When enabled, encrypts data to and from the LDAP server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name for registering with the LDAP server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the user name for registering with LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password for registering with the LDAP server.</td>
</tr>
</tbody>
</table>

**Managing Favorites Contacts and Groups**

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

The system web interface displays several types of favorites.

<table>
<thead>
<tr>
<th>Directory Server Registration</th>
<th>Types of Contacts</th>
<th>Presence State Displayed</th>
</tr>
</thead>
</table>
| LDAP with H.350 or Active Directory | • Directory entries created locally by the user.  
• References to LDAP directory entries added to Favorites by the user.  
These entries are available only if the system can successfully access the LDAP/Active Directory server. Users can delete these entries from Favorites, but they can’t edit these entries. Users can copy these entries to other Favorites and remove them from those groups. | Unknown |

Create a Favorites Contact

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

Procedure
1. In the system web interface, go to Manage Favorites.
2. Click Create New Favorite.
3. Enter the contact call information and click Save.
   ITP endpoint contact to be added as <addr1>;<addr2>;<addr3> where <addr> must be H.323 Extension(E.164) or H.323 Name or SIP address.

Create a Favorites Group

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

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

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

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

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

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

- Microsoft Internet Explorer
- Mozilla Firefox

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

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

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

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

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

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

Setting Up Speed Dial

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

The system displays Speed Dial contacts on the RealPresence Centro system’s local interface and on a paired RealPresence Touch device.

Enable Speed Dial

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

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

Add Speed Dial Contacts

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

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

Image File Requirements for Speed Dial Contacts

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

- JPEG format (.jpg or .jpeg extension)
- Image dimensions within a range of 300 to 2000 pixels (both width and height)
Upload an Image File for Speed Dial Contacts

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

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

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

Remove Speed Dial Contacts

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

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

Setting Up and Configuring Directory Servers

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

Configuring a Directory Server

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

<table>
<thead>
<tr>
<th>Supported Directory Servers</th>
<th>Authentication Protocols</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
</table>
| Microsoft Skype for Business Server 2015 | NTLM v2 only | Contact groups but not distribution lists | Might include:  
  - SIP address (SIP URI) |
### Supported Directory Servers

<table>
<thead>
<tr>
<th>Supported Directory Servers</th>
<th>Authentication Protocols</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDAP</strong></td>
<td>Any of the following:</td>
<td>Not Supported</td>
<td>Might include:</td>
</tr>
<tr>
<td>with H.350 or Active Directory</td>
<td>• NTLM v2 only</td>
<td></td>
<td>• H.323 IP address (raw IPv4 address, DNS name, H.323 dialed digits, H.323 ID, or H. 323 extension)</td>
</tr>
<tr>
<td></td>
<td>• Basic</td>
<td></td>
<td>• SIP address (SIP URI)</td>
</tr>
<tr>
<td></td>
<td>• Anonymous</td>
<td></td>
<td>• ISDN number</td>
</tr>
</tbody>
</table>

**Polycom GDS**

<table>
<thead>
<tr>
<th>Supported Directory Servers</th>
<th>Authentication Protocol</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom GDS</td>
<td>Proprietary</td>
<td>Not Supported</td>
<td>Might include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• H.323 IP address (raw IPv4 address, DNS name, or H.323 extension)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISDN number</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Supported Directory Servers</th>
<th>Authentication Protocol</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype for Business Server 2015</td>
<td>NTLM v2 only</td>
<td>Contact groups but not distribution lists</td>
<td>Might include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SIP address (SIP URI)</td>
</tr>
</tbody>
</table>

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

Topics:
- Configure General Audio Settings
- Configure Audio Input Settings
- Test StereoSurround
- Polycom Acoustic Fence
- USB and Bluetooth Headset Support

Configure General Audio Settings

You can configure audio settings in the system web interface.

Some audio settings are unavailable when you connect a SoundStructure digital mixer to your system.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sound Effects Volume</td>
<td>Sets the volume level of the ringtone and user alert tones.</td>
</tr>
<tr>
<td>Ringtone</td>
<td>Specifies the ringtone for incoming calls.</td>
</tr>
<tr>
<td>User Alert Tones</td>
<td>Specifies the tone for user alerts.</td>
</tr>
<tr>
<td>Audio Mute Auto-Answered Calls</td>
<td>Specifies whether to automatically mute incoming calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must first enable Auto Answer Point-to-Point Video or Auto Answer Multipoint Video in Call Settings to use this feature.</td>
</tr>
<tr>
<td>Enable Keyboard Noise Reduction and Polycom NoiseBlock</td>
<td>Specifies whether the system microphones mute when the system detects keyboard typing or other extraneous noises but no one is talking. NoiseBlock unmutes the system when it detects speech, regardless if there’s background noise or not.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> M-Mode is disabled when you enable this setting. If you use an external echo canceller, keyboard noise reduction is not available.</td>
</tr>
<tr>
<td>Transmission Audio Gain (dB)</td>
<td>Specifies the audio level (in decibels) that the system transmits sound. Unless otherwise advised, Polycom recommends setting this value to 0 dB.</td>
</tr>
<tr>
<td>Enable Audio Mute Reminder</td>
<td>Specifies if the system displays a notification that the microphones are muted when it detects someone speaking.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Join and Leave Tones</td>
<td>The system plays a tone when someone joins or leaves a conference call.</td>
</tr>
<tr>
<td>Note:</td>
<td>This setting is available only when you install the multipoint option key.</td>
</tr>
<tr>
<td>Enable Acoustic Fence</td>
<td>Specifies if the system uses Acoustic Fence technology.</td>
</tr>
<tr>
<td>Acoustic Fence Sensitivity</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Configure Audio Input Settings

You can configure the audio input settings for your system.

**Procedure**

1. In the system web interface, go to Admin Settings > Audio/Video/Content > Audio > Audio Input.
2. Configure the following settings and select Save.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the 3.5mm connector for line-level stereo audio input.</td>
</tr>
<tr>
<td></td>
<td>Displays embedded audio from the HDMI connector.</td>
</tr>
<tr>
<td></td>
<td>Displays the USB Headset audio level.</td>
</tr>
<tr>
<td>Audio Input Level</td>
<td>Sets the 3.5 mm audio input level. Choose a value from 0 to 10.</td>
</tr>
<tr>
<td>Associate with Video Content Ports</td>
<td>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.</td>
</tr>
<tr>
<td>Audio Input Level</td>
<td>Sets the audio input level. Choose a value from 0 to 10.</td>
</tr>
<tr>
<td>Audio Meter</td>
<td>Displays the audio level for the HDMI input port, left and right channels.</td>
</tr>
</tbody>
</table>

**Note:** Playback to ALL locations, Video Content Associated and Playback to Far Sites playback options are not supported during an AVMCU call.
3.5 mm Audio Input

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

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

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

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

Test StereoSurround

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

Procedure

1. Make sure the microphones are positioned correctly.
2. In the system web interface, go to Admin Settings > Audio/Video/Content > Audio > Audio Input.
3. Gently blow on the left and right leg of each Polycom microphone while watching the audio 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.
5. Optional: Exchange the right and left speakers if they are reversed.
6. 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 approximately 80 to 90 dBA in the middle of the room.
7. Repeat the steps above for Admin Settings > Audio/Video/Content > Audio > Audio Output.

Polycom Acoustic Fence

Polycom Acoustic Fence technology uses standard Polycom microphones to build a virtual audio boundary around one or several people.

This feature works in mono mode only. Enabling Polycom Acoustic Fence disables Polycom StereoSurround.

Polycom Acoustic Fence technology provides the following features:

- Mutes sounds outside the fence when no one is speaking inside it
- Lowers sounds outside the fence by 12 dB when someone is speaking inside it.
- Mutes speakers when they leave the fenced area

In addition to the primary microphone, you need at least one more microphone to create the fence. You can use up to three ceiling microphones with the RealPresence Centro system.
The boundary radius can be from two to several feet around the following Polycom peripheral devices:

- Table microphone
- Ceiling microphone

**Note:** Microphones connected to a Polycom Microphone IP Adapter currently don’t support Polycom Acoustic Fence technology.

For more details on Polycom Acoustic Fence technology, search the Polycom Knowledge Base for acoustic fence.

**Configure the Acoustic Fence**

You can configure your system to use Polycom Acoustic Fence technology.

**Procedure**

1. In the system web interface, go to **Admin Settings > Audio/Video/Content > Audio**.
2. In the system web interface, go to **Audio/Video > Audio > General Audio Settings**.
3. Select the **Enable Acoustic Fence** check box.
4. Set **Acoustic Fence Sensitivity** from 0 to 10, where 0 is the minimum microphone sensitivity and 10 is the maximum. Higher values increase the radius of the fence area around the primary microphone.

**USB and Bluetooth Headset Support**

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

The USB 2.0 ports support USB headsets. RealPresence Group 700 system has USB 2.0 port on the front panel and also includes a USB 3.0 port on rear panel, which does not support USB headsets.

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

Only a single headset can connect to the system at one time. Once connected, the headset is used as the primary audio input and output device for the system. So when a USB headset is plugged in, microphones, 3.5 mm audio input (in Playback Option echo cancelled mode), and speakers are all turned off; audio is heard only through the USB headset. This is similar to a headset plugged in or paired with a cell phone.

Headsets with these sampling rates are supported: 8 kHz, 16 kHz, 24 kHz, 32 kHz or 48 kHz.

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

Topics:

- Maximize HDTV Video Display
- Monitor Profiles
- Prevent Monitor Burn-In
- Adjust Brightness for Room Lighting
- Monitors with CEC
- Panoramic Video Layout for RealPresence Centro Systems
- Video Input Settings for RealPresence Centro Systems
- Configure RS-232 Serial Port Settings
- Configuring Monitor Settings
- Configure Secondary Monitors for Content

Maximize HDTV Video Display

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

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

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

Monitor Profiles

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

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

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

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

Configure Monitor Profile Settings

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

Procedure

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

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

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

**Note:** When the default profile settings of monitor 1 and monitor 2 are set to Far-Near and Content-Far-Near and the monitor 2 is turned off the profile of monitor 1 is changed to Content-Far-Near from Far-Near.

Configure Call Settings

**Prevent Monitor Burn-In**

Configure when you want your device to go to sleep after a period of inactivity.

Monitors and devices provide display settings to help prevent image burn-in. Plasma televisions can be particularly vulnerable to this problem. Refer to your monitor's documentation or manufacturer for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Ensure that static images are not displayed for long periods.
- Set the **Time before system goes to sleep** to 60 minutes or less.
- To keep the screen clear of static images during a call, disable the following settings:
  - **Display Icons in a Call:** Admin Settings > General Settings > System Settings > Call Settings
Show Time in Call: Admin Settings > General Settings > Date and Time > Time in Call

- Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.
- Consider decreasing the monitor’s sharpness, brightness, and contrast settings if they are set to their maximum values.

Procedure
1. In the system web interface, go to Admin Settings > Audio/Video/Content > Sleep.
2. For Display, select whether you want to display a black screen or no signal message.
3. For Time Before System Goes to Sleep, select how long the device can be idle before it goes to sleep.
4. Select the Enable Mic Mute in Sleep Mode check box to mute your microphones while the system is asleep.

Adjust Brightness for Room Lighting

In certain environments, bright content from displays, windows, or light fixtures can cause the cameras auto exposure setting to darken the exposure beyond what is preferred.

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

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

Monitors with CEC

You can use some Consumer Electronics Control (CEC) features with HDMI-connected monitors that support the CEC protocol.

Your system supports the following CEC commands:

- **System Standby**: When the system goes to sleep, connected monitors switch to standby mode to save power.
- **One Touch Play**: You can wake connected monitors with your system remote control.

Remember the following when enabling CEC on your system:

- If you connect a monitor with an HDMI splitter, the splitter must support CEC. Due to HDMI splitter limitations, monitors behind a 1xM (one-input multiple-output) splitter might not switch to the correct input when waking up.
- The system doesn’t respond to CEC commands from a monitor remote control.
• If a monitor is connected to two endpoints, the monitor displays the active endpoint when the other is sleeping.

CEC functionality is enabled by default on the four primary monitors of RealPresence Centro systems. Any monitors connected externally to the system must also support CEC, so that the feature can operate with the system.

**Enable CEC Controls**

You can enable CEC in the system web interface.

Make sure your monitor’s CEC settings are configured correctly (see your monitor’s documentation).

**Procedure**

1. In the system web interface, go to **Admin Settings > Audio/Video/Content > Monitors > Consumer Electronics Control**.
2. Select the **Enable Consumer Electronics Control** check box.

**Disable CEC Controls**

You can disable CEC in the system web interface.

**Procedure**

1. In the system web interface, go to **Admin Settings > Audio/Video/Content > Monitors > Consumer Electronics Control**.
2. Clear the **Enable Consumer Electronics Control** check box.

**Panoramic Video Layout for RealPresence Centro Systems**

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

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

The following figure shows the active speaker with the panoramic view of all in-room participants at the top of the screen.
Figure 1: Panoramic filmstrip and active speaker view

Video Input Settings for RealPresence Centro Systems

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

Configure Video Input Settings

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

Procedure

» Configure the following video input settings for the system.

Input 1: Panoramic Camera

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Displays the device name using the video input port (read only)</td>
</tr>
<tr>
<td>Optimized for</td>
<td>Specifies Motion or Sharpness for the video input.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Motion</strong>—This setting is for showing people or other video with motion.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sharpness</strong>—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.</td>
</tr>
<tr>
<td>Brightness</td>
<td>Specifies the adjustment for a bright background. This setting is best used in situations where the subject appears darker than the background.</td>
</tr>
</tbody>
</table>
### Setting Description

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

### Input 2: Content Camera

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Specifies the video input type as HDMI or VGA. Choose Auto to automatically select the video input type.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the default name of the video input. You can also enter your own name for the device.</td>
</tr>
<tr>
<td>Display as</td>
<td>Specifies whether the video input is to be used for People or Content.</td>
</tr>
<tr>
<td></td>
<td>The selection you make determines the available settings for the device in the embedded interface. For example, a People source has settings for PTZ and near/far camera control, but a Content source has different settings.</td>
</tr>
</tbody>
</table>
### Setting Description

**Input Format**
Specifies the source type of the device. This setting is read only unless the system does not detect the device.

**Optimized for**
Specifies [Motion](#) or [Sharpness](#) for the video input.
- **Motion**—This setting is for showing people or other video with motion.
- **Sharpness**—The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is required for HD calls between 512 kbps and 2 Mbps.

---

### Configure RS-232 Serial Port Settings

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RS-232 Mode</strong></td>
<td>Specifies the mode used for the RS-232 serial port. Available settings depend on the system model.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong>: Disables the serial port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pass Thru</strong>: 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. This option is only available in point-to-point calls.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed Caption</strong>: Receives closed captions from a dial-up modem or a stenographer machine through the RS-232 port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Camera Control</strong>: Passes data to and from a third-party camera.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Control</strong>: Receives control signals from a touch-panel control. Allows any device connected to the RS-232 port to control the system using API commands.</td>
</tr>
</tbody>
</table>
### Configuring Monitor Settings

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

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

### Configure Secondary Monitors for Content

If you have a multiple monitor setup with more than one touch monitor, and you want to use touch to control content on secondary monitors, you must configure settings on both the local and system web interfaces. The primary touch monitor is the one that you use to control the system's local interface. Secondary monitors are any additional monitors connected to the system.

The touch monitors should be HID compliant with HDMI interface only. If only one touch monitor is connected to the system, the following configuration steps are not necessary.

**Procedure**

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

4. In the system's web interface, go to Admin Settings > Audio/Video > Monitors.

5. For Monitor 1 at Enable, select Auto or Manual.
   At Monitor Profile, select Far, Then Near or Far Only.

6. For Monitor 2, at Monitor Profile, select Content Only or one of the other content profiles.
   If you have 3 monitors, follow the steps above for monitors 1 and 2 and select Far Only, Content Only, or Near Only for monitor 3.
   Now you can use the primary monitor to control the system's local interface, and a secondary monitor to show content.
Configuring a Camera or Camera Control System

Topics:

- Integrating RealPresence Group Series with Polycom EagleEye Cube HDCI
- Setting Up a Polycom EagleEye IV Camera
- Improve Camera Tracking Performance
- Polycom EagleEye Director II Camera System
- Setting Up a Polycom EagleEye Producer System
- Set Up the Polycom EagleEye Director
- Setting Up Polycom EagleEye Acoustic Camera

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

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

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

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

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

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

Integrating RealPresence Group Series with Polycom EagleEye Cube HDCI

The Polycom EagleEye Cube is an HDCI camera designed to work with RealPresence Group Series systems.

The EagleEye Cube HDCI camera has 1080p 60Hz video transmission, focus distance of 0.5 to 6 meters as fixed focus and 5x digital zoom with pan and tilt capabilities suitable for small and medium meeting
spaces. You can use the remote control or the RealPresence Group Series system web interface to configure the EagleEye Cube HDCI camera.

**Position the EagleEye Cube HDCI Camera**

Set the EagleEye Cube HDCI camera so the line of sight hits in the middle of the room (or wherever it needs to go).

- Make sure the EagleEye Cube HDCI camera is on a mounting bracket.
  - The camera’s viewing angle is approximately 37 degrees above and 37 degrees below its direct line of sight.
- For the optimal performance of the camera system faces detection feature, ensure ample lighting on face of participants and minimal backlighting.

**LED Indicators**

LED indicators display when you power on the EagleEye Cube HDCI camera and indicate system behaviors.

**Polycom EagleEye Cube LED Indicators and Status**

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>LED Position</th>
<th>System Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking Amber</td>
<td>All</td>
<td>Updating camera firmware</td>
</tr>
<tr>
<td>Amber</td>
<td>Center</td>
<td>Standby/Asleep</td>
</tr>
<tr>
<td>White</td>
<td>Alternate</td>
<td>Booting up camera</td>
</tr>
<tr>
<td>Red</td>
<td>Center</td>
<td>Microphone muted</td>
</tr>
<tr>
<td>White</td>
<td>One LED (position depends on the speaker)</td>
<td>System isn't in a call and active speaker tracking is on</td>
</tr>
</tbody>
</table>

**Configure Camera Settings**

You can configure Polycom EagleEye Cube HDCI settings using a RealPresence Group Series system.

**Procedure**

1. In the system web interface of the RealPresence Group Series system, go to **Admin Settings > Audio/Video > Video Inputs > General Camera Settings**.
2. Select the input the Polycom EagleEye Cube camera uses.

**Camera Tracking**

The Polycom EagleEye Cube HDCI camera detects the people in the room and provides group framing during a conference. EagleEye Cube HDCI detects the people in the room and sets up group 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.
Change Camera Tracking Settings
You can change camera tracking settings in the system web interface.

1. In the RealPresence Centro system web interface, go to Admin Settings > Audio/Video > Video Inputs > General Camera Settings, select the input used by the Polycom EagleEye Cube HDCI.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Mode</td>
<td>Specifies the tracking mode:</td>
</tr>
<tr>
<td></td>
<td><strong>Frame Speaker</strong> - This is the default setting. During a conference, this</td>
</tr>
<tr>
<td></td>
<td>mode frames the active speaker, then when someone else starts speaking, the</td>
</tr>
<tr>
<td></td>
<td>camera view changes to frame the new speaker. Note that when the tracking</td>
</tr>
<tr>
<td></td>
<td>mode is set to Frame Speaker and the local microphone is muted, the camera</td>
</tr>
<tr>
<td></td>
<td>tracking mode automatically switches to Frame Group.</td>
</tr>
<tr>
<td></td>
<td><strong>Frame Group</strong> - Enables automatic tracking and framing of the group</td>
</tr>
<tr>
<td></td>
<td>participants in the room without displaying the camera motion between frames.</td>
</tr>
<tr>
<td></td>
<td><strong>Off</strong> - Disables automatic tracking. All camera control must be handled</td>
</tr>
<tr>
<td></td>
<td>manually.</td>
</tr>
<tr>
<td>Tracking Speed</td>
<td>Specifies the tracking speed:</td>
</tr>
<tr>
<td></td>
<td><strong>Slow</strong> - Detects meeting participants at a slow speed rate.</td>
</tr>
<tr>
<td></td>
<td><strong>Normal</strong> - This is the default tracking speed. Detects meeting participants</td>
</tr>
<tr>
<td></td>
<td>at a normal speed rate.</td>
</tr>
<tr>
<td></td>
<td><strong>Fast</strong> - Detects meeting participants at a fast speed rate.</td>
</tr>
</tbody>
</table>

| Framing Size     | Specifies the framing view:                                                 |
|                  | **Wide** - Establishes a wide view of meeting participants.                 |
|                  | **Medium** - This is the default group framing view. Establishes a medium   |
|                  | view of meeting.                                                           |
|                  | **Tight** - Establishes a close-up view of meeting participants.             |

Enable Camera Tracking
You can enable EagleEye Cube HDCI camera tracking in the local interface.

Procedure
1. In the local interface of the RealPresence Group Series system, go to Camera.
2. Select Camera Tracking On.
Disable Camera Tracking
You can disable camera tracking in the local interface.

Procedure
1. In the local interface of the RealPresence Group Series system, go to Camera.
2. Select Camera Tracking Off.

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

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

<table>
<thead>
<tr>
<th>Participant Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>People Minutes</td>
<td>The total people count for each minute of the call. For example, If there are five people in a sixty minute meeting and five additional people join at 10 minutes after the start of the meeting, the total People Minutes will be 550. (5<em>60) + (5</em>50).</td>
</tr>
<tr>
<td>People Count (call begin)</td>
<td>Number of people on the call during the first minute of the call, tracked with EagleEye Cube HDCI camera system.</td>
</tr>
<tr>
<td>People Count (peak value)</td>
<td>Peak number of people participating in the call, tracked with the EagleEye Cube HDCI camera system.</td>
</tr>
<tr>
<td>People Count (call end)</td>
<td>Number of people participating on the call during the last minute of the call, tracked with the EagleEye Cube HDCI camera system.</td>
</tr>
</tbody>
</table>

EagleEye Cube HDCI Camera Software Updates
Updates to the EagleEye Cube HDCI software are included with the RealPresence Group Series system software updates. No license number or key is needed to update the camera software. Software for an EagleEye Cube HDCI camera is automatically updated when connected with the RealPresence Group Series system.

Procedure
» Connect the EagleEye Cube HDCI to the system.
The system detects the EagleEye Cube HDCI and updates it, if necessary.

**Note:** When the EagleEye Cube HDCI software update version is higher or equal to the RealPresence Group Series system software, software update can't be performed.

**Factory Restore the EagleEye Cube HDCI**

If the EagleEye Cube HDCI camera isn’t 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 reinstall the software. Keep the EagleEye Cube powered on during the factory restore process.

**Procedure**

1. Connect the EagleEye Cube HDCI cable to the RealPresence Group Series system to power on.
2. Insert a straightened paper clip through the pinhole and press and hold the restore button for 5 seconds.
3. Release the restore button when the LED indicators alternate amber.
   The camera enters factory restore mode. The factory restore takes approximately 2 to 3 minutes to complete. The camera automatically powers off and back on when the process is complete.

**Setting Up a Polycom EagleEye IV Camera**

The Polycom EagleEye IV cameras are digital with a 4k sensor that is specifically designed to work with RealPresence Centro systems. Available accessories are a privacy cover, wide-angle lens, and digital extender. EagleEye IV cameras have either 4x or 12x zoom lenses.

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

**EagleEye IV Camera Orientation**

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

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

**Enable an Inverted Camera Position for the EagleEye IV Camera**

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

**Procedure**

1. In the system web interface, go to Admin Settings > Audio/Video > Video Inputs, and choose EagleEye IV camera.
2. At Orientation, select Inverted and click Save.
Enable a Normal Camera Position
You might want to disable the inverted camera position in your environment.

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

Replace the EagleEye IV Camera
On the EagleEye Director II camera, you can replace an EagleEye IV camera with another EagleEye IV camera.

Procedure
1. Power off the EagleEye Director II camera.
2. Disconnect and remove the existing EagleEye IV camera.
3. Connect the desired EagleEye IV camera.
4. Power on the EagleEye Director II camera.

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

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

Polycom EagleEye Director II Camera System
The Polycom EagleEye Director II camera system is an automatic camera positioning system that works in conjunction with a RealPresence Centro system to provide accurate close-up views of the person who is speaking. The EagleEye Director II camera system also provides smooth transitions between the close-up view of the person who is speaking and the group view when there is no active speaker.
The EagleEye Director II camera system uses two cameras. Initially, the current view is captured by one camera, while the other camera is searching and tracking the next target. If two persons speak alternately, the camera tracks the person who is speaking, while the other camera tracks the other person who is speaking. The camera system continuously scans the room and commands the movable camera to pan, tilt, and zoom, framing users with face detection technology. By providing automatic and intelligent views in various speaking scenarios during a conference, the EagleEye Director II camera system delivers a user experience similar to a newscast video production.

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

**Note:** The Polycom EagleEye Director II camera system is compatible with two Polycom EagleEye IV-12X cameras and does not support a single camera configuration. The cameras must be paired with the EagleEye Director II camera system. A wide angle adapter is supported if it is used with both EagleEye IV cameras.

The EagleEye Digital Extender and RealPresence Digital Breakout Adapter can help with installations that require longer connections between your camera and system (except for the required audio connection). For information, see the [Polycom RealPresence Group Series Integrator Reference Guide](#).

The Horizontal Field of View (HFOV) of the analytics camera is 80 degrees. The analytics camera provides participant count details and PIP video. The participants who are outside the HFOV are not detected by the EagleEye Director II analytics camera system and are not counted or shown in the PIP.

The camera system detects the speaker through participant voices. If there is a microphone for a local speaker along with the EagleEye Director II camera system, the performance of the EagleEye Director II camera system affects the frame speaker behavior.

During an active conference call while using the camera system, Polycom recommends that you do not to use a microphone for local speakers.
Position the EagleEye Director II Camera System

Follow these guidelines to position the EagleEye Director II camera system to work with your RealPresence Centro system.

Procedure

1. Make sure the EagleEye Director II camera system is on a level surface or mounting bracket. The camera’s viewing angle is approximately 5 degrees above and 15 degrees below its direct line of sight as shown below.

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

3. To ensure the best view from the camera system voice-tracking feature, follow these suggestions:
   - Make sure that ambient room noise is quiet enough to allow the camera system to locate the participant who is speaking.
   - Set up the audio connection from the RealPresence Centro system to the camera system, whether you connect it directly to the audio output of the system or to an audio processor managing the room audio.
4. Set the camera system on a wall. Place the camera between 5.5 and seven feet from the ground. This figure shows optimal placement of the camera system:
5. Ensure that people are sitting within a three to 33 feet (0.91 m ~ 10.1 m) viewing range from the device.

The following figure shows the viewing range of EagleEye Director II camera system.

![Viewing Range Diagram]

**Indicator Lights**

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

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

**Figure 3:**

![LED Status Diagram]

The following table shows the LED status of EagleEye Director II camera system with its corresponding behavior.
<table>
<thead>
<tr>
<th>LED Color/State</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Power On, EagleEye Director II camera system is in active state</td>
</tr>
<tr>
<td>Blinking Blue</td>
<td>Receive IR, EagleEye Director II camera system boot up</td>
</tr>
<tr>
<td>Fast Blinking Blue</td>
<td>Power On, MCU is being initialized, Adjust Analytics camera status</td>
</tr>
<tr>
<td>Amber</td>
<td>Standby/Asleep</td>
</tr>
<tr>
<td>Alternate Amber and Blue</td>
<td>Software update, Factory restore, USB image update</td>
</tr>
<tr>
<td>Blinking Amber</td>
<td>USB plugged in</td>
</tr>
<tr>
<td>Green</td>
<td>In a call</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Receive IR in a call</td>
</tr>
<tr>
<td>Fast Blinking Red</td>
<td>EagleEye Director II camera system error</td>
</tr>
</tbody>
</table>

**View System Status for EagleEye Director II Camera System**

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

**Procedure**

- Do one of the following:
  - In the local interface, go to **Settings > System Information > Status**.
  - In the web interface, go to **Diagnostics > System > System Status**.

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

**System Status**

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Alerts</td>
<td>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.</td>
</tr>
<tr>
<td>Call Control</td>
<td>Displays the status of the Auto-Answer Point-to-Point Video and Meeting Password settings.</td>
</tr>
<tr>
<td>Audio</td>
<td>Displays the connection status of audio devices such as microphones, Polycom SoundStation IP conference phone, and Polycom SoundStructure card.</td>
</tr>
</tbody>
</table>
### Diagnostic Screen

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Displays the connection status of the camera that is connected. If the camera is not connected or is not selected as the current camera source, this choice is not visible on the screen. In addition, the details of the EagleEye cameras attached to the EagleEye Director II camera system are displayed.</td>
</tr>
<tr>
<td>LAN</td>
<td>Displays the connection status of the IP Network.</td>
</tr>
</tbody>
</table>
| Servers           | • Always displays the Gatekeeper and SIP Registrar Server.  
                    • Displays the active Global Directory Server, LDAP Server, or Microsoft Server.  
                    • If enabled, displays the Provisioning Service, Calendaring Service, or Presence Service. |
| Log Management    | Displays the status of the Log Threshold setting.  
                    When a system device or service encounters a problem, you see an alert next to the **System** button on the menu. |

### EagleEye Director II Camera System Diagnostics

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

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

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

**Perform a Factory Restore**

A factory restore completely erases the system and restores it to the factory software version and default configuration. During a factory restore, the LED indicator on the front of the EagleEye Director II camera alternates between blue and amber.

**Note**: Do not power off the camera during the factory restore process.
Procedure

1. With the camera 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 camera.
3. Hold the Restore button for an additional five seconds, and then release it when the LED alternates amber and blue.

The camera enters factory restore mode. The factory restore takes approximately eight minutes to complete. The camera automatically powers off and back on when the process is complete.

Setting Up a Polycom EagleEye Producer System

The Polycom® EagleEye™ Producer system is a camera-peripheral technology that provides room framing and participant counting. Using facial recognition technology, the device scans the room and commands the movable Polycom® EagleEye™ III and IV cameras to pan, tilt, and zoom.

Position the EagleEye Producer system on a level surface, ideally on top of a monitor. You can mount the Polycom® EagleEye™ III, Polycom® EagleEye™ IV cameras on top of the EagleEye Producer. The EagleEye Producer includes a 'bunk bed' mount for use with the universal camera mounting solution. Available accessories include the EagleEye Digital Extender and the Digital Breakout Adapter.

Ensure that the EagleEye Producer field of view includes the all conference participants. The system supports a wide angle lens on the EagleEye IV camera. EagleEye IV cameras are available with either 4x or 12x zoom capability.

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

The EagleEye Producer system and EagleEye Director II camera system are tested to support the accessories:

- 10 meter cable HDCI to mini-HDCI
- Digital Breakout Adapter
- EagleEye Digital Extender

For more information on the required cables, or setting or positioning the EagleEye Producer, refer to the Polycom EagleEye Producer Setup Sheet document on Polycom Support.

Calibration

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

Automatically Calibrate the Room View

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

Procedure

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

2. Enable **Tracking**.

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

**Manually Calibrate**

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

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

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

**Procedure**

1. Ensure that the **Make This Camera Your Main Camera** video input setting in administration settings in the Group system web interface specifies the EagleEye Producer as the main camera.

2. Turn **Self View** on in the local interface of the system to view the room in the self view window.

3. Press the **Home** button on the system remote control for five seconds to get to the Home screen.

   The EagleEye Producer LED changes to a fast blue blink when on the Home screen.

4. Press the **Up** and **Down** arrow buttons on the remote control to align the webcam with the EagleEye camera to show the best room view when group framing.

5. To exit the Home screen, press any key on the remote control except the **Up** or **Down** arrow button.

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

**Camera Tracking**

The Polycom EagleEye Producer detects the people in the room and provides framing during a conference. Frame Speaker with a Normal tracking speed and Medium view is enabled by default. When an EagleEye Producer is connected to a RealPresence Centro system, camera tracking starts automatically when you initiate a call and stops automatically when you hang up from a call. You can also manually start camera tracking in the local interface of the system. EagleEye Producer detects the people in the room and sets up framing. You can set the tracking mode and speed, and specify the type of group framing, which enables automatic tracking of group participants in the room and frames the active speaker. EagleEye Producer is integrated with 4 microphones to detect the active speaker.

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

**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.
Change the EagleEye Camera

On the EagleEye Producer, to change an EagleEye camera to another EagleEye camera, you must power off the EagleEye Producer first.

Procedure
1. Power off the EagleEye Producer.
2. Disconnect and remove the existing EagleEye camera.
3. Connect the desired EagleEye camera.
   - For information about how to connect an EagleEye camera, see the Polycom EagleEye Producer Setup Sheet.

Note: The camera on the EagleEye Producer can be either an EagleEye IV or EagleEye III camera. When used with the EagleEye IV an additional adapter cable is required, which is included in the EagleEye Producer kit.

An EagleEye Digital Extender and the Digital Breakout Adapter are available for the EagleEye Producer. For more information on these accessories, refer to the RealPresence Group Series Integrator Reference Guide.

Change Camera Tracking Settings

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

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

Enable Camera Tracking

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

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

Disable Camera Tracking

You can disable camera tracking in the local interface.

Procedure
- In the local interface of the RealPresence Centro system, go to Camera and select Camera Tracking Off.
**Update EagleEye Producer Software**

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

**Procedure**

» Connect the EagleEye Producer to the system.

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

**Update the EagleEye Producer System Image**

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

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

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

**Procedure**

1. Create a folder named `plcm-eep-cmd` in the USB root directory.
2. Create a subfolder named `update` in the `plcm-eep-cmd` folder.
3. Copy the EagleEye Producer update image (polycom-eagleeyeproducer-xxx-1.0.0.xx-xxxx.img) into the `update` folder.
4. Plug in the EagleEye Producer power cable to power it on and allow it to fully boot up.
   The LED turns solid blue.
5. Plug the USB drive into EagleEye Producer.
   The LED blinks amber and then turns solid blue in a few seconds.
6. Unplug the EagleEye Producer power cable, but leave the USB drive plugged in.
7. Plug in the EagleEye Producer power cable and allow it to boot up.
   The LED turns solid blue. The EagleEye Producer starts the image update and the LED blinks blue and amber. The image update takes approximately ten minutes to complete. The EagleEye Producer automatically reboots when the image update is complete. The camera tilts up and then down during the reboot and the LED returns to solid blue.
8. Remove the USB drive.
   The update log is saved in `[USB root directory]/eepout/[EEP SN]/log`.

**Download System Logs and Configurations**

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

1. Create a folder named `plcm-eep-cmd` in the USB root directory.
2. Create a subfolder named `log` in the `plcm-eep-cmd` folder.
3. Create a blank text file named `downloadlogflag` in the `log` folder.
4. Plug the USB drive into the EagleEye Producer.
   The LED blinks amber and then turns solid blue.
5. Remove the USB drive.

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

Participant Count CDR Details

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

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

<table>
<thead>
<tr>
<th>Participant</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>People Minutes</td>
<td>The total people count for each minute of the call. For example, if there are five people in a sixty minute meeting and five additional people join at 10 minutes after the start of the meeting, the total People Minutes will be 550. (5<em>60)+(5</em>50).</td>
</tr>
<tr>
<td>People Count (call begin)</td>
<td>Number of people on the call during the first minute of the call, tracked with EagleEye Producer camera system.</td>
</tr>
<tr>
<td>People Count (peak value)</td>
<td>Peak number of people participating in the call, tracked with the EagleEye Producer camera system.</td>
</tr>
<tr>
<td>People Count (call end)</td>
<td>Number of people participating on the call during the last minute of the call, tracked with the EagleEye Producer camera system.</td>
</tr>
</tbody>
</table>

Perform a Factory Restore

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

**Procedure**

1. While the EagleEye Producer system is powered off, insert a straightened paper clip through the pinhole and press and hold the **Restore** button.
2. While holding the **Restore** button, plug in the power cable to power on the EagleEye Producer.
3. Hold the **Restore** button for five additional seconds, and then release it when the LED alternates amber and blue.
   
   The EagleEye Producer enters factory restore mode. The factory restore takes approximately eight minutes to complete. The EagleEye Producer automatically reboots when the process is complete.
4. Calibrate the room view when the reboot is complete.
   
   **Note**: Keep the Polycom EagleEye Producer powered on during the factory restore process.

---

**Set Up the Polycom EagleEye Director**

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

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

**Procedure**

1. Power on the EagleEye Director.
   
   You can verify that the device is detected and compatible with the system’s software on the System Status screen.
   
   - In the system web interface, go to **Diagnostics > System > System Status > EagleEye Director**. If you see **EagleEye Director** among the status settings, the device has been detected.
2. Calibrate the cameras.
   
   If you notice that the speaker is not framed accurately, ensure that the vertical bar of the EagleEye Director is vertical. Placing the EagleEye Director on a horizontal surface can help to ensure that the vertical bar is vertical. You might also need to recalibrate the cameras.
3. Adjust the room view.

**Indicator Lights**

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

**Adjust the Room View**

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

**Procedure**

1. Do one of the following:
   - From the local interface, go to Settings > Administration > Camera Tracking > Calibration, and then select Begin Calibration.
   - From the system web interface, go to Admin Settings > Audio/Video > Video Inputs, and then select the Input used by the EagleEye Director.
2. Do one of the following:
   - In the local interface, select Skip to move to the Adjust Room View screen.
   - In the system web interface, select Adjust Room View.
3. Use the arrow buttons and zoom controls on the remote control or system web interface to show the room view you want far site participants to see.
4. Select Finish to save the settings and return to the Camera Settings screen.

**Camera Tracking in the Local Interface**

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

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

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

**Disable Camera Tracking for EagleEye Director**

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

Do one of the following

- In the local interface, go to Settings > Administration > Camera Tracking > Settings.
  - For the Tracking Mode setting, select Off. In this mode, the tracking function is disabled. You must manually move the camera using the remote control or a touch device.
- In the system web interface, go to Admin Settings > Audio/Video > Video Inputs, and then select the Input used by the EagleEye Director.
  - Disable the Use Voices to Track People setting.
- If the RealPresence Centro system is paired with a Polycom touch device, touch Cameras on the Home screen or the Call screen and select Stop Camera Tracking.
Enable Camera Tracking for EagleEye Director

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

Do one of the following:

- In the local interface, go to **Settings > Administration > Camera Tracking > Settings**.
  - For the **Tracking Mode** setting, select **Voice**. This is the default tracking mode. In this mode, the camera automatically tracks the current speaker in the room using a voice tracking algorithm. When you select the **Voice Tracking Mode**, you can also choose the **Tracking Speed**. This speed determines how quickly the camera moves to each person who speaks. The default speed is **Normal**. If voice tracking does not work as expected, make sure the microphones are functioning properly.

- In the system web interface, go to **Admin Settings > Audio/Video > Video Inputs**, and then select the **Input** used by the EagleEye Director.
  - Enable the **Use Voices to Track People** setting.

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

Camera Presets

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

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

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

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

Configure FECC on the Far-end Site Camera

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

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

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

Transfer EagleEye Director Logs

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

Procedure

1. Attach a USB storage device formatted in FAT32 to the back panel of the EagleEye Director.
2. Restart the EagleEye Director by following these steps:
   a. Unplug the 12v adaptor attached to the side of the EagleEye Director.
   b. Wait a 5 seconds.
   c. Plug the 12v adaptor into the side of the EagleEye Director.
      It could take up to two minutes for the EagleEye Director to restart.
3. Remove the USB storage device.
   A log file using the name format of eagleeyedirector_info_xxxxx.tar.gz is generated on the USB storage device.

EagleEye Director Software Updates

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

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

Perform a Factory Restore for the EagleEye Director

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

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

Procedure

1. Press and hold the restore button on the back of the EagleEye Director for 2-3 seconds while the power light cycles.
When normal video content is displayed on the monitor instead of a blue screen, the EagleEye Director has been successfully restored.

2. Release the restore button.

Troubleshooting EagleEye Director Camera Calibration

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

• Ensure all cables are tightly plugged in, then attempt camera detection again. If you are using EagleEye Director version 1.0 software, you might need to ensure that the ball stubs are tightly pressed into the hole on the base after checking the cables.

• Ensure that all seven EagleEye Director tracking microphones are working correctly. Five of those microphones are horizontal and two are vertical reference audio microphones. Calibration fails if any of the microphones do not work.

• Restart the RealPresence Centro system.

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

Troubleshooting EagleEye Director Camera Tracking

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

Setting Up Polycom EagleEye Acoustic Camera

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

The Polycom EagleEye Acoustic camera can also be pointed down to show an item in front of the display, as shown next.
If you are using the EagleEye Digital Extender or the Digital Breakout Adapter with the Polycom EagleEye Acoustic camera, the audio from the camera is not passed to the system. You must use a tabletop microphone array or a ceiling microphone array.
Configuring Remote Control Behavior

Topics:

- Configure Remote Control Behavior
- Programming the Remote Control
- Using the RealPresence Centro System Remote Control

You can configure the behavior of your remote control.

Configure Remote Control Behavior

You can customize how the remote control paired to your system behaves.

When you configure your system for a Zoom environment, the remote control must use DTMF tones by default.

This information applies to Polycom and third-party remote controls.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keypad Audio Confirmation</td>
<td>Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad. Enable this setting when using your system in a Zoom environment.</td>
</tr>
<tr>
<td>Numeric Keypad Function</td>
<td>Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones). If you set this option to Presets, you can generate DTMF tones by pressing the # key on the remote control while in a call. Choose Tones if your system is in a Zoom environment.</td>
</tr>
<tr>
<td>Use Non-Polycom Remote</td>
<td>Configures the system to accept input from a programmable, non-Polycom remote control. In most cases the Polycom remote works as designed, even when you enable this feature. However, try disabling this feature if you experience difficulty with the Polycom remote. For more information about system IR codes, refer to the Polycom RealPresence Group Series Integrator Reference Guide.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
**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 you set the remote control to channel 3, it can control a room system set to any Channel ID.
**Hang-up Button Long Press** | Specifies the behavior of the remote control **Hang-up** button when you press it for a long time.
- **Hang-up / Power Off**: Holding down the **Hang-up** button powers off the room system.
- **Hang-up / Sleep**: Holding down the **Hang-up** button puts the system to sleep.
- **Hang-up Only**: Holding down the **Hang-up** button has no function other than hanging up the call.
**# Button Function** | Specifies the behavior of the **#** button on the remote control.
- **#, then @**: Pressing the # button once displays the hash symbol. Pressing the # button twice quickly displays the @ symbol.
- **@, then #**: Pressing the # button once displays the @ symbol. Pressing the # button twice quickly displays the # symbol.

3. Click **Save**.

---

### Programming the Remote Control

Use the remote control to power on and off your system, or to put the system to sleep or wake it. For details about how to use the remote control, refer to the *Polycom RealPresence Centro User Guide*.

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

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

### Set the Remote Control Channel ID

You can set the remote control channel ID in the system web interface.

**Procedure**

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

Set the Remote Control Channel ID for a Specific System

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

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

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

Procedure

1. Press and hold and for 2-3 seconds on the remote control.
2. After the IR red LED appears on the remote control, release both keys.
   The LED remains lit for 10 seconds.
3. While the LED is lit, enter a 2-digit ID between 00 and 15.
   If you do not enter the ID during the 10 seconds the LED is lit, the LED flashes six times and you must repeat steps 1 and 2. Be sure to enter the ID during the next 10-second window.

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

Confirm the Channel ID

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

Procedure

1. While blocking the IR signal from the remote control using your hand or some other object, press and hold and for 2-3 seconds.
2. After the LED on the remote control comes on, release both keys.
   The LED remains lit for 10 seconds.
3. While the LED is lit, enter the 2-digit ID between 00 and 15 that you believe is the channel ID.
   If you do not enter the ID during the 10 seconds the LED is lit, the LED flashes six times and you must repeat steps 1 and 2. Be sure to enter the ID during the next 10-second window.
4. If you entered the current channel ID, the LED flashes twice.
   Otherwise, the LED flashes six times and allows you to repeat step 3.
Using the RealPresence Centro System Remote Control

The remote control enables you to operate the RealPresence Centro system and control the system with touch monitors or a touch device. You can place calls, adjust the volume, and navigate menus. To control the system, point the remote control toward the monitors.

Recharge the Remote Control Battery on the RealPresence Centro System

When the remote control battery power is low, a notification displays on the RealPresence Centro Home screen. You can use the USB ports on the base of the solution to charge the battery. Recharging the battery can take from 20 minutes up to multiple hours.

Procedure

1. Pull the battery out of the end of the remote control.
2. Insert the USB plug of the battery into a USB port on the system.
3. Wait until the status light on the battery turns green before removing it from the port.
4. Insert the charged battery into the remote control.
Enabling Mobile Devices as Controllers

Topics:
  - Enabling RealPresence Mobile

Enabling RealPresence Mobile

Polycom SmartPairing™ allows you to detect and pair a RealPresence Centro system from the RealPresence Mobile application on an Android or Apple iPad tablet. After you pair the application and the system, you can use the RealPresence Mobile application to perform two basic functions:
  - Use the application as a remote control for the room system.
  - Swipe to transfer a call from the RealPresence Mobile application to the room system.

SmartPairing Prerequisites

Telnet must be enabled before you can use SmartPairing on RealPresence Centro systems. Because telnet is disabled by default in all Security Profiles, SmartPairing is also disabled by default. The setting to enable telnet is not configurable when the Security Profile is set to Maximum or High.

Security Profiles and SmartPairing

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Telnet Setting Default</th>
<th>SmartPairing Available?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum / High</td>
<td>Disabled, Not Configurable</td>
<td>No</td>
</tr>
<tr>
<td>Medium / Low</td>
<td>Disabled, Configurable</td>
<td>Yes. To use SmartPairing, do the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Enable telnet. In the system web interface, go to Admin Settings &gt; Security &gt; Global Security &gt; Access and at Enable Telnet Access, select the checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Send an API command or use the system web interface.</td>
</tr>
</tbody>
</table>

Configure SmartPairing

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

Procedure

1. In the RealPresence Centro system web interface, go to Admin Settings > General Settings > Pairing > SmartPairing.
2. Configure these settings.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SmartPairing Mode</strong></td>
<td>Specifies the method used to pair with the room system, if SmartPairing is enabled:</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Automatic</td>
</tr>
<tr>
<td></td>
<td>• Manual</td>
</tr>
<tr>
<td><strong>Signal Volume</strong></td>
<td>Specifies the relative signal strength of the ultrasonic signal within the loudspeaker audio output signal. The selections are Auto, and levels are 1 to 10.</td>
</tr>
</tbody>
</table>
Enabling Content Sharing

Topics:

- Configure Content Sharing
- Adjust Audio Level for Content
- Configure Monitor 1 as the Content Monitor
- Configure Monitor 2 as the Content Monitor
- Setting Up a Polycom Content Display Application
- Closed Captioning
- Enable VisualBoard Content Sharing
- Prerequisites for the VisualBoard Application
- Configure the Polycom UC Board
- Sharing Content During Calls
- Configuring DVD Player Settings

Configure Content Sharing

You can configure content sharing in the RealPresence Centro system web interface. For content to display properly, the system's Monitor 2 must support Progressive mode, and the output resolution should be set to a Progressive setting, such as 1280x720p or 1920x1080p. Interlaced output for Monitor 2 is not supported. Do not use the resolution setting 1920x1080i.

Procedure

1. In the system web interface, go to Admin Settings > Audio/Video > Video Inputs and select the input you want to configure for content.
2. For the Display as setting, select Content for the input that will display content.

When you connect a content-sharing device such as a laptop to the input, the content starts displaying. If the content-sharing device is already connected, you must manually show the content from the local interface. For more information about sharing content, refer to the Polycom RealPresence Centro User Guide.

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

3. In the system web interface, go to Admin Settings > Network > Dialing Preference.
4. Enable H.239.

Note: While in a call, you cannot enable or disable H.239.
Adjust Audio Level for Content

You can adjust the audio level for content in the RealPresence Centro system web interface.

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

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

Configure Monitor 1 as the Content Monitor

To use the VisualBoard application on your RealPresence Centro system's Monitor 1, you must configure monitor settings on the system web interface. If you are using a touch monitor as Monitor 1, you can run the VisualBoard application on the monitor and touch the screen to interact with the application.

Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use Game Mode, if that setting is available.

Procedure

1. In the system web interface, go to Admin Settings > Audio/Video > Monitors.
3. For the Monitor Profile setting, select Content, then Far, then Near or Content, then Far.

Configure Monitor 2 as the Content Monitor

The VisualBoard application runs on Monitor 2 by default, but you might want to make configuration changes to the monitor settings in the RealPresence Centro system web interface. Some monitors might delay the time between writing and displaying, due to processing within the monitor. When using the VisualBoard application with a monitor, configure your monitor or projector to use Game Mode, if that setting is available.

Procedure

1. In the system web interface, go to Admin Settings > Audio/Video > Monitors.
2. To configure monitor 1, go to System > Admin Settings > Monitors.
   - At Enable, select either Auto or Manual. If you chose Manual, select any of the available profiles, except Content, then Far, then Near or Content, then Far.
3. To configure monitor 2, at Monitor Profile, enable one of the content profiles, such as Content, then Far, then Near, Content, then Far, Content, then Near, or the Content Only profile.

Setting Up a Polycom Content Display Application

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

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

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

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

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

◦ Operating System: Windows 7 or 8
◦ Minimum computer: 500 MHz Pentium® III (or equivalent); 256 MB memory
Recommended computer: 1 GHz Pentium III (or equivalent); 512 MB memory

• Connect the computer or computers to the IP network.

Closed Captioning

You can provide real-time text transcriptions or language translations of the video conference by displaying closed captions on your RealPresence Centro system. The captioner can be present or listen to the conference audio with a phone or browser.

When the captioner sends a unit of text, all sites see it on the main monitor for 15 seconds until the text disappears automatically.

Closed captions are supported between Polycom systems with software version 4.1.3 or later, including a system hosting a multipoint call, HDX systems with any software version, and Polycom VSX® systems with software version 7.0 or later.

Captions are provided in any language that uses the Latin alphabet.

Depending on the system's capabilities, captions can be entered using one of the following methods:

• Remotely through a dial-up connection to the system's serial RS-232 port
• In the room using equipment connected directly to the serial port
• In the room or remotely using the system web interface

Enter Closed Captions on the System Web Interface

Closed captioners can provide captions from inside the conference room, or from a remote location, by entering the captions directly into the system web interface.

Procedure

1. In the system web interface, go to Utilities > Tools > Closed Caption.
2. Log in using this information if prompted:
   - User Name: Your user name defined for the video conferencing system.
   - Password: Meeting password defined for your video conferencing system.
3. In the Closed Caption screen, type the caption text into the text field.
   - Text wraps to the next line after 32 characters.
4. Press **Send** to send the text to the sites in the conference.

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

Closed captioners can provide captions from inside the conference room, using equipment connected directly to the serial port of the system.

**Procedure**

1. Ensure that the computer and the system are configured to use the same baud rate and parity settings.
2. In the system web interface, go to **Admin Settings > General Settings > Serial Ports**.
3. Set the RS-232 mode to **Closed Caption**.
4. On the computer, start the transcription application.
5. Enter text using the stenographic machine connected to the computer.
6. To stop sending closed captions, close the transcription application.

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

Closed captioners can provide captions from inside the conference room, or from a remote location, via a dial-up connection to the serial port of the system.

Ensure that the computer and the system use the same baud rate and parity settings.

**Procedure**

1. In the system web interface, go to **Admin Settings > General Settings > Serial Ports**.
2. Set the RS-232 mode to **Closed Caption**.
3. Establish a dial-up connection between the computer and the system.
   a. Connect a null modem adapter to the RS-232 serial port.
   b. Connect an RS-232 cable to the modem and to the null modem adapter.
   c. Connect the modem to a phone line.
   d. Configure the modem for 8 bits, no parity.
      You may need to configure the modem to answer automatically. You may also need to configure it to ignore DTR signals.
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.

**Enable VisualBoard Content Sharing**

You must enable the VisualBoard application before you can use it with the RealPresence Centro system.

**Procedure**

1. From the system web interface, go to **Admin Settings > Audio/Video/Content > Content**.
2. Select **Enable VisualBoard**, and then select **Save**.
Prerequisites for the VisualBoard Application

Before you can begin using the VisualBoard application, ensure that you have done the following:

- The touch monitor should be HID compliant with HDMI interface only.
- Installed and configured one of the following: USB mouse or UC Board hardware
- Enabled the VisualBoard setting in the RealPresence Centro system web interface at Admin Settings > Audio/Video/Content > Content.
- When setting up the VisualBoard application, note that only one USB storage device can be connected to one host port, whether it is connected directly or through a hub.

Configure the Polycom UC Board

With the Polycom® UC Board, you can show and annotate content in real-time from RealPresence Centro systems by using the stylus and receiver included with the UC Board hardware. You can use either a second monitor or a whiteboard and projector. For flat, cold surfaces such as white boards with projectors, Polycom suggests that you use the Polycom UC Board.

Two monitors are required to use the Polycom UC Board. The second monitor can be either a projector used with a whiteboard, or a monitor.

Polycom recommends the following installation tips:

- Use LED backlit, LCD displays instead of CFL LCD displays.
- Do not use plasma backlit displays.
- The UC Board hardware sensor and pen are designed for cold surfaces, such as white boards with projectors.
- Mount the hardware sensor on the top of the display device. Room lights can interfere with the sensor when it is mounted on the bottom of the display.

The UC Board sensor supports one stylus at a time. It does not support using two styluses simultaneously.

For more information on setting up and using the UC Board, refer to the Polycom UC Board Quick Start Guide, available with the UC Board hardware and at Polycom Support.

To set up two monitors and configure to show content:

1. To configure monitor 1, in the system web interface, go to Admin Settings > Audio/Video > Monitors. At Enable, select either Auto or Manual. If you chose Manual, select any of the available profiles.

2. To configure monitor 2, at Monitor Profile, enable one of the content profiles.
   To improve performance, configure your monitor or projector to use Game Mode, if that setting is available.

Sharing Content During Calls

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

- A DVD player connected directly to a video input on a system
• People+Content IP installed on a computer, with any system
• A computer connected directly to a system or a Polycom touch device

RealPresence Centro systems achieve maximum content frame rate of 30 fps for 1080p with a 1080p Resolution option key installed, and 60 fps for 720p. If you use Content as the Quality Preference in your network IP settings, you can achieve a content frame rate of 60 fps for 1080p with the 1080p Resolution option key installed.

RealPresence Centro systems can achieve maximum content frame rate of 60 fps for 1080p, while the camera sends a maximum frame rate of 1080p 30 fps.

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

**Configuring DVD Player Settings**

On RealPresence Centro systems, you can connect a DVD player to an HDMI or VGA input to play content.

**Adjust DVD Audio Settings for Content**

DVD inputs are active when you select the camera source configured as DVD. This means that both the audio and video inputs are active—you cannot select one or the other. Because the microphone inputs remain active while the DVD player is playing, call participants might want to mute the microphones while playing DVDs. You can configure DVD audio settings in the RealPresence Centro system web interface.

**Procedure**

1. In the system web interface, go to Admin Settings > Audio/Video/Content > Audio > Audio Input.
2. Set Line In Level for playback volume of the DVD player relative to other audio from the system.

   Enable DVD Audio Out Always On unless you have the DVD inputs and outputs both connected to the same device to play and record.
Configuring Call Recording

Topics:

• Polycom RealPresence Media Suite Recording

Polycom RealPresence Media Suite Recording

Users can use Polycom® Media Suite solution to record calls directly from the RealPresence Centro system, remotely log in to Polycom RealPresence Media Suite to record or live stream calls.

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

Enable Recording Controls

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Enter the server domain name for RealPresence Media Suite.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the server user name for RealPresence Media Suite.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the server password for RealPresence Media Suite.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Enter the IP address for the RealPresence Media Suite server.</td>
</tr>
</tbody>
</table>

4. Click Save to save the connection settings.

Recording Calls Remotely

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

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

Users can also remotely record calls in the following ways:

- **Dial RealPresence Media Suite directly**: Use the default recording settings defined by a RealPresence Media Suite administrator. Before recording a call using this method, users must obtain the IP address, H.323 extension, or SIP URL of the RealPresence Media Suite.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Media Suite Type</th>
<th>Connection Method</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Suite system</td>
<td>If the both the video conferencing system and the RealPresence Media Suite system are not registered to the gatekeeper or to a SIP server, dial the RealPresence Media Suite IP address. If the both the video conferencing system and the RealPresence Media Suite system are registered to a gatekeeper, dial the RealPresence Media Suite E.164 extension for H.323. If the both the video conferencing system and the RealPresence Media Suite system are registered to a SIP server, dial the RealPresence Media Suite SIP address.</td>
<td>10.11.12.13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1234</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CS123</td>
</tr>
<tr>
<td>Media Suite Type</td>
<td>Connection Method</td>
<td>Example</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>VRR</td>
<td>For SIP calls:</td>
<td>If the RealPresence Media Suite IP is 11.12.13.14 and the VRR number is 4096, dial 11.12.13.14##4096. If the SIP peer prefix of the RealPresence Media Suite is 8888 and the VRR number is 4096, dial 88884096.</td>
</tr>
<tr>
<td></td>
<td>[VRR number]@[RealPresence Media Suite IP] or [SIP peer prefix] [VRR number]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For H.323 calls:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>[RealPresence Media Suite IP]##[VRR number] or [RealPresence Media Suite E.164 prefix][VRR number]</td>
<td></td>
</tr>
</tbody>
</table>
Customizing the Local Interface

Topics:

- Change the Background Image on the Home Screen
- Change the Startup Image on the Home Screen
- Set Up the Address Bar

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

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

In the system’s local interface, go to Settings > Administration. The local interface has a subset of the administration settings that are available in the system web interface.

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

Change the Background Image on the Home Screen

You can upload a custom background image to display on your system. The image must have a pixel size of 1920 x 1080 (width by height) in a .jpg file format, and a file size less than 5 MB.

Procedure

1. In the system web interface, go to Admin Settings > General Settings > Home Screen Settings > Background.
2. Browse to the desired image file and click Choose File > Upload.
   The custom image displays on all four monitors.

Change the Startup Image on the Home Screen

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

You must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format.
Procedure
1. In the system web interface, go to Admin Settings > General Settings > Home Screen Settings > Startup Background.
2. Click Choose File to search for and select the image you want to upload.
3. When the image name appears next to Choose File, click Upload.

Set Up the Address Bar
You can customize what displays in the address bar of the system’s local interface Home screen.

The system local interface displays an address bar at the bottom of the Home screen. The address bar can contain the following information:
- None
- IP Address
- H.323 Extension
- SIP Address
- Pairing Code

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Address Bar (Left Element)     | Allows you to select which element you want displayed on the left side of the address bar on the local interface. The choices are:  
|                                | • None                                                                       |
|                                | • IP Address                                                                 |
|                                | • 323 Extension                                                              |
|                                | • Pairing Code                                                               |
| Address Bar (Right Element)    | Allows you to select which element you want displayed on the right side of the address bar on the local interface. The choices are:  
|                                | • None                                                                       |
|                                | • SIP Address                                                                |
|                                | • 323 Extension                                                              |
|                                | • Pairing Code                                                               |
## Call a Favorite Contact

In the RealPresence Centro system web interface, at **Place a Call**, you can call a favorite contact.

### Procedure

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

## Call a Speed Dial Contact

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

### Procedure

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

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

## Call a Recent Call Contact

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

### Procedure

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

Place a Call
You can manually dial calls from the Dashboard or Place a Call page.

Procedure
2. Enter the number.
3. Click Call.
   The call is placed according to the default settings you selected in Admin Settings > Network > Dialing Preferences. You can select settings other than the defaults in the two lists below the text entry field.
4. To require a password, select Meeting Password and enter a password in the field that displays below the check box.

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

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

To browse LDAP global directory entries, LDAP must be enabled through Polycom RealPresence Resource Manager. If LDAP is not enabled through RealPresence Resource Manager, you can still search the global directory, but you cannot browse the global directory.

Browse Global Contact Entries to Call
You can browse the global contact entries to call in the global directory in the RealPresence Centro system web interface.

Procedure
1. In the system web interface, 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.

Place a Cascaded Call
From your RealPresence Centro system, you can include multiple sites in a cascaded call if the sites you call have internal multipoint capability.
Keep the following points in mind regarding cascaded calls:

- H.239 is not supported in cascaded calls.
- Cascaded multipoint is not supported in SIP calls.
- HD and SD multipoint are not supported when the system hosts a cascaded call.
- You cannot change the near-end layout.
- The encryption padlock icon might not accurately indicate whether a cascaded call is encrypted.
- You cannot call a group of contacts by using Speed Dial or Favorites to call the group.

Procedure
1. Create and call a group in the directory, or place calls one at a time to several other sites.
2. Ask each far site to call additional sites.
   - Along with these additional sites, each far site in the original multipoint call can add one audio-only connection.

Large Conference
You can provision RealPresence Centro systems to join large conference AVMCU and Skype for Business meetings.

RealPresence Centro has the ability to join large conference meeting with up to 250 participants in a call. Large conference meetings with participant count above 250 are supported with minor limitations.
## RealPresence Centro system behavior in large conference meetings

<table>
<thead>
<tr>
<th>Role</th>
<th>Normal Meetings</th>
<th>Normal Meetings</th>
<th>Large Meetings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than 75 Participants</td>
<td>75 to 250 Participants</td>
<td>More than 250 Participants</td>
</tr>
<tr>
<td>Roster</td>
<td>Full Roster List</td>
<td>No Roster List</td>
<td>No Roster List</td>
</tr>
<tr>
<td>Video View</td>
<td>Gallery View</td>
<td>Gallery View</td>
<td>Gallery View</td>
</tr>
<tr>
<td>Video/Audio/Content</td>
<td>All participants</td>
<td>All participants</td>
<td>For 250 participants (Presenter + Attendee) + Next 25 participants can receive, but cannot share Video and Content.</td>
</tr>
</tbody>
</table>
Setting Up a Polycom RealPresence Touch Device

Topics:

- Positioning the RealPresence Touch Device
- Run the RealPresence Touch Device Setup Wizard (OOB)
- Power Off the RealPresence Touch
- Wake the RealPresence Touch
- Enable the RealPresence Touch Device
- Pairing the Device
- Managing the RealPresence Touch Device
- Customize the RealPresence Touch Screens
- Setting Up and Configuring Directory Servers for the RealPresence Touch
- Enable Skype for Business Mode
- Disable Skype for Business Mode
- Updating Software
- Restart a RealPresence Touch Device
- Restart a System from a RealPresence Touch Device
- Troubleshooting the RealPresence Touch Device

Positioning the RealPresence Touch Device

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

Run the RealPresence Touch Device Setup Wizard (OOB)

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

Procedure

1. Ensure that you have completed the setup wizard on the system.
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. You can also enable EAP/802.1 authentication by providing the identity and password.

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`.

**Power Off the RealPresence Touch**

If you need to move your RealPresence Touch device to another area, power off the device before you disconnect the Ethernet cable.

**Procedure**

1. On any screen, tap `Menu, Settings, and then Administration`.
2. Sign in using your Admin ID and password.
3. Scroll down to `Power and Pairing`.
4. Touch RealPresence Touch Power until a Shutting down... message displays.
   - The RealPresence Touch is powered off.

**Wake the RealPresence Touch**

The RealPresence Touch goes to sleep after two minutes of inactivity. To wake it, you can touch the screen.

**Procedure**

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

**Enable the RealPresence Touch Device**

Before your users can control the system with the RealPresence Touch device, you must enable the device on the RealPresence Centro system's web interface. Once the device is enabled, you can pair it to the system.
**Procedure**

1. On the system web interface, go to Admin Settings > General Settings > Pairing > Polycom Touch Device.
2. Select the Enable Polycom Touch Device check box and click **Save**.
   
   Note that only one device can be paired to a system at a time.

**Pairing the Device**

When you configure the RealPresence Touch to pair with a particular RealPresence Centro system, the RealPresence Touch makes an IP connection to the room system. If the connection is lost, the RealPresence Touch automatically attempts to restore the connection.

After you have completed RealPresence Touch setup, you can pair to a different system using RealPresence Touch settings.

**Pairing States**

The following table describes the pairing and connection states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpaired</td>
<td>The RealPresence Touch is not associated with a system.</td>
</tr>
<tr>
<td>Paired and Connected</td>
<td>The RealPresence Touch is associated with a system through the pairing process. This is normal operating mode. A RealPresence Touch can be connected to only one system at a time.</td>
</tr>
<tr>
<td>Paired and Disconnected</td>
<td>The RealPresence Touch is associated with a system, but communication is disrupted, usually because of a system power off or LAN issue. Communication is automatically restored when a system and the touch device are successfully connected to the LAN.</td>
</tr>
</tbody>
</table>

**Pair For the First Time**

To pair your RealPresence Touch with a RealPresence Centro system that has not been paired before, you must enter the system’s credentials before connection can be established.

**Procedure**

1. After completing the out-of-box (OOB) setup wizard, the RealPresence Touch displays the pairing screen.
2. Tap the Manually Pair tab.
3. Enter the **IP Address**, **Admin ID**, and **Password** for the system.
4. Tap **Pair**.
   
   The pairing connection begins, and the Home screen displays when the pairing is successful.
Pair to a Previously Paired System

If you have paired with a RealPresence Centro system before, you can select it from a previously paired list of systems. You do not have to enter the system credentials again, unless the credentials have changed.

Procedure
1. On the Home screen, tap **Menu, Settings**, then **Administration**.
2. Sign in using your admin ID and password.
3. Scroll down to **Power and Pairing** and tap **UNPAIR AND RETURN TO PAIRING SCREEN**.
4. On the **Recently Paired** tab, tap the system that you want to pair with.
   - The pairing connection begins, and the Home screen displays when the pairing is successful.
   - If you unpair from the system, any current calls on the system are still active. To hang up the calls, repair to the room system and select **More Options**, then **Participants, More Options**, and **Remove** or **Remove All**.

After the room system and the RealPresence Touch are paired, the system web interface and the RealPresence Touch interface display information about each other and about their connection status.

Unpair a RealPresence Touch

You can unpair the RealPresence Touch and a RealPresence Centro system.

Procedure
1. In the system web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
2. Clear the check box next to **Enable Polycom Touch Device**.
3. Click **Save**.
   - The system cannot pair with any touch device while the **Enable Polycom Touch Device** check box is cleared.

Remove a System from the Paired System List

After attempting to pair a device, a “Cannot Pair as a Dedicated Device” message might be displayed. This means that another device is already paired to the same RealPresence Centro system. An administrator can determine which device is paired and can unpair the device using the system web interface.

Procedure
1. In the system web interface, go to **Admin Settings > General Settings > Pairing > Polycom Touch Device**.
2. Click **Forget this Device**.
3. Click **Save**.
   - Now you can pair another system.
Managing the RealPresence Touch Device

You can remotely manage certain features of your RealPresence Touch when it is paired to a RealPresence Centro. For a list of supported browsers, refer to the Polycom RealPresence Centro Release Notes.

You can manage the following features remotely:

- **Download Logs**: Downloads the RealPresence Touch logs to the location specified in the device.
- **Network Settings**: Specifies whether the system acquires an IP address automatically or manually. With the manual method, the other settings that are available from the RealPresence Touch become available on the web.
- **Pair**: Pairs and unpairs from systems. Before you can connect to or pair with a device, you must know the device's IP Address and the User Name and password used to connect.
- **Security**: System security allows configuration of the following settings:
  - Changes the admin ID and password of the RealPresence Touch.
  - Provision to disable the TLS v1.0.
- **Software Updates**: Updates the RealPresence Touch software. You can update from the default Polycom server or your own server by entering the appropriate IP address.
- **View RealPresence Touch Screens**: Shows the screen currently being displayed on the RealPresence Touch. You can click Refresh at any time to see if the screen has changed.

Open a Remote Management Window

You can open a remote management window for your RealPresence Touch in a RealPresence Centro system web browser.

**Procedure**

1. In a web browser, enter the IP address of the RealPresence Touch device.
2. In the login window, enter the **ID** and **Password** you use to access the administrative features of the RealPresence Touch.
   
   You can access the remote management features by using the Navigation menu or the Dashboard. To return to the Dashboard, click the Home icon.

Pair Using RealPresence Touch Web Interface

To pair your RealPresence Touch with a RealPresence Centro system, you must enter the system's credentials before connection can be established.

**Procedure**

1. In the RealPresence Touch web interface, click **Pairing**.
2. At **Device**, select **RealPresence Centro**.
3. Enter the **IP Address or Host Name**, **User Name**, and **Password** for the system.
4. Click **Pair**.

   The pairing connection begins, and the Home screen displays when the pairing is successful.
Unpair Using the RealPresence Touch Web Interface
You can unpair the RealPresence Touch and a RealPresence Centro system.

Procedure
1. In the RealPresence Touch web interface, click Pairing.
2. Click Unpair.

Change the RealPresence Touch User Name and Password
You can change the security credentials for the RealPresence Touch device.

Procedure
1. In the RealPresence Touch web interface, click Security.
2. At Admin ID, enter your admin ID.
3. At Current Password, enter the current password.
4. At Password, enter the new password.
5. At Confirm Password, reenter the new password.
6. Click Save.

Configure Network Settings
The RealPresence Touch device has a separate admin settings that allow administrators to configure
network and security settings on the device.

Procedure
1. From the Home screen on the device, touch Administration.
2. Tap Network Settings.
3. Configure the following settings.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set IP Address</td>
<td>Specifies how the RealPresence Touch device obtains an IP address.</td>
</tr>
<tr>
<td></td>
<td>• Obtain IP address automatically. Select if the device gets an IP address from the DHCP server on the LAN.</td>
</tr>
<tr>
<td></td>
<td>• Enter IP address manually. Select if the IP address is not automatically assigned.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address currently assigned to the device, if it obtains the IP address automatically. If you select Enter IP address manually, enter the IP address here.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask currently assigned to the device. If you selected Enter IP address manually, enter the subnet mask here.</td>
</tr>
<tr>
<td>Settings</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the gateway currently assigned to the device. If you selected <strong>Enter IP address manually</strong>, enter the gateway IP address here.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Displays the DNS servers assigned to the device. 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server 1</strong>: If the RealPresence Touch device does not automatically obtain a DNS server address, add a DNS server address here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server 2</strong>: If the RealPresence Touch device does not automatically obtain a DNS server address, add a DNS server address here.</td>
</tr>
<tr>
<td>VLAN</td>
<td>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.</td>
</tr>
<tr>
<td>LAN Speed</td>
<td>Specifies whether to use 10 Mbps, 100 Mbps, or 1000 Mbps for the LAN speed. If the <strong>Autonegotiation</strong> setting is enabled, this setting is read-only. To change the <strong>Autonegotiation</strong> setting, in the RealPresence Centro system web interface, go to <strong>Admin Settings &gt; Network &gt; LAN Properties &gt; LAN Options</strong>. Select or clear the <strong>Autonegotiation</strong> checkbox.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Choose the Duplex mode that is supported by the switch, either <strong>Full</strong> or <strong>Half</strong>. If the <strong>Autonegotiation</strong> setting is enabled, this setting is read-only. To change the <strong>Autonegotiation</strong> setting, use the RealPresence Centro system web interface, and go to <strong>Admin Settings &gt; Network &gt; LAN Properties &gt; LAN Options</strong>. Select or clear the <strong>Autonegotiation</strong> checkbox.</td>
</tr>
<tr>
<td>Enable EAP/802.1X</td>
<td>Specifies whether EAP/802.1X network access is enabled. The following authentication protocols are supported:</td>
</tr>
</tbody>
</table>
| (under EAP 802.1X in the system local interface) | • EAP-MD5  
• EAP-PEAPv0 (MSCHAPv2)  
• EAP-TTLS  
• EAP-TLS                                                                                                                                                                                                                                                                                 |
| EAP/802.1X Identity             | 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                                                                                                                                                                                                 |
| (under EAP 802.1X in local interface) |                                                                                                                                                                                                                                                                                                                                 |
### Enable Recent Calls and Speed Dial

You can enable the recent calls and speed dial icons in the RealPresence Centro system web interface.

- **Recent Calls**: In the system web interface, go to **Admin Settings > General Settings > System Settings > Recent Calls**. Select the Enable Recent Calls checkbox.
- **Speed Dial**: In the system web interface, go to **Admin Settings > General Settings > Home Screen Settings > Speed Dial**. Select the Enable Speed Dial checkbox.

### Customize the RealPresence Touch Screens

You can use the RealPresence Centro system web interface to configure how information is displayed on the Home screen of the RealPresence Touch device. These settings are included in the System settings profile, and included in bundled provisioning when using RealPresence Resource Manager.

You can configure the RealPresence Touch home screen in the system web interface.

**Procedure**

1. In the system web interface, go to **Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration**.
2. Configure the settings on the Home Screen Settings screen that are described in the following topics.

### Choose the Home Screen Icons

You can choose home screen icons for your RealPresence Centro system local interface. By default, two icon buttons appear in the lower center of the RealPresence Touch Home screen; users see only the Place a Call and Show Content icons. However, you can customize the number of screens and Home screen icons in a preferred order. Once you customize the Home screen configuration, users can scroll through one to three Home Screens, with up to three icons on each screen.

**Procedure**

1. In the web user interface, go to **Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration**.
2. Under Configure Home Screen, click Configure Home Screen Options.
3. At Home screen 1 > Button 1, select one to three icon buttons to appear per screen in your preferred order.

You can select from the following icon buttons:

- None (no icon)
- Place a Call
- Show Content
- Keypad
4. If you want to include more than one Home screen, continue selecting icon buttons for **Home Screen 2** and **Home Screen 3** until all screens are configured.

   For example, **Home Screen 1 > Button 1 > Recent Call Button 2 > Place a Call > Button 3 > Contacts**.

5. To save your selections, click **Save**.

   Your new selections should display on the Home screens of the RealPresence Touch device.

### Choose the Place a Call Screen Icons

You can customize the **Place a Call** screen to display certain icon buttons for your RealPresence Centro system. Since there are four ways to place a call by default, after you tap the **Place a Call** button, all the selections display on the screen. You can customize one of the icon buttons to be the default. All of the other **Place a Call** icon buttons continue to display at the top of the screen.

**Procedure**

1. In the system web interface, go to **Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration**.
2. Under **Configure Home Screen**, click **Place A Call Screen**.
3. Under **Select Preferred Sub Menu**, choose from the following:
   - Keypad
   - Contacts
   - Recent Calls
   - Speed Dials
4. Click **Save**.

   Your new selections should display on the RealPresence Touch Place a Call screen.

   To revert back to the default icons, at **Configure Home Screen**, select **Default Configuration**, and click **Save**.

### Change the Background Image

The RealPresence Touch device allows you to upload a custom background image that is separate from the RealPresence Centro system monitor background. If a custom image is not loaded, the image from the primary system screen displays as the RealPresence Touch device background when it is paired with the system (default behavior). To create a custom background on the RealPresence Touch, you must upload an image with pixel size of 1920 x 1080 (width by height) in a .jpg file format that is less than 5 MB.

**Procedure**

1. In the system web interface, go to **Admin Settings > General Settings > Home Screen Settings > RealPresence Touch Background**.
Setting Up and Configuring Directory Servers for the RealPresence Touch

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

Set Up Directory Servers for the RealPresence Touch

You can use the RealPresence Touch device to set up directory servers.

Procedure

1. In the RealPresence Touch web interface, go to Admin Settings > Servers > Directory Servers.
2. Configure the following settings:

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

<table>
<thead>
<tr>
<th>Directory Servers Supported</th>
<th>Authentication Protocols</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype for Business Server 2015</td>
<td>NTLM v2 only</td>
<td>Contact groups but not distribution lists</td>
<td>Might include: SIP address (SIP URI)</td>
</tr>
</tbody>
</table>

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

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

---

**Enable Skype for Business Mode**

After the Polycom® RealPresence Centro™ system is registered with the Skype for Business Server Online or On-premises, you can enable Skype mode.

When the Polycom® RealPresence Centro™ system is signed into Skype for Business Online, Skype mode is required and enabled automatically, and users can control the Polycom® RealPresence Centro™ system with the RealPresence Touch device. You cannot disable Skype Mode in Skype for Business Online deployments.

**Procedure**

1. In the Polycom® RealPresence Centro™ system web interface, go to **Admin Settings > General Settings > Home Screen Settings > Skype Mode**.
2. Select **Enable Skype mode**.
3. Click **Save**.
Disable Skype for Business Mode

You can disable Skype mode in the Polycom® RealPresence Centro™ system web interface. You cannot disable Skype Mode in Skype for Business Online deployments. To disable Skype for Business mode:

Procedure

1. In the Polycom® RealPresence Centro™ web interface, go to Admin Settings > General Settings > Home Screen Settings > Skype Mode.
2. Select Disable Skype mode.
3. Click Save.

Updating Software

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

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

For additional details on software compatibility, refer to the appropriate version of the release notes available at Polycom Support.

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

Update files for the RealPresence Touch are located on the Polycom support server. You can store the update files on a USB device, RealPresence Resource Manager system, or on your own web server. No license number or key is needed to update the RealPresence Touch.

You can configure the Polycom touch device to get software updates using any of the following methods:

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

Dynamic Polycom Touch Device Software Updates

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

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

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

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

Procedure

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

Managing Polycom Touch Device Software on Your Server

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

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

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

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

Set a Software Version as Current

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

Procedure

1. Run the setcurel 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/setcurel.sh X.X.X-XXX
   - Windows: <root dir>/vega/platform/setcurel.bat X.X.X-XXX
2. Follow the onscreen instructions for setting the current release.
Remove a RealPresence Touch Software Version

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

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

Update Software from the Web Interface

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

**Procedure**
1. Open a supported browser.
2. Configure the browser to allow cookies.
3. In the browser address line, enter the IP address of your RealPresence Touch device using the format `http://IPaddress` (for example, `http://10.11.12.13`).
4. Enter the Admin ID as the user name (default is admin), and then enter the Admin remote access password.
   The default password is the RealPresence Touch serial number.
   The first time you open the device web interface each day, and after you select any of the interface options, you might need to enter a user name and password.
5. On the device's 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**.
8. Click **Check for Software Updates**.
9. Click **Download and Install Software**.
   Download progress displays during installation.

Update Software from the Local Interface

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

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

Update RealPresence Touch Software from a USB Storage Device

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

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

Update the Software and the Factory Restore Partition From a USB Storage Device

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

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

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

- Use USB 2.0 devices (some USB 3.0 devices might not work with the RealPresence Touch).
- Format the primary partition as FAT32.
- Place all software update data into the root directory of the primary partition.

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

**Restart a RealPresence Touch Device**

You can restart a RealPresence Touch device when it’s paired with a RealPresence Centro system.

**Procedure**

1. On the device, go to **Settings > Administration**.
2. Enter the administrator password.
3. Tap **Restart Touch Controller**.

**Restart a System from a RealPresence Touch Device**

When the RealPresence Centro system is paired with a RealPresence Touch device and is enabled for Skype for Business, you can restart the room system using the RealPresence Touch device.

**Procedure**

1. On the RealPresence Touch device, navigate to **Settings > Administration**.
2. Enter the administrator password.
3. Under RealPresence Centro, tap **Restart Room System**.

**Troubleshooting the RealPresence Touch Device**

You might need to diagnose and troubleshoot issues with your RealPresence Touch device.

**View System Details and Connection Status**

You can view certain RealPresence Centro system details about the paired system on the RealPresence Touch; this information might be useful for troubleshooting or for technical support.

**Procedure**

1. On any screen on the RealPresence Touch, tap **Menu** and then **Settings**.
   
   The **System Information** screen is displayed.

2. Under **Device Connection Status**, tap the room system that you want information on.

System details and connection status information is listed for the connected room system.

**View Call Statistics**

When your RealPresence Centro system is paired with a RealPresence Touch, you might want to view certain call statistics, such as bitrates, compression formats, and packet loss during a call.

**Note:** In a Skype for Business call, for packet loss information, check the QoE report on the AVMCU server.
Procedure

1. During a call, on any screen, tap Call Statistics (located at the top left of your screen).
   Call statistics for each stream in the current call are now displayed.
2. To view statistics for another call participant, switch to that participant and tap Call Statistics again.
   To view more information about a specific stream, navigate to the desired stream and tap More Information.

Download RealPresence Touch Logs

You can download RealPresence Centro system logs using the RealPresence Touch.

Procedure

1. In the RealPresence Touch web interface, click Download Logs.
2. A .tar file is downloaded to your local computer.
   You can extract the file and open it to review the log information.

Transfer RealPresence Touch Logs to a USB Storage Device

You might find log files useful when troubleshooting. You can transfer RealPresence Touch logs to a USB storage device. The USB storage device must be in FAT32 format.

Procedure

1. Insert a USB storage device into the RealPresence Touch device.
2. On the RealPresence Touch device, do one of the following:
   • Tap Administration and enter the user name and password for the device.
   • Tap Menu > Administration and enter your user name and password.
3. Tap Transfer RealPresence Touch Logs to USB Device.
   A message displays while the logs are being transferred to the USB storage device.
   After a success message displays, click OK.

Perform a Factory Restore on the RealPresence Touch

If the RealPresence Touch device is not functioning correctly or you have forgotten the Administration password, you can use the factory restore button to reset the device. This operation completely erases the RealPresence Touch device's settings and reinstalls the default platform and applications. Do not power off the device during the factory restore process.

The restore button pinhole is on the back of the RealPresence Touch, as shown in the following figure.
Procedure
1. Disconnect the ethernet cable to power off the device.
2. Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
3. Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
4. Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
5. Follow the instructions on the setup wizard.
   When the process is complete, the device displays the splash screen and then the home screen.

Perform a Factory Restore Using a USB Storage Device

If you want to install a particular software build on the RealPresence Touch, you can perform a factory restore using a USB storage device. Do not power off the device during the factory restore process.

Procedure
1. Copy a build package (.tgz file) to the root directory of a USB storage device.
2. Disconnect the ethernet cable to power off the device.
3. Insert the USB storage device into the side USB port of the device.
4. Using a pin or paper clip, insert it into the pin hole, and press and hold the factory restore button.
5. Continue to hold the factory restore button for a full 5 seconds and connect the Ethernet cable.
6. Wait for the RealPresence Touch device to power on and display the setup wizard (also called the OOB, out-of-box wizard).
7. Follow the instructions on the setup wizard.
   When the process is complete, the device displays the splash screen and then the home screen.

Test the Software Download URL

If your RealPresence Centro system or Polycom touch device is not updating properly, and you entered polycom as the Server Address, the system resolves downloads.polycom.com to an IP address. The system then checks for a software update using http.

Procedure
1. Open a browser.
2. Try to access the appropriate URL for your system or device.
<table>
<thead>
<tr>
<th>System or Device</th>
<th>Test URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Touch</td>
<td><a href="http://downloads.polycom.com/video/rp_touch/vega/infotxt">http://downloads.polycom.com/video/rp_touch/vega/infotxt</a></td>
</tr>
<tr>
<td>RealPresence Centro</td>
<td><a href="https://downloads.polycom.com/video/centro/rseries/info.txt">https://downloads.polycom.com/video/centro/rseries/info.txt</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://downloads.polycom.com/video/centro/millennium/info.txt">https://downloads.polycom.com/video/centro/millennium/info.txt</a></td>
</tr>
</tbody>
</table>

3. If the computer returns platform, or apps and platform, you can reach the Polycom software server from your location and the URL is working.
System Maintenance

Topics:
- Managing System Profiles
- Resetting and Restoring a RealPresence Centro System
- Logs
- Retrieving Log Files
- Upgrading RealPresence Centro System Software
- Downgrading System Software

Managing System Profiles

If you manage systems that support multiple applications, you can use profiles to change RealPresence Centro system settings. You can store a system profile on a computer as a .profile file using the system web interface. The number of profiles you can save is unlimited. Polycom recommends only using profiles as a way to back up system settings. Attempting to edit a stored profile or upload a stored profile from one system to a different system can result in instability or unexpected results.

The following settings are included in a profile:
- Home screen settings
- User access levels
- Icon selections
- Option keys
- System behaviors

Passwords are not included when you store a profile.

Store a Setting Profile

You can store the current setting profile on your computer.

Procedure

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

Upload a Profile

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

Resetting and Restoring a RealPresence Centro System

If the RealPresence Centro system is not functioning correctly or you have forgotten the Admin Room Password, you can reset the system with Delete System Settings enabled. This procedure effectively refreshes your system, deleting all settings except the following:

- Current software version
- Remote control channel ID setting
- Directory entries
- CDR data and logs

Reset a RealPresence Centro System

You can reset a RealPresence Centro system in the local interface.

Procedure
1. Go to Settings > System Information > Diagnostics > Reset System.
2. Enable Delete System Settings.
3. Click Reset System.

After about 15 seconds, the system restarts and displays the setup wizard.

Perform a Factory Restore on the RealPresence Centro System

If the RealPresence Centro system is not functioning correctly, you can use the factory restore button to reset the system.

The factory restore operation completely erases the system's flash memory and reinstalls the software version and default configuration stored in its factory partition. The following items are erased from the system:

1. Software updates
2. All system settings including option keys and the remote control channel ID
3. Directory entries
4. CDR data
Procedure

1. Power off the system by using the power button on the front of the system. Do not unplug the power cord.
2. Straighten a paper clip and use the paper clip to press and hold the factory restore button. The restore button is located on the base of the system beneath the LAN port, as shown in the following figure.

3. While continuing to hold the restore button, press the power button and power on the system.
4. Continue holding the restore button until the base flashes blue and amber lights, then release it. The screen might stay blank for up to 3 minutes, and then displays the softupdate progress until the factory restore is complete. During this process, do not power off the system. When it is complete, the system restarts automatically.

Perform a Factory Restore Using a USB Storage Device

When you use the restore button to perform a factory restore, the system is restored to the software version placed on the system in the factory. You can perform a factory restore on the RealPresence Centro using two USB storage devices if you want to restore the system to the current software version, an earlier software version that is not the factory version, or change the default restore software version. The USB storage device must be in FAT32 format.

Procedure

1. Copy the software package (.tar file) and the software key (sw_keys.txt file) to the root directory of two different USB storage devices.
2. Power off the system. The power button is shown with a red circle in the following figure.
3. Insert the two USB storage devices into two service USB ports on the system. These ports are shown with red rectangles in the following figure.
4. Straighten a paper clip and use the paper clip to press and hold the restore button. The restore button is shown with the red arrow in the following figure.
5. While continuing to hold the restore button, press the power button and power on the system. During the factory restore process, the system indicators flash blue and amber, and the softupdate progress screen displays until the restore is complete. Do not power off the system during the factory restore process. When the process is complete, the system restarts automatically.

6. When the LEDs have stopped flashing and the install wizard (out of box) screen displays, the factory restore process is complete.

After the factory restore process is complete, remove the USB storage devices from the system. If you used a software version later than the factory software version, the software version used during the restore is now the default version for a factory restore of the system.

Delete Data and Configuration System Files

You can remove sensitive data and configuration information from the RealPresence Centro system for security purposes.

Procedure

1. Power off the RealPresence Centro system by holding down the Power sensor for 3 to 5 seconds.
2. Unplug all network connections.
3. Perform a factory restore.
4. Wait for the system to start up and display the setup wizard.
5. Power off the system.

Logs

Logs contain information about RealPresence Centro system activities and configurations to help you troubleshoot issues.

View Log File Status

You can view the log file status for your system in the system web interface.

Procedure

» In the system web interface, go to Diagnostics > System > System Status and select the More Info link for Log Threshold.
Configure System Log Management

When the system log fills past your configured threshold, the system triggers the following actions:

Procedure

1. In the system web interface, go to Admin Settings > Security > Log Management.
2. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Percent Filled</td>
<td>Displays as a percentage how full the logs are. When the logs are full, system deletes the oldest entries.</td>
</tr>
<tr>
<td>Percent Filled Threshold</td>
<td>Reaching the configured threshold triggers a notification, creates a log entry, and transfers the log if you set Transfer Frequency to Auto At Threshold. Off disables logging threshold notifications.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Specifies the folder name for log transfers. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- System Name and Timestamp—Folder name is the system name and the timestamp of the log transfer. For example, if the system name is Marketing, the folder name might be marketing_&lt;date_and_time&gt;.</td>
</tr>
<tr>
<td></td>
<td>- Timestamp—Folder name is the timestamp of the log transfer (e.g., &lt;yyyyMMddhhmmssSSS&gt;).</td>
</tr>
<tr>
<td></td>
<td>- Custom—Lets you specify a folder name for manual log transfers.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Specifies the type of storage device used for log file transfers.</td>
</tr>
<tr>
<td>Transfer Frequency</td>
<td>Specifies when the system transfers logs:</td>
</tr>
<tr>
<td></td>
<td>- Manual—The transfer starts when you select the Start Log Transfer button, which is visible only on the local interface. If the log fills before you transfer, new events overwrite the oldest events.</td>
</tr>
<tr>
<td></td>
<td>- Auto at Threshold—The transfer starts automatically when the system reaches the Percent Filled Threshold.</td>
</tr>
</tbody>
</table>

Configure System Log Level and Remote Logging

You can determine how the system logs capture device and server events.

Procedure

1. In the system web interface, go to Diagnostics > System > System Log Settings.
2. Configure the following settings and select Save.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Level</strong></td>
<td>Sets the minimum log level of messages stored in the system's flash memory. <strong>DEBUG</strong> logs all messages, while <strong>WARNING</strong> logs the fewest number of messages. Polycom recommends that you use the default value <strong>DEBUG</strong>. When you enable <strong>Enable Remote Logging</strong>, the log level is the same for both remote and local logging.</td>
</tr>
<tr>
<td><strong>Enable Remote Logging</strong></td>
<td>Specifies whether remote logging is enabled. Enabling this setting causes the 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 <strong>Save</strong>. The system supports remote logging encryption using TLS. If you use UDP or TCP transport, Polycom recommends remote logging only on secure, local networks.</td>
</tr>
</tbody>
</table>
| **Remote Log Server Address**  | Specifies the server address and port. If you don’t specify the port, the system uses a default destination port. The system determines the default port by how you configure **Remote Log Server Transport Protocol**:

- **UDP**: 514
- **TCP**: 601
- **TLS**: 6514

You can specify the address and port in the following formats:

- **IPv4 address**: `192.0.2.0:<port>`, where `<port>` is the elective destination port number in the 1-65535 range.
- **IPv6 address**: `[2001::abcd:1234]:<port>`, where `<port>` is the elective destination port number in the 1-65535 range.
- **FQDN**: `logserverhost.company.com:<port>`, where `<port>` is the elective destination port number in the 1-65535 range. |
| **Remote Log Server Transport Protocol** | Specifies the transport protocol for sending logs to a remote server:

- **UDP**
- **TCP**
- **TLS** (secure connection) |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable H.323 Trace</td>
<td>Logs additional H.323 connectivity information.</td>
</tr>
<tr>
<td>Enable SIP Trace</td>
<td>Logs additional SIP connectivity information.</td>
</tr>
<tr>
<td>Send Diagnostics and Usage Data to Polycom</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Retrieving Log Files

You might find log files useful when troubleshooting. You can generate log files for the RealPresence Centro systems and touch devices. The following related topics explain how to retrieve those log files.

#### Download System Log Files

You can use the RealPresence Centro system web interface to get system logs. The date and time of system log entries are shown in GMT.

**Procedure**

1. Go to Diagnostics > System > Download Logs.
2. Click Download system log and then specify a location on your computer to save the file.

   In the dialog boxes that appear, designate where you want the file to be saved.

#### Transfer System Log Files

You can transfer logs to a USB flash drive to free up space on your system.

**Procedure**

1. In the local interface, go to Settings > Administration > Security > Log Management.
2. Click Transfer System Log to USB Device.

    **Note:** Wait until the system displays a message that the log transfer has completed successfully before you remove the USB flash drive.

The system saves a file in the USB flash drive named according to the settings in the system web interface.

### SNMP Reporting

Systems support SNMP versions 1, 2c, and 3.

SNMP can provide the following event information about your system:

- Alert conditions located on the system alert screen
- Details of jitter, latency, and packet loss
- Low battery power in the remote control
- System power on
- Successful or unsuccessful administrator login
- Call fail for a reason other than a busy line
- User help request
- Video or audio call connection or disconnection

SNMPv3 does the following:
- Provides secure connections between the SNMP manager and agent
- Supports both IPv4 and IPv6 networks
- Logs all configuration change events
- Supports a user-based security model
- Supports trap destination addresses

Configure SNMP Management
You can monitor your system remotely with SNMP.

Procedure
1. In the system web interface, go to Admin Settings > Servers > SNMP.
2. Configure the following settings and select Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Enables administrators to monitor the system remotely using SNMP.</td>
</tr>
<tr>
<td>Enable Legacy Notifications</td>
<td>Supports sending notifications compatible with the legacy MIB.</td>
</tr>
<tr>
<td>Enable New Notifications</td>
<td>Supports sending notifications compatible with the new MIB.</td>
</tr>
<tr>
<td>Version1</td>
<td>Enables your system to use the SNMPv1 protocol.</td>
</tr>
<tr>
<td>Version2c</td>
<td>Enables your system to use the SNMPv2c protocol.</td>
</tr>
<tr>
<td>Version3</td>
<td>Enables your system to use the SNMPv3 protocol. Enabled by default, you can't configure other SNMPv3 settings unless this is on.</td>
</tr>
<tr>
<td>Read-Only Community</td>
<td>Specifies the SNMP community string for your system. For security reasons, don't use the default community string (public).</td>
</tr>
</tbody>
</table>

Note: Polycom doesn’t support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Name</td>
<td>Specifies the name of the person responsible for remotely managing the system.</td>
</tr>
<tr>
<td>Location Name</td>
<td>Specifies the system location.</td>
</tr>
<tr>
<td>System Description</td>
<td>Provides details about the system.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the User Security Model (USM) account name for SNMPv3 message transactions. The maximum length is 64 characters.</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>Specifies the type of SNMPv3 authentication algorithm used.</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Specifies the SNMPv3 authentication password. The maximum length is 48 characters.</td>
</tr>
<tr>
<td>Privacy Algorithm</td>
<td>Specifies the cryptographic privacy algorithm for SNMPv3 packets.</td>
</tr>
<tr>
<td></td>
<td>• CFB-AES128</td>
</tr>
<tr>
<td></td>
<td>• CBC-DES</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>Specifies the unique ID of the SNMPv3 engine. You might need this information to match the configuration of an SNMP console application. The ID is automatically generated, but you can create your own as long as it is between 10 and 32 hexadecimal digits. You can separate each group of two hex digits by a colon (:) 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 (for example, :F: is equivalent to :0f:). The ID can't be all zeros or Fs.</td>
</tr>
<tr>
<td>Listening Port</td>
<td>Specifies the port SNMP uses to listen for system messages (the default is port 161).</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Specifies the transport protocol used.</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
**Destination Address1** | Specifies the IP addresses of SNMP managers where SNMP traps are sent.
**Destination Address2** | Each address has four settings:
- IP address (accepts IPv4 and IPv6 addresses, hostnames, and FQDNs)
- Message type (TRAP or INFORM)
- Protocol (SNMP v1, v2c, or v3)
- Port where SNMP traps are sent (default is 162)
**Destination Address3** | Disabling the Port setting also disables the corresponding destination address.

### Download MIBs for SNMP Management
You can download MIB data for your system.

A MIB helps your SNMP management console resolve SNMP traps and provide human-readable descriptions of those traps.

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

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

Be aware of these points when performing system upgrades:
- If you did not purchase additional system options, you need only to provide a serial number to activate the software. You do not need an option key.
- If you do not have a support agreement, contact an authorized Polycom dealer to get an upgrade key.
- For DoD Unified Capabilities Approved Product List (UC APL) software releases, go to www.polycom.com/solutions/industry/federal_government/certification_accreditation.html.

Ensure you have the required information ready before you begin installing and activating software updates or options:
- License numbers and system serial numbers.
- Software or option keys. Obtain these by logging in to Polycom Support and requesting them from the Activation/Upgrade link. If you do not have a support agreement, contact an authorized Polycom dealer to get a key.
RealPresence Centro systems perform several internal restarts while running software updates. Each restart takes about 2 or 3 minutes and improves the reliability of the update process by freeing up memory. If you are updating a system using a web browser, the internal restart is not visible from the system web interface.

You can downgrade software to an earlier version at any time.

You need an account on Polycom Support before you begin. Be sure to set up an account if you don't already have one.

Serial and License Numbers

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

- The 14-digit serial number is the unique number that identifies your system. You can find it on the System Information screen and on a label on the system. Serial numbers are case sensitive.
- The license number is the number that you receive when you purchase a software update or system option. License numbers have the following format:
  
  Software update license: U1000-0000-0000-0000-0000
  System option license: K1000-0000-0000-0000-0000

Create a Serial and License Number File for Multiple Systems

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

Procedure

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

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

license number<TAB>system serial number

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

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

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

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

A text file with only serial numbers might look like this:
Software or System Option Keys

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

There are two types of keys:

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

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

Update System Software from a USB Storage Device

You can use a USB storage device to update one or multiple systems with a setup wizard to guide you through the process.

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

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

Procedure

1. If you are updating to a major or minor release (x.y), obtain keys (.txt) for each system that you want to update from the Polycom website.
2. Save the text file as sw_keys.txt and place it in the root directory of the USB storage device.
3. Open a browser and navigate to Polycom Support.
4. Under Documents and Downloads, select Telepresence and Video.
5. Navigate to the page that has the desired update for your system.
6. Save a software package (.tar) file from the Polycom website to the root directory of a USB storage device.
7. 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.
8. Click OK.
   - Follow the setup wizard instructions to complete the update.

Update System Software from a .tar File

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

Procedure

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

Downgrading System Software

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

If your system is not provisioned, you can put the software package on a USB device to downgrade the system to an earlier version.

Determine the Software Version

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

Procedure
   » In the local interface, go to Settings > System Information > Information > System Detail or click the System link in the system web interface.

Delete System Settings

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

Procedure
   » In the local interface, go to Settings > System Information > Diagnostics > Reset System and select Delete System Settings.
General Troubleshooting

The following table provides general troubleshooting information, including symptoms, problems and possible solutions for your RealPresence Centro system.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The system does not respond to the remote control.</td>
<td>The remote control battery is not charged.</td>
<td>Charge the remote control battery.</td>
</tr>
<tr>
<td></td>
<td>The room lights operate in the 38 Kz range and interfere with the remote control signals.</td>
<td>Turn off the room lights and try the remote control again.</td>
</tr>
<tr>
<td></td>
<td>A touch control device, such as the RealPresence Touch, might be paired to the room system.</td>
<td>Only one device can be paired at a time. To use the remote control, unpair the touch control device.</td>
</tr>
<tr>
<td></td>
<td>When configured for Skype for the Business/Office 365 user experience, the system is paired to the RealPresence Touch device.</td>
<td>When the system is configured for Skype Mode by the system administrator, use the RealPresence Touch as the only control device.</td>
</tr>
</tbody>
</table>
### Troubleshooting

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picture is blank on the main monitor.</td>
<td>The room system is sleeping. This is normal after a period of inactivity.</td>
<td>Pick up the remote control to wake up the system.</td>
</tr>
<tr>
<td>The monitor remains blank after you pick up the remote control.</td>
<td>The monitor is powered off.</td>
<td>Power on the monitor.</td>
</tr>
<tr>
<td></td>
<td>The monitor's power cord is not plugged in.</td>
<td>Connect the monitor's power cord and the power on the monitor.</td>
</tr>
<tr>
<td></td>
<td>The monitor is not correctly connected to the room system.</td>
<td>Verify that the monitor is connected correctly according to the set up sheet that you received with the system.</td>
</tr>
<tr>
<td>You lost the administration password for your system or device.</td>
<td>You cannot access the administration settings without a valid password.</td>
<td>Refer to the factory restore topics to learn how to reset your system.</td>
</tr>
<tr>
<td>The system is experiencing video issues during calls, such as packet loss.</td>
<td>You have not configured the Network Quality settings in the system web interface.</td>
<td>Refer to the following Lost Packet Recovery topic link.</td>
</tr>
</tbody>
</table>

### View Remote Sessions on the System

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

**Procedure**

1. In the system web interface, go to **Diagnostics > System > Sessions**.
2. In the system web interface, go to **Admin Settings > General Settings > Date and Time > Time in Call**.
3. Configure these settings.

### Placing a Test Call

To test a feature that is only available in an active video call, you can call a Polycom test number.

Polycom support is available to assist you when you encounter difficulties. First though, If you are having problems making a call, try the troubleshooting tips and then call our test numbers. When you finish configuring the RealPresence Centro system, you can call a Polycom video site to test your setup.

You can find a list of worldwide numbers that you can use to test your system at [www.polycom.com/videotest](http://www.polycom.com/videotest).

When placing test calls, try these ideas:

- Make sure the number you dialed is correct, then try the call again. For example, you might need to dial 9 for an outside line or include a long distance access or country code.
• To find out if the problem exists in your system, ask the person you were trying to reach to call you instead.
• Find out if the system you are calling is powered on and is functioning properly.
• If you can make calls but not receive them, make sure that your system is configured with the correct number.

Top LED Light Ring on the RealPresence Centro System

The top light ring indicates where the active speaker has been detected. It gives a visual notification to participants in the room, telling them which speaker is active.

<table>
<thead>
<tr>
<th>Indicator Light</th>
<th>System Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED off</td>
<td>No video is being sent to the far-end site in a call</td>
</tr>
<tr>
<td>Amber</td>
<td>Sleep</td>
</tr>
<tr>
<td>Blue</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>Not in a call</td>
</tr>
<tr>
<td>Green</td>
<td>In an audio or a video call</td>
</tr>
<tr>
<td>Red</td>
<td>Microphones muted</td>
</tr>
<tr>
<td>Blinking blue</td>
<td>System starting</td>
</tr>
<tr>
<td>Blinking blue and amber</td>
<td>Software update</td>
</tr>
</tbody>
</table>

RealPresence Centro System Status and LED Indicators

The RealPresence Centro system has LED indicators at the bottom of the system to let you know whether the system is in standby mode, active, or in a call. The following table lists the LED indicators that display on the system and the status associated with each indicator.

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No LED</td>
<td>The system is off.</td>
</tr>
<tr>
<td>Amber</td>
<td>The system is sleep or in standby mode.</td>
</tr>
<tr>
<td>Blue</td>
<td>The system is on, but not in a call.</td>
</tr>
<tr>
<td>Red</td>
<td>The system is on or in an audio or video call with the microphones muted.</td>
</tr>
<tr>
<td>Green</td>
<td>The system is in an audio or a video call.</td>
</tr>
<tr>
<td>Blinking green</td>
<td>The system is in a call with the video muted.</td>
</tr>
</tbody>
</table>
EagleEye Producer Indicator Lights

An LED is integrated into the front of the EagleEye Producer unit. Different LED lights refer to different system states. These allow you to identify the current system state for the EagleEye Producer system. Detailed LED and system states mappings are shown in the following table.

<table>
<thead>
<tr>
<th>LED Indicator Lights System State</th>
<th>LED</th>
<th>System State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Blue Power On, EagleEye Producer Normal State</td>
<td></td>
</tr>
<tr>
<td>Blinking Blue</td>
<td>Blinking Blue On, Not in a Call, Receive IR EagleEye Producer Boot Up</td>
<td></td>
</tr>
<tr>
<td>Fast Blinking Blue</td>
<td>Fast Blinking Blue Calibrate Webcam Room View</td>
<td></td>
</tr>
<tr>
<td>Amber</td>
<td>Amber Standby - Asleep</td>
<td></td>
</tr>
<tr>
<td>Alternate Amber and Blue</td>
<td>Alternate Amber and Blue Software update, Factory restore, USB image update</td>
<td></td>
</tr>
<tr>
<td>Blinking Amber</td>
<td>Blinking Amber USB disk plugged in</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>Green On, In a call</td>
<td></td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Blinking Green On, In a call, Receive IR in a call</td>
<td></td>
</tr>
<tr>
<td>Fast Blinking Red</td>
<td>Fast Blinking Red System error</td>
<td></td>
</tr>
<tr>
<td>Blink</td>
<td>Blink Blink Needs attention, Receive IR</td>
<td></td>
</tr>
</tbody>
</table>

Audio and Video Tests

You can perform audio and video diagnostic tests on your system.

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speaker Test</td>
<td>Tests the audio cable connections. A 473 Hz tone indicates that the local audio connections are correct. If you run a test during a call, people on the far site also hear the test tone.</td>
</tr>
</tbody>
</table>
## Diagnostic Screen

<table>
<thead>
<tr>
<th><strong>Diagnostic Screen</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Audio Meters          | Measures the strength of audio signals from microphones, far-site audio, and any device connected to the audio line in.  
                         Meters function only when the associated input is enabled.  
                         Note: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system. |
| Camera Tracking       | Provides diagnostics specific to the EagleEye Director, if the camera is connected to the system.  
                         **Audio**  
                         • Verifies microphone functionality. To use this feature, speak aloud and verify that you can see dynamic signal indications for two vertical microphones and five horizontal microphones. If no signal indication appears for a specific microphone, manually power off the EagleEye Director and then power it back on.  
                         • Also verifies the reference audio signal: Set up a video call. Let the far side speak aloud and verify that you can see dynamic signal indications for the two reference audio meters. If no signal indication appears for a specific microphone, firmly connect the reference cable.  
                         After you verify microphone functionality, calibrate the camera again.  
                         **Video**  
                         • **Left Camera** shows video from the left camera.  
                         • **Right Camera** shows video from the right camera.  
                         • **Color Bars** displays the color bar test screen.  
                         Note: If you connect EagleEye Director but don’t selected it as the current camera source, this choice doesn’t display on the screen. |

---

### Audio Meters on the RealPresence Centro System

Audio meters indicate the strength of the audio input and output of your microphones, far-site audio, and any device connected to the audio ports. To avoid or fix audio distortion, you can configure the Audio Meter setting in the local or web RealPresence Centro system interface.
The meters allow you to identify front, back, left, and right audio channels. To determine which side of the RealPresence Centro system is the front, refer to the following figure. Note that when you face the front of the system, the removable corner is on the lower right side of the base.

![Diagram of audio channel references](image)

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Front audio channel</td>
</tr>
<tr>
<td>2</td>
<td>Left audio channel</td>
</tr>
<tr>
<td>3</td>
<td>Back audio channel</td>
</tr>
<tr>
<td>4</td>
<td>Right audio channel</td>
</tr>
</tbody>
</table>

### Set Audio Meter Levels

You can set audio meter levels for your RealPresence Centro system so that normal and loud audio peaks are within an acceptable audio range.

**Procedure**

1. Do one of the following:
   - In the system web interface, go to Diagnostics > Audio and Video Tests > Audio Meter.
   - In the local interface, go to Settings > System Information > Diagnostics > Audio Meter.
2. To test the audio levels, do one of the following:
   - To check the near-site audio, speak into your microphones.
   - To check the far-site audio, ask a call participant to speak or call a phone in the far-site room to hear it ring.
3. For normal speech and program material, set the audio signal levels so that you see peaks between +3 dB and +7 dB.
   
   Occasional peaks of +12 dB to +16 dB with loud transient noises are acceptable. If you see +20 on the audio meter, the audio signal is 0 dBFS and the audio might be distorted. A meter reading of +20dB corresponds to 0dBFS in the room system audio. A signal at this level is likely clipping the audio system.
System Diagnostics
To assist in troubleshooting, you can view RealPresence Centro system diagnostics in either the system web interface or the local interface.

Access Diagnostic Screens in the Web Interface
You can access RealPresence Centro system diagnostics in the system web interface.

Procedure
1. In the system web interface, go to **Diagnostics** > **System** > **System Status**.
2. For details, click **More Info**.

Access Diagnostic Screens in the Local Interface
You can access RealPresence Centro system diagnostics in the system local interface.

Procedure
» In the system local interface, select **Settings** > **System Information** > **Diagnostics**.

This screen includes the following system diagnostic details:

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near End Loop</td>
<td>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 is sent to the far site in a call. This test is not available when you are in a call.</td>
</tr>
<tr>
<td>Ping</td>
<td>Tests whether the system can connect with a far-site IP address that you specify. PING returns abbreviated Internet Control Message Protocol results. It returns H.323 information only if the far site is configured for H.323. It returns SIP information only if the far site is configured for SIP. If the test is successful, the system displays a message.</td>
</tr>
<tr>
<td>Trace Route</td>
<td>Tests the routing path between the local system and the IP address entered. If the test is successful, the system lists the hops between the system and the IP address you entered.</td>
</tr>
<tr>
<td>Diagnostic Screen</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Color Bars</td>
<td>Tests the color settings of your monitor for optimum picture quality. If the color bars generated during the test aren’t clear or the colors don’t look correct, adjust the monitor settings.</td>
</tr>
<tr>
<td>Speaker Test</td>
<td>Tests the audio cable connections. A 473 Hz tone indicates that the local audio connections are correct. If you run a test during a call, people on the far site also hear the test tone.</td>
</tr>
<tr>
<td>Audio Meters</td>
<td>Measures the strength of audio signals from microphones, far-site audio, and any device connected to the audio line in. Meters function only when the associated input is enabled. Note: Some audio meters are unavailable when a SoundStructure digital mixer is connected to the room system.</td>
</tr>
</tbody>
</table>
## Diagnostic Screen

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera Tracking</td>
<td>Provides diagnostics specific to the EagleEye Director, if the camera is connected to the system.</td>
</tr>
</tbody>
</table>

### Audio
- Verifies microphone functionality. To use this feature, speak aloud and verify that you can see dynamic signal indications for two vertical microphones and five horizontal microphones. If no signal indication appears for a specific microphone, manually power off the EagleEye Director and then power it back on.
- Also verifies the reference audio signal: Set up a video call. Let the far side speak aloud and verify that you can see dynamic signal indications for the two reference audio meters. If no signal indication appears for a specific microphone, firmly connect the reference cable.

After you verify microphone functionality, calibrate the camera again.

### Video
- **Left Camera** shows video from the left camera.
- **Right Camera** shows video from the right camera.
- **Color Bars** displays the color bar test screen.

**Note:** If you connect EagleEye Director but don’t select it as the current camera source, this choice doesn’t display on the screen.

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Displays the following information about each session connected to the system:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Connection type, such as web or local interface</td>
</tr>
<tr>
<td></td>
<td>ID associated with the session, typically Admin or User</td>
</tr>
<tr>
<td></td>
<td>Remote IP address (addresses of people logged in to the system from their computers)</td>
</tr>
</tbody>
</table>
### Diagnostic Screen

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
</table>
| Reset System      | **Note:** Do not use this setting unless your administrator tells you to do so. Even if a password is already set, enter the password again to reset the system. Returns the system to its default settings. When you select this setting using the remote control, you can do the following:  
  - Keep your system settings (such as system name and network configuration) or restore system settings.  
  - Keep or delete the directory stored on the system. System reset does not affect the global directory.  
  - Keep or delete all PKI certificates and certificate revocation lists (CRLs). Before you reset the system, you might ask your administrator to download the Call Detail Report (CDR) and CDR archive. For more information about these reports, contact your administrator. |

---

### Viewing System Details on the Local Interface

You might need to view certain RealPresence Centro system details on the local interface to do video conferencing tasks, such as pairing, or to perform troubleshooting tests to provide information for your own testing or for technical support. You can also review information about calls, network usage, and performance on the various system screens in the local interface.

Available system menus vary based on how your administrator configured the system. Therefore, this section might describe settings that you cannot access on your system. To find out more about these settings, please talk to your administrator.

The System Information screen has the following choices:

- Information
- Status
- Diagnostics
- Call Statistics (in a call only)

### Access the Information Screen

You can access RealPresence Centro system status screen in the local interface.

**Procedure**

» Go to 📦 > **System Information** > **Information** to view the following system details.
## Diagnostic Screen Description

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
</table>
| System Detail     | Displays the following system information:  
  - System Name  
  - Model  
  - Hardware Version  
  - System Software  
  - Serial Number  
  - MAC Address  
  - IP Address |
| Network           | Displays the following network information:  
  - IP Address  
  - Host Name  
  - 323 Name  
  - 323 Extension (E.164)  
  - SIP Address  
  - Link-Local  
  - Site-Local  
  - Global Address |
| Usage             | Displays the following usage information:  
  - Time in Last Call  
  - Total Time in Calls  
  - Total Number of Calls  
  - System Up Time |

## Access the Status Screen

You can access RealPresence Centro system status screen in the local interface.

### Procedure

» Go to 🗄 > **System Information** > **Status**.

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for the out of a call status:
<table>
<thead>
<tr>
<th>Status Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Alerts</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Call Control</strong></td>
<td>Displays the status of the Auto-Answer Point-to-Point Video and Meeting Password settings.</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>Displays the connection status of audio devices such as the microphones and SoundStation IP.</td>
</tr>
<tr>
<td><strong>VisualBoard</strong></td>
<td>Displays the connection status of the VisualBoard, if one is connected. If VisualBoard is not connected, this choice is not visible on the screen.</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td>Displays the connection status of the IP network.</td>
</tr>
</tbody>
</table>
| **Servers** | • Always displays the Gatekeeper and SIP Registrar Server.  
• Displays the active Global Directory Server, LDAP Server, or Microsoft Server.  
• If enabled, displays the Provisioning Service, Calendaring Service, or Presence Service. |
| **Log Management** | Displays the status of the Log Threshold setting. You can download system logs, call detail reports, and configuration profiles using the system web interface. |

When a system device or service encounters a problem, you see an alert next to the Settings button on the menu. This screen includes the following system status details for in a call status:

- When a change occurs in the system status or a potential problem exists, you see an alert next to the **System** button on the menu.

<table>
<thead>
<tr>
<th>Status Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Call Statistics</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
View Call Statistics for an Active Point-to-Point Call With the Remote Control

You might need to view call statistics on the RealPresence Centro system local interface to do some troubleshooting for users. You can only view call statistics during a call. During a point-to-point call, you can view call statistics about a call participant or about an active stream. As a shortcut during a call, press the **Back** button on your remote control for two or more seconds to display the Call Statistics screen.

**Procedure**

» Go to System Information > Call Statistics.

Streams associated with the participant are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and select **More Information**.

View Call Statistics for an Active Multipoint Call with the Remote Control

During a RealPresence Centro system multipoint call, you can view call statistics about any of the call participants or about an active stream.

**Procedure**

1. Go to System Information > Call Statistics.

A list of participants in the call displays.

2. Do one of the following:

   • To view a participant's details, select **Participants**, navigate to the desired participant, and select **More Information**. The participants' active streams are displayed beneath the participant information.

   • To quickly access information about a particular stream or streams associated with a particular user, navigate to **Streams** for calls using Advanced Video Coding (AVC) or **Participant Streams** for calls using Scalable Video Coding (SVC). Use the **Back** and **Next Participant** buttons to navigate to the participant with the stream or streams you want to view. Navigate to the desired stream and select **More Information**.

   • To quickly access a list of all active audio, video, and content streams within the call, navigate to **Active Streams** (available in SVC calls only). Select the desired stream, and select **More Information**.

View Call Statistics for an Active Multipoint Call on the Polycom Touch Control

During a multipoint call, you can view call statistics about any of the call participants or about an active stream.

**Procedure**

1. Touch **Participants**. A list of participants in the call displays.

2. Touch **View Call Statistics** and do one of the following:

   • To view a participant's details, navigate to the desired participant, and touch **i**.
The participants’ active streams are displayed beneath the participant information. To view more information about a specific stream, navigate to the desired stream and touch "I".

From an individual stream view you can select Next Stream to view the next stream in the stream list. To quickly access a list of all active audio, video, and content streams within the call, navigate to Active Streams. This setting is available in SVC calls only. Select the desired stream and touch "I".

Provisioning Service Registration Failure

If automatic provisioning is enabled but the RealPresence Centro system does not register successfully with the provisioning service, you might need to change the Domain, User Name, Password, or Server Address used for registration. For example, users might be required to periodically reset passwords used to log into the network from a computer. If such a network password is also used as the provisioning service password, you must also update it on the system. To avoid unintentionally locking a user out of network access in this case, systems do not automatically retry registration until you update the settings and register manually on the Provisioning Service screen.

Call Detail Report (CDR)

When enabled, the Call Detail Report (CDR) feature keeps a record of every incoming, outgoing, and missed call that occurs on the system. 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 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 of 150 entries is not exceeded and records are not lost.

The size of a CDR can become unmanageable if you don't download the record periodically. A full report with 150 entries results in a CDR of approximately 50 KB. Your connection speed can also affect how fast the CDR downloads. You can set up a schedule to download and save the CDR after every 120 calls to keep track of all call entries and make the file easy to download and view.

Note: The RealPresence Resource Manager system captures CDR information for the EagleEye Producer and the EagleEye Director II cameras and generates it to the RealPresence Resource Manager system CDR. The call details include People Minutes and People Count (Call Begin) at the beginning of a call and People Count (Peak Value) at the end of a call.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row ID</td>
<td>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.</td>
</tr>
<tr>
<td>Start Date</td>
<td>The call start date, in the format dd-mm-yyyy.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The call start time, in 24-hour format hh:mm:ss.</td>
</tr>
<tr>
<td>End Date</td>
<td>The call end date.</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End Time</td>
<td>The call end time.</td>
</tr>
<tr>
<td>Call Duration</td>
<td>The length of the call.</td>
</tr>
<tr>
<td>Account Number</td>
<td>If <strong>Require Account Number to Dial</strong> is enabled on the system, the value entered by the user is displayed in this field.</td>
</tr>
<tr>
<td>Remote System Name</td>
<td>The far site’s system name.</td>
</tr>
<tr>
<td>Call Number 1</td>
<td>The number dialed from the first call field, not necessarily the transport address.</td>
</tr>
<tr>
<td></td>
<td>For incoming calls — The caller ID information from the first number received from a far site.</td>
</tr>
<tr>
<td>Call Number 2</td>
<td>For outgoing calls — The number dialed from the second call field, not necessarily the transport address.</td>
</tr>
<tr>
<td></td>
<td>For incoming calls — The caller ID information from the second number received from a far site.</td>
</tr>
<tr>
<td>Call Rate</td>
<td>The type of call — Either H.323 (IP) or SIP.</td>
</tr>
<tr>
<td>System Manufacturer</td>
<td>The name of the system manufacturer, model, and software version, if they can be determined.</td>
</tr>
<tr>
<td>Call Direction</td>
<td>In—For calls received.</td>
</tr>
<tr>
<td></td>
<td>Out—For calls placed from the system.</td>
</tr>
<tr>
<td>Conference ID</td>
<td>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.</td>
</tr>
<tr>
<td>Call ID</td>
<td>Identifies individual calls within the same conference.</td>
</tr>
<tr>
<td>Total H.320 Channels Used</td>
<td>Number of narrow-band channels used in the call.</td>
</tr>
<tr>
<td>Endpoint Alias</td>
<td>The alias of the far site.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Polycom use only.</td>
</tr>
<tr>
<td>View Name</td>
<td>Names the web or local interface used in the call.</td>
</tr>
<tr>
<td>User ID</td>
<td>Lists the ID of the user who made the call.</td>
</tr>
<tr>
<td>Endpoint Transport Address</td>
<td>The actual address of the far site (not necessarily the address dialed).</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audio Protocol (Tx)</td>
<td>The audio protocol transmitted to the far site, such as G.728 or G.722.3.</td>
</tr>
<tr>
<td>Audio Protocol (Rx)</td>
<td>The audio protocol received from the far site, such as G.728 or G.722.</td>
</tr>
<tr>
<td>Video Protocol (Tx)</td>
<td>The video protocol transmitted to the far site, such as H.263 or H.264.</td>
</tr>
<tr>
<td>Video Protocol (Rx)</td>
<td>The video protocol received from the far site, such as H.261 or H.263.</td>
</tr>
<tr>
<td>Video Format (Tx)</td>
<td>The video format transmitted to the far site, such as CIF or SIF.</td>
</tr>
<tr>
<td>Video Format (Rx)</td>
<td>The video format received from the far site, such as CIF or SIF.</td>
</tr>
<tr>
<td>Disconnect Local ID and Disconnect Reason</td>
<td>The identity of the user who initiated the call and the reason the call was disconnected.</td>
</tr>
<tr>
<td>Q.850 Cause Code</td>
<td>The Q.850 cause code showing how the call ended.</td>
</tr>
<tr>
<td>Total H.320 Errors</td>
<td>The number of H.320 errors experienced during the call.</td>
</tr>
<tr>
<td>Average Percent of Packet Loss (Tx)</td>
<td>The combined average of the percentage of both audio and video packets transmitted that were lost during the five 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.</td>
</tr>
<tr>
<td>Average Percent of Packet Loss (Rx)</td>
<td>The combined average of the percentage of both audio and video packets received that were lost during the five 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.</td>
</tr>
<tr>
<td>Average Packets Lost (Tx)</td>
<td>The number of packets transmitted that were lost during a call.</td>
</tr>
<tr>
<td>Average Packets Lost (Rx)</td>
<td>The number of packets from the far site that were lost during a call.</td>
</tr>
<tr>
<td>Average Latency (Tx)</td>
<td>The average latency of packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Average Latency (Rx)</td>
<td>The average latency of packets received during a call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Maximum Latency (Tx)</td>
<td>The maximum latency for packets transmitted during a call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Maximum Latency (Rx)</td>
<td>The maximum latency for packets received during a call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Average Jitter (Tx)</td>
<td>The average jitter of packets transmitted during a call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Average Jitter (Rx)</td>
<td>The average jitter of packets received during a call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Maximum Jitter (Tx)</td>
<td>The maximum jitter of packets transmitted during a call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Maximum Jitter (Rx)</td>
<td>The maximum jitter of packets received during a call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Call Priority</td>
<td>The AS-SIP call precedence level assigned to the call (populated only when AS-SIP is enabled on the system).</td>
</tr>
</tbody>
</table>

### Download a Call Detail Report (CDR)

You can download a CDR using the RealPresence Centro system web interface.

**Procedure**

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

### Troubleshoot a Manual System Software Update

If your system does not successfully perform a software update, you can use Polycom best practices to troubleshoot the issue.

If you entered `polycom` as the server address, it should resolve as `downloads.polycom.com` to an IP address using DNS. The RealPresence Centro system then checks for a software update using http protocol. If this does not occur, do the following.
Procedure

1. On a local computer, open a supported browser on the same network as the system.
   a. If successful, it will return platform, which signifies that you can connect to the Polycom software server from your location.
   b. If not successful, you did not connect to the Polycom server. Your network might be blocking the link; contact your IT department to help troubleshoot the issue. If this does not resolve the problem, the server might be down. Contact Polycom Support to learn the server status.

Knowledge Base

For more troubleshooting information for your RealPresence Centro system, you can search the Knowledge Base at Polycom Support.

Before You Contact Polycom Technical Support

If you are not able to make test calls successfully and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support at Polycom Support.

Enter the following information about your RealPresence Centro system, then ask a question or describe the problem. This information helps us to respond faster to your issue. In addition, please provide any diagnostic tests or troubleshooting steps that you have already tried.

Locate the System Serial Number

You can view the system serial number on the local interface of the RealPresence Centro system.

Procedure

» To locate the system serial number (14 digits), go to Settings > System Information > Information > System Detail or locate the number on the back of the system.

Locate the Software Version

You can view the software version on the local interface of the RealPresence Centro system.

Procedure

» To locate the software version, go to Settings > System Information > Information > System Detail.

Locate Active Alert Messages

You can view the active alert messages on the local interface of the RealPresence Centro system.

Procedure

» To locate the active alert messages, go to Settings > System Information > Status > Active Alerts for messages generated by your system.
Located the IP Address and H.323 Extension Settings

You can view IP Address and H.323 extension settings on the local interface of the RealPresence Centro system.

Procedure

» To locate the IP Address and H.323 Extension settings, go to Settings > System Information > Information > Network.

Located the LAN Status

You can view the LAN status on the local interface of the RealPresence Centro system.

Procedure

» In the system web interface, go to Settings > System Information > Status > LAN.

Located Diagnostics on the Local Interface

You can view diagnostics on the local interface of the RealPresence Centro system.

Procedure

» In the system local interface, go to Settings > System Information > Diagnostics.

Contacting Technical Support

If you are not able to make test calls successfully on your RealPresence Centro system and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support.

To contact Polycom Technical Support, go to Polycom Support.

Enter the following information, then ask a question or describe the problem. This information helps us to respond faster to your issue:

• The 14-digit serial number from the System Detail screen or the back of the system
• The software version from the System Detail screen
• Any active alerts generated by the system
• Information about your network
• Troubleshooting steps you have already tried

You can find the system detail information in the local interface by going to Settings > System Information > Information or in the system web interface by clicking System in the blue bar at the top of the system web interface screen.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components, such as RealPresence Centro systems, only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers successfully design, deploy, optimize, and manage
Polycom visual communication within their third-party UC environments. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook, Skype for Business Server 2015 integrations. For additional information and details please refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.
The following section provides information on the RealPresence Centro system back panel views.

**Polycom RealPresence Centro System**

This following figure and table shows how the system web interface settings relate to hardware input and outputs for the RealPresence Centro system. Polycom recommends that you use either the HDMI or VGA video input, but not both.

![RealPresence Centro System Back Panel](image)

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Location in Web Interface:</th>
<th>Input/ Output</th>
<th>Supported Formats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Audio/Video &gt; Video Inputs &gt; Input 2</td>
<td>Video Input 2/Audio Input 1</td>
<td>HDMI version 1.3</td>
<td>Main video and audio input</td>
</tr>
<tr>
<td></td>
<td>Audio/Video &gt; Audio &gt; Audio Input &gt; Type: HDMI</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Polycom, Inc.
<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Location in Web Interface:</th>
<th>Input/ Output</th>
<th>Supported Formats</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2           | Audio/Video > Monitors > Monitor 2 | Video Output 2 | • HDMI version 1.3  
• DVI-D | Output for Monitor 2; does not include audio |
| 3           | N/A                        | USB connections | USB 3.0 | Use these ports for the following tasks:  
• Connect secondary touch monitors  
• Perform software updates  
• Charge the remote control battery |
| 4           | Audio/Video > Video Inputs > Input 2 | Video Input 2 | VGA | Video input for Content |
| 5           | Audio/Video > Audio > Audio Input > Type: 3.5mm | Audio Input 2 | 3.5mm Stereo | Stereo line-level input  
3.5mm audio is independent and not associated with any video input |
<p>| 6           | N/A                        | Microphone Input | Polycom Microphone | Audio input for up to two Polycom microphone arrays or a SoundStructure mixer; supports up to 3 ceiling microphones for Acoustic Fence Technology |
| 7           | General Settings &gt; Serial Ports | Serial Port | RS-232 | Serial port |
| 8           | Network &gt; LAN Properties | LAN Port | Ethernet | Connectivity for IP calls, People +Content IP, and the system web interface |</p>
<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Location in Web Interface: Admin Settings &gt; Input/ Output</th>
<th>Supported Formats</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9           | N/A USB connection                                       | USB 2.0           | Main service port. Use this port for the following tasks:  
|             |                                                          |                   | • Perform a software update using a USB storage device  
|             |                                                          |                   | • Perform a factory restore using a USB storage device  
|             |                                                          |                   | **Note:** For a factory restore, insert one USB storage device into this port, and the other USB storage device into the port at Ref. number 11. |
| 10          | N/A Power Input                                          | 12 0/240 VAC      | Power input  |
| 11          | N/A USB connection                                       | USB 2.0           | Use this port only to perform a factory restore using a USB storage device. Insert one USB storage device into this port, and the other USB storage device into the port at Ref. number 9.  
|             |                                                          |                   | **Note:** This port cannot be used to perform a software update using a USB storage device. |
| 12          | N/A                                                      | N/A               | Factory restore button  |
| 13          | N/A Power button                                         | N/A               | Power the system on and off  |
# Port Usage

**Topics:**
- Inbound Ports for RealPresence Group Series
- Outbound Ports for RealPresence Group Series

## Inbound Ports for RealPresence Group Series

IP port usage information for your system is important when you are setting up new videoconferencing equipment and you must know the type, protocol, or function of the port, and if it is configurable.

The following table shows the IP port usage for inbound traffic to RealPresence Centro systems.

<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>On By Default?</th>
<th>Enable/Disable?</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Static</td>
<td>TCP</td>
<td>Secure API</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Settings &gt; Security&gt; Global Security &gt; Access Enable SSH Access: Enable to open port 22</td>
</tr>
<tr>
<td>23</td>
<td>Static</td>
<td>TCP</td>
<td>Telnet Diagnostics</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Enable Telnet Access</td>
</tr>
<tr>
<td>Inbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>----------</td>
<td>-------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>24</td>
<td>Static</td>
<td>TCP</td>
<td>Polycom API</td>
<td>No</td>
<td>No</td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Enable Telnet Access</td>
</tr>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>Web UI over HTTP</td>
<td>Yes</td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Enable Web Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RealPresence Touch over HTTP</td>
<td></td>
<td></td>
<td>- Disables HTTP and HTTPS port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Restrict to HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Disables HTTP port</td>
</tr>
<tr>
<td>Inbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>----------</td>
<td>---------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>Static</td>
<td>UDP</td>
<td>SNMP</td>
<td>No</td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Enable SNMP Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Settings &gt; Servers &gt; SNMP &gt; Listening Port</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>Web UI over HTTPS</td>
<td>Yes</td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Access &gt; Enable Web Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RealPresence Touch over HTTPS</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1719</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 RAS</td>
<td>No</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Use Gatekeeper</td>
<td></td>
</tr>
<tr>
<td>1720</td>
<td>Static</td>
<td>TCP</td>
<td>H.225.0 Call Signaling</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Enable IP H.323</td>
<td></td>
</tr>
<tr>
<td>Inbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>5001</td>
<td>Static</td>
<td>TCP</td>
<td>People +Content™ IP client application for content sharing. Used by systems and the RealPresence Touch device</td>
<td>Yes</td>
<td>Admin Settings &gt; Audio / Video &gt; Video Input &gt; General Camera Settings &gt; Enable People +Content IP</td>
<td>No</td>
</tr>
<tr>
<td>5060</td>
<td>Static</td>
<td>TCP</td>
<td>SIP (Protocol depends on Transport Protocol setting)</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; SIP &gt; Enable SIP</td>
<td>No</td>
</tr>
<tr>
<td>5061</td>
<td>Static</td>
<td>TLS</td>
<td>SIP</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; SIP &gt; Enable SIP</td>
<td>No</td>
</tr>
</tbody>
</table>

Polycom, Inc.
<table>
<thead>
<tr>
<th>Inbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Configuration</th>
<th>On By Default?</th>
<th>(Low Security Profile)</th>
<th>Enable/Disable?</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152-65535</td>
<td>Dynamic</td>
<td>TCP</td>
<td>H.245</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Enable IP H.323</td>
<td></td>
<td></td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; Firewall &gt; Fixed Ports &gt; TCP Ports (1024-65535)</td>
</tr>
<tr>
<td>16384-32764 (Default)</td>
<td>Dynamic</td>
<td>UDP</td>
<td>RTP/RTCP Video and Audio</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Enable IP H.323</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; SIP &gt; Enable SIP</td>
<td></td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; Firewall &gt; Fixed Ports &gt; UDP Ports (1024-65535)</td>
</tr>
</tbody>
</table>

**Outbound Ports for RealPresence Group Series**

IP port usage information for your system is important when you are setting up new videoconferencing equipment and must know the type, protocol, or function of the port, and if it is configurable.

The following table shows IP port usage for outbound traffic from RealPresence Centro systems.
<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>On By Default?</th>
<th>Enable/Disable?</th>
<th>Configurable Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Static</td>
<td>TCP</td>
<td>Polycom Product Registration for RealPresence Centro system software installation and for the RealPresence Touch device</td>
<td>Yes</td>
<td>Uncheck &quot;Register&quot; checkbox during the setup wizard</td>
<td>No</td>
</tr>
<tr>
<td>123</td>
<td>Static</td>
<td>UDP</td>
<td>NTP</td>
<td>Yes</td>
<td>Admin Settings &gt; General Settings &gt; Date and Time &gt; System Time &gt; Time Server</td>
<td>No</td>
</tr>
<tr>
<td>162</td>
<td>Static</td>
<td>UDP</td>
<td>SNMP TRAP</td>
<td>No</td>
<td>Admin Settings &gt; Servers &gt; SNMP &gt; Enable SNMP &gt; Destination Address &lt;1,2,3&gt; &gt; Port</td>
<td>Yes - Admin Settings &gt; Servers &gt; SNMP &gt; Destination Address &lt;1,2,3&gt; &gt; Port</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Enable/Disable?</td>
<td>Configurabl e Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>389</td>
<td>Static</td>
<td>TLS</td>
<td>LDAP</td>
<td>No</td>
<td>Admin Settings &gt; Servers &gt; Directory Servers &gt; Server Type</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Admin Settings &gt; Servers &gt; Directory Servers &gt; Server Type = LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LDAP to ADS (External Authentication)</td>
<td>No</td>
<td>Admin Settings &gt; Security &gt; Global Security &gt; Authentication &gt; Enable Active Directory External Authentication</td>
<td>No</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>RealPresence Resource Management (Provisioning, Monitoring, Softupdate)</td>
<td>No</td>
<td>Admin Settings &gt; Servers &gt; Provisioning Service &gt; Enable Provisioning</td>
<td>No</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>Microsoft Exchange Server (Calendaring)</td>
<td>No</td>
<td>Admin Settings &gt; Servers &gt; Calendaring Service &gt; Enable Calendaring Service</td>
<td>No</td>
</tr>
<tr>
<td>443</td>
<td>Static</td>
<td>TLS</td>
<td>Microsoft Skype Address Book</td>
<td>No</td>
<td>Admin Settings &gt; Servers &gt; Directory Servers &gt; Server Type</td>
<td>No</td>
</tr>
<tr>
<td>514</td>
<td>Static</td>
<td>UDP</td>
<td>SYSLOG</td>
<td>No</td>
<td>Diagnostics &gt; System &gt; System Log Settings &gt; Enable Remote Logging</td>
<td>Yes - outgoing port can be specified in the <em>Remote Log Server Address</em> field.</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default? (Low Security Profile)</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>----------</td>
<td>-------------------</td>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>601</td>
<td>Static</td>
<td>TCP</td>
<td>SYSLOG</td>
<td>No</td>
<td>Diagnostics &gt; System &gt; System Log Settings &gt; Enable Remote Logging</td>
<td>Yes - outgoing port can be specified in the Remote Log Server Address field.</td>
</tr>
<tr>
<td>1718</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 Gatekeeper Discovery</td>
<td>No</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Use Gatekeeper = Auto</td>
<td></td>
</tr>
<tr>
<td>1719</td>
<td>Static</td>
<td>UDP</td>
<td>H.225.0 RAS</td>
<td>No</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Use Gatekeeper</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes - outgoing port can be specified in the <strong>Primary Gatekeeper IP Address</strong> field.</td>
<td></td>
</tr>
<tr>
<td>1720</td>
<td>Static</td>
<td>TCP</td>
<td>H.225.0 Call Signaling</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; H.323 &gt; Enable IP H.323</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default? (Low Security Profile)</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>----------</td>
<td>----------</td>
<td>---------------------------------------</td>
<td>----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>3601</td>
<td>Static</td>
<td>TCP</td>
<td>GDS</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5060</td>
<td>Static</td>
<td>UDP TCP</td>
<td>SIP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes - outgoing port can be specified in the dial string (user@domain:port) Note that the transport protocol used depends on Admin Settings &gt; Network &gt; IP Network &gt; SIP &gt; Transport Protocol = Auto, TCP, or UDP</td>
</tr>
<tr>
<td>5061</td>
<td>Static</td>
<td>TLS</td>
<td>SIP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes - outgoing port can be specified in the dial string (user@domain:port) Note that the transport protocol used depends on Admin Settings &gt; Network &gt; IP Network &gt; SIP &gt; Transport Protocol = Auto or TLS</td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>(Low Security Profile)</td>
<td>Enable/Disable?</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>----------</td>
<td>---------------------------------</td>
<td>----------------</td>
<td>------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>5222</td>
<td>Static</td>
<td>TCP</td>
<td>RealPresence Resource Manager: XMPP</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6514</td>
<td>Static</td>
<td>TLS</td>
<td>SYSLOG</td>
<td>No</td>
<td>Diagnostics &gt; System &gt; System Log Settings &gt; Enable Remote Logging</td>
<td>Yes - outgoing port can be specified in the Remote Log Server Address field</td>
</tr>
<tr>
<td>49152-65535</td>
<td>Dynamic</td>
<td>TCP</td>
<td>H.245</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; Enable IP H. 323</td>
<td></td>
</tr>
<tr>
<td>Outbound Port</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>On By Default?</td>
<td>Enable/Disable?</td>
<td>Configurable Port Number</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>----------</td>
<td>------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>16384-32764</td>
<td>Dynamic</td>
<td>UDP</td>
<td>RTP/RTCP Video and Audio</td>
<td>Yes</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; Enable IP H. 323 Admin Settings &gt; Network &gt; IP Network &gt; Enable SIP</td>
<td>Admin Settings &gt; Network &gt; IP Network &gt; Firewall &gt; Fixed Ports &gt; UDP Ports (1024-65535)</td>
</tr>
</tbody>
</table>
Security Profile Default Settings

Topics:
- **Maximum Security Profile Default Settings**
- **High Security Profile Default Settings**
- **Medium Security Profile Default Settings**
- **Low Security Profile Default Settings**

The RealPresence Centro system has Maximum, High, Medium, and Low security profiles.

### Maximum Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **Maximum** security profile.

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Maximum</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>Place a Call</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>Search Box</td>
<td>No value</td>
</tr>
<tr>
<td>Speed Dial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Search Box</td>
<td>No value</td>
</tr>
<tr>
<td>Manual Dial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry box</td>
<td>No value</td>
<td>Yes</td>
</tr>
<tr>
<td>VideoAudio</td>
<td>Video</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144</td>
<td>Auto</td>
</tr>
<tr>
<td></td>
<td>Auto, H.323, SIP</td>
<td>Auto</td>
</tr>
</tbody>
</table>

Polycom, Inc.
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Auto Answer Point to Point Video</td>
<td>Yes, No, Do Not Disturb</td>
</tr>
<tr>
<td>Auto Answer Multipoint Video</td>
<td>Yes, No, Do Not Disturb</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Call Detail Report Checkbox</td>
</tr>
<tr>
<td>Enable Recent Calls Checkbox</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Home Screen Settings</td>
<td>Speed Dial Checkbox</td>
</tr>
<tr>
<td></td>
<td>Calendar Checkbox</td>
</tr>
<tr>
<td></td>
<td>Background Choose image file</td>
</tr>
<tr>
<td></td>
<td>Startup Background Choose image file</td>
</tr>
<tr>
<td></td>
<td>Kiosk Mode Checkbox</td>
</tr>
<tr>
<td></td>
<td>Home Screen Icons Checkbox</td>
</tr>
<tr>
<td></td>
<td>Address Bar None IP Address</td>
</tr>
<tr>
<td></td>
<td>SIP Address None</td>
</tr>
<tr>
<td></td>
<td>H.323 Extension</td>
</tr>
<tr>
<td></td>
<td>Pairing Code None</td>
</tr>
<tr>
<td></td>
<td>RealPresence Touch Background Choose image file</td>
</tr>
<tr>
<td></td>
<td>Skype Mode Checkbox</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Enable Polycom Touch Device</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Note: Disabling this setting closes the SSH port.</td>
<td></td>
</tr>
<tr>
<td>SmartPairing</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

### Serial Ports

#### Mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Range: None, Admin password only, Username/Password</th>
<th>Admin password only</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-232 Modem</td>
<td>Note: Some systems support only a subset of listed modes.</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Control</td>
<td>Camera Control</td>
<td>Closed Caption</td>
<td>Pass Thru</td>
</tr>
</tbody>
</table>

#### Login Mode

<table>
<thead>
<tr>
<th>Login prompt type</th>
<th>None, Admin password only, Username/Password</th>
<th>Username/Password</th>
<th>Yes</th>
</tr>
</thead>
</table>

### Network

#### IP Network

<table>
<thead>
<tr>
<th>Enable SIP</th>
<th>Checkbox</th>
<th>Enabled</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Protocol</td>
<td>Auto, TLS, TCP, UDP</td>
<td>TLS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Dialing Preference

**Dialing Options**

<table>
<thead>
<tr>
<th>Scalable Video Coding Preference (H.264)</th>
<th>SVC then AVC</th>
<th>SVC then AVC</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable H.239</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>Enable Audio-Only Calls</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>TIP</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Type Order</td>
<td>Video</td>
<td>Video</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Video Then Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Then Video</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Dialing Order</td>
<td>IP, H.323, SIP</td>
<td>IP H.323</td>
<td>Yes</td>
</tr>
<tr>
<td>Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP, H.323, SIP</td>
<td>SIP</td>
<td>Yes</td>
</tr>
<tr>
<td>Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP, H.323, SIP</td>
<td>H.323</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Audio/Video

### Sleep

<table>
<thead>
<tr>
<th>Enable Mic Mute in Sleep Mode</th>
<th>Checkbox</th>
<th>Enabled</th>
<th>Read-only</th>
</tr>
</thead>
</table>

### Video Inputs

### General Camera Settings
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Maximum</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>Allow Other</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Participants In a Call to Control Your Camera</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable People</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>+Content IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Camera</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Preset Snapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Icons</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom StereoSurround</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Global Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Profile</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Profile</td>
<td>Maximum</td>
<td>Maximum</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Active</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Directory External Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Enable Network Intrusion Detection System (NIDS)</strong></td>
<td>Checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Enable Web Access</strong></td>
<td>Checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Allow Access to User Settings</strong></td>
<td>Checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Restrict to HTTPS</strong></td>
<td>Checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read-only</td>
<td></td>
</tr>
</tbody>
</table>
| **Web access port (http)**  
*Note:* You cannot select this setting if the **Restrict to HTTPS** setting is enabled. | 16-bit integer                                                         |
<p>|                                                                                   | Grayed out (80)                                                         |
|                                                                                   | Read-only                                                               |
| <strong>Enable Telnet Access</strong>                                                           | Checkbox                                                                 |
|                                                                                   | Disabled                                                                |
|                                                                                   | Read-only                                                               |
| <strong>Enable SNMP Access</strong>                                                             | Checkbox                                                                 |
|                                                                                   | Disabled                                                                |
|                                                                                   | Yes                                                                     |
| <strong>API Port</strong>                                                                      |                                                                         |</p>
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>Off, 2-10</td>
</tr>
<tr>
<td>Port Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours</td>
</tr>
<tr>
<td>Reset Port Lock Counter After</td>
<td>Off, [1..24] hours</td>
</tr>
<tr>
<td>Enable Whitelist</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480</td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>10, 15, 20, 25, 30, 35, 40, 45, 50</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Require AES Encryption for Calls</td>
<td>Off</td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Disable TLS v1.0</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Local Accounts</td>
<td></td>
</tr>
<tr>
<td>Account Lockout</td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Lock Admin Account</td>
<td>2-10</td>
</tr>
<tr>
<td>After Failed Logins</td>
<td></td>
</tr>
<tr>
<td>Admin Account</td>
<td>1, 2, 3, 5 minutes</td>
</tr>
<tr>
<td>Lock Duration</td>
<td></td>
</tr>
<tr>
<td>Reset Admin Account</td>
<td>Off, [1..24] hours</td>
</tr>
<tr>
<td>Lock Duration</td>
<td></td>
</tr>
<tr>
<td>Lock User Account</td>
<td>2-10</td>
</tr>
<tr>
<td>After Failed Logins</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours</td>
</tr>
<tr>
<td>Lock Duration</td>
<td></td>
</tr>
<tr>
<td>Reset User Account</td>
<td>Off, [1..24] hours</td>
</tr>
<tr>
<td>Lock Duration</td>
<td></td>
</tr>
</tbody>
</table>

### Login Credentials

<table>
<thead>
<tr>
<th>Use Room Password for Remote Access</th>
<th>Checkbox</th>
<th>Enabled</th>
<th>Read-only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require User Login for System Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Password Requirements
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Maximum Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin (Room, Remote), User (Room, Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>8-16</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180</td>
<td>60</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>1-4</td>
<td>4</td>
<td>Yes</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>1-7</td>
<td>7</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Access (Admin Remote, User Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>1-4</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>User (Room), Admin (Room)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>9</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>1-4</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Meeting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-20, 32</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Reject Previous Passwordes</td>
<td>8-16</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>1-4</td>
<td>2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**SNMP**

Note: SNMP passwords are applicable only when the system uses SNMP v3.

<table>
<thead>
<tr>
<th>Maximum Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>12</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>1</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>8-16</td>
<td>10</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>1-4</td>
<td>2</td>
</tr>
<tr>
<td>Can contain ID or its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

## Security Banner

| Security Banner | | | |
|------------------|-------------------|------------|
| Enable Security Banner | Checkbox | Enabled | Yes |
| Banner Text | DoDCustom | DoD | Yes |
| Local System Banner Text | Unicode characters, 2048 bytes max | DoD Banner Text | Yes |
| Remote System Banner Text | Unicode characters, 2048 bytes max | DoD Banner Text | Yes |

## Certificates

<table>
<thead>
<tr>
<th>Certificate Options</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Validate Peer Certificates from Browser</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Maximum</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Server</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Revocation</td>
<td>Revocation Method</td>
<td>OCSPCRL</td>
</tr>
<tr>
<td></td>
<td>Allow Incomplete Revocation Checks</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Servers</td>
<td>Directory Servers</td>
<td>Server Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft LDAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Polycom GDS</td>
</tr>
<tr>
<td></td>
<td>Registration Status</td>
<td>N/A</td>
</tr>
<tr>
<td>SNMP</td>
<td>Version1</td>
<td>Checkbox</td>
</tr>
<tr>
<td></td>
<td>Version2c</td>
<td>Checkbox</td>
</tr>
<tr>
<td></td>
<td>Version3</td>
<td>Checkbox</td>
</tr>
<tr>
<td></td>
<td>Provisioning Service</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Calendaring Service</td>
<td>Enable Calendaring Service</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Recording Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Changing Maximum Security Profile Default Values

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

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

Other Restrictions When Using the Maximum Security Profile

The following settings are not available in the “User Settings” menu (they are configurable only in their respective sections of the **Admin Settings**):

- Camera > Allow Other Participants in a Call to Control Your Camera
- Meetings > Mute Auto Answer Calls
High Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **High** security profile.

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Place a Call</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>Search Box</td>
</tr>
<tr>
<td>Speed Dial</td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Search Box</td>
</tr>
<tr>
<td>Manual Dial</td>
<td></td>
</tr>
<tr>
<td>Entry box</td>
<td>No value</td>
</tr>
<tr>
<td>Video Audio</td>
<td>Video</td>
</tr>
<tr>
<td>Video</td>
<td>Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144</td>
</tr>
<tr>
<td>Audio</td>
<td>Auto</td>
</tr>
<tr>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>H.323</td>
<td>Auto</td>
</tr>
<tr>
<td>SIP</td>
<td>Auto</td>
</tr>
</tbody>
</table>

**General Settings**

**System Settings**

**Call Settings**

<table>
<thead>
<tr>
<th>Auto Answer Point to Point Video</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Disturb</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------</td>
<td>---</td>
</tr>
<tr>
<td>Auto Answer Multipoint</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Video</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recent Calls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable Recent Calls</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Home Screen Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Calendar</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Background</td>
<td>Choose image file</td>
<td>No file selected</td>
</tr>
<tr>
<td>Startup Background</td>
<td>Choose image file</td>
<td>No file selected</td>
</tr>
<tr>
<td>Kiosk Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Home Screen Icons</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Address Bar</td>
<td>None</td>
<td>IP Address</td>
</tr>
<tr>
<td>RealPresence Touch</td>
<td>Choose image file</td>
<td>No file selected</td>
</tr>
<tr>
<td>Background</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Pairing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Polycom Touch Device</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Note: Disabling this setting closes the SSH port.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Security Profile Default Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>SmartPairing Mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Automatic</td>
</tr>
<tr>
<td></td>
<td>Manual</td>
</tr>
</tbody>
</table>

## Serial Ports

### Mode

<table>
<thead>
<tr>
<th>RS-232 Mode Note: Some systems support only a subset of listed modes.</th>
<th>Off Control</th>
<th>Camera Control</th>
<th>Closed Caption</th>
<th>Pass Thru</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Mode</strong></td>
<td>None, Admin password only, Username/Password</td>
<td>Admin password only</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

## Network

### IP Network

<table>
<thead>
<tr>
<th>Enable SIP</th>
<th>Checkbox</th>
<th>Enabled</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Protocol</td>
<td>Auto TLS TCP UDP</td>
<td>TLS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Dialing Preference

<table>
<thead>
<tr>
<th>Scalable Video Coding Preference (H.264)</th>
<th>SVC then AVC</th>
<th>AVC Only</th>
<th>Yes</th>
</tr>
</thead>
</table>

### Dialing Options

<table>
<thead>
<tr>
<th>Scalable Video Coding Preference (H.264)</th>
<th>SVC then AVC</th>
<th>SVC then AVC</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable H.239</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Audio-Only Calls</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>TIP</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Type Order</td>
<td>Video</td>
<td>Video</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Video Then Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Then Video</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOICEDIALPREFERENCES_SIP_SPEAKERPHONE</td>
<td>(only displays if Polycom SoundStation IP 7000 is connected)</td>
<td></td>
</tr>
<tr>
<td>Video Dialing Order</td>
<td>IP</td>
<td>IP H.323</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP</td>
<td>SIP</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP</td>
<td>H.323</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio/Video</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sleep</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Mic Mute in Sleep Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Inputs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Camera Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Other Participants in a Call to Control Your Camera</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable People +Content IP</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>Enable Camera Preset Snapshot Icons</td>
<td>Checkbox</td>
<td>High</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom StereoSurround</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Global Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Profile</td>
<td>Maximum</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Network Intrusion Detection System (NIDS)</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Access to User Settings</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrict to HTTPS</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>Web access port (http)</td>
<td></td>
<td>16-bit integer</td>
<td></td>
</tr>
<tr>
<td>Note: You cannot select this setting if the Restrict to HTTPS setting is enabled.</td>
<td></td>
<td>Grayed out (80)</td>
<td></td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Enable SSH Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>Off, 2-10</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Port Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours</td>
<td>1 minute</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset Port Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Whitelist</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>10, 15, 20, 25, 30, 35, 40, 45, 50</td>
<td>25</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Encryption

<table>
<thead>
<tr>
<th>Require AES Encryption for Calls</th>
<th>Off When Available</th>
<th>Required for Video Calls Only</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Disable TLS v1.0</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Local Accounts

#### Account Lockout

<table>
<thead>
<tr>
<th></th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Admin Account After Failed Logins</td>
<td>Off 2-10</td>
<td>3</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Account Lock Duration</td>
<td>1, 2, 3, 5 minutes</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset Admin Account Lock Counter After Failed Logins</td>
<td>Off [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock User Account After Failed Logins</td>
<td>2-10</td>
<td>3</td>
<td>Yes</td>
</tr>
<tr>
<td>User Account Lock Duration</td>
<td>1, 3, 5, 10, 15, 20, 30 minutes 1, 2, 4, 8 hours</td>
<td>1 minute</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset User Account Lock Counter After Failed Logins</td>
<td>Off [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Login Credentials

<table>
<thead>
<tr>
<th></th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Room Password for Remote Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Require User Login for System Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Password Requirements

Admin (Room, Remote), User (Room, Remote)
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>1-4</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>1-7</td>
</tr>
</tbody>
</table>

**Remote Access (Admin Remote, User Remote)**

<table>
<thead>
<tr>
<th></th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>1-16, 32</td>
<td>6</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

**User (Room), Admin (Room)**

<table>
<thead>
<tr>
<th></th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>6</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
<td>Configurable?</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td></td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Meeting</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-20, 32</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Admin Settings Area

| Admin Settings Area | High | | | |
|---------------------|------|------|------|
|                     | Range | Default Value | Configurable? |
| Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |

### SNMP

**Note:** SNMP passwords are applicable only when the system uses SNMP v3.

<table>
<thead>
<tr>
<th>SNMP</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>8</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

### Certificates

<table>
<thead>
<tr>
<th>Certificate Options</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Validate Peer Certificates from Browser</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
</tr>
<tr>
<td></td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Server</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Revocation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revocation Method</td>
<td>OCSPCRL</td>
<td>OCSP</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Banner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Security Banner</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Banner Text</td>
<td>DoDCustom</td>
<td>Custom</td>
<td>Yes</td>
</tr>
<tr>
<td>Local System Banner Text</td>
<td>Unicode characters, 2048 bytes max</td>
<td>Null (no text)</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote System Banner Text</td>
<td>Unicode characters, 2048 bytes max</td>
<td>Null (no text)</td>
<td>Yes</td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Type</td>
<td>Off</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Microsoft</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Polycom GDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Status</td>
<td>N/A</td>
<td>Disabled</td>
<td>Read only</td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version1</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Version2c</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Version3</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Provisioning Service</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Admin Settings Area

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Calendaring Service</td>
<td></td>
</tr>
<tr>
<td>Enable Calendaring Service</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Recording Service</td>
<td></td>
</tr>
<tr>
<td>Enable Recording Service</td>
<td>Checkbox</td>
</tr>
<tr>
<td></td>
<td>Domain Name</td>
</tr>
</tbody>
</table>

### Diagnostics Area

<table>
<thead>
<tr>
<th>Diagnostics Area</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>System</td>
<td></td>
</tr>
<tr>
<td>System Log Settings</td>
<td></td>
</tr>
<tr>
<td>Enable Remote Logging</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Remote Log Server Transport Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

### Changing High Security Profile Default Values

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

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

Configure Security Profiles
Medium Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the Medium security profile.

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
</table>

### Place a Call

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Search Box</th>
<th>No value</th>
<th>Yes</th>
</tr>
</thead>
</table>

### Speed Dial

<table>
<thead>
<tr>
<th>Edit</th>
<th>Search Box</th>
<th>No value</th>
<th>Yes</th>
</tr>
</thead>
</table>

### Manual Dial

<table>
<thead>
<tr>
<th>VideoAudio</th>
<th>Video</th>
<th>Yes</th>
</tr>
</thead>
</table>

| Auto, 128, 256, 384, 512, 768, 1024, 1472, 1920, 2048, 3072, 3840, 4096, 6144 | Auto | Yes |

<table>
<thead>
<tr>
<th>Auto</th>
<th>Auto</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>H.323</th>
<th>Auto</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>SIP</th>
<th>Auto</th>
<th>Yes</th>
</tr>
</thead>
</table>

### General Settings

### System Settings

#### Call Settings

<table>
<thead>
<tr>
<th>Auto Answer Point to Point Video</th>
<th>Yes</th>
<th>No</th>
<th>Do Not Disturb</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Answer Multipoint Video</td>
<td>Yes</td>
<td>No</td>
<td>Do Not Disturb</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td><strong>Recent Calls</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Recent Calls</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Home Screen Settings</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calendar</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background</td>
<td>Choose image file</td>
<td>No file</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Startup Background</td>
<td>Choose image file</td>
<td>No file</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kiosk Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home Screen Icons</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address Bar</td>
<td>None</td>
<td>None</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Extension</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pairing Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RealPresence Touch</td>
<td>Choose image file</td>
<td>No file</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pairing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Polycom Touch</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: Disabling this setting closes the SSH port.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartPairing Mode</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Serial Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS-232 Mode</td>
<td></td>
<td>Off</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Camera Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Closed Caption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pass Thru</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Mode</td>
<td></td>
<td>Range: None, Admin password only, Username/Password</td>
<td>Admin password only</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SIP</td>
<td></td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Transport Protocol</td>
<td></td>
<td>Auto, TLS, TCP, UDP</td>
<td>TLS</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dialing Preference</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalable Video Coding Preference (H.264)</td>
<td></td>
<td>SVC then AVC</td>
<td>SVC then AVC</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AVC Only</td>
<td>AVC Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialing Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalable Video Coding Preference (H.264)</td>
<td></td>
<td>SVC then AVC</td>
<td>SVC then AVC</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AVC Only</td>
<td>AVC Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable H.239</td>
<td></td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable Audio-Only Calls</td>
<td></td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>TIP</td>
<td></td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>-------</td>
<td>---------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Call Type Order</td>
<td>Video</td>
<td>Video</td>
<td>Video</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video Then Phone</td>
<td>Video Then Phone</td>
<td>Video</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Then Video</td>
<td>Phone Then Video</td>
<td>Video</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)</td>
<td>VOICEDIALPREFERENCE_SIP_SPEAKERPHONE (only displays if Polycom SoundStation IP 7000 is connected)</td>
<td>Video</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Video Dialing Order</td>
<td>IP</td>
<td>IP</td>
<td>IP H.323</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td>H.323</td>
<td>H.323</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td>SIP</td>
<td>SIP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Audio Dialing Order Preference 1 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP</td>
<td>IP</td>
<td>SIP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td>H.323</td>
<td>H.323</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td>SIP</td>
<td>SIP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Audio Dialing Order Preference 2 (only displays if Enable Audio-Only Calls checkbox is selected)</td>
<td>IP</td>
<td>IP</td>
<td>H.323</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>H.323</td>
<td>H.323</td>
<td>H.323</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td>SIP</td>
<td>SIP</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### 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
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Enable Camera Preset Snapshot Icons</td>
<td>Checkbox</td>
</tr>
</tbody>
</table>

**Audio**

| Polycom StereoSurround | Checkbox | Disabled | Yes |

**Security**

**Global Security**

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Profile</td>
<td>Maximum</td>
<td>Medium</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Authentication**

| Enable Active Directory External Authentication | Checkbox | Disabled | Yes |

**Access**

<table>
<thead>
<tr>
<th>Enable Network Intrusion Detection System (NIDS)</th>
<th>Checkbox</th>
<th>Enabled</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Web Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Access to User Settings</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Restrict to HTTPS</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Web access port (http)</td>
<td>16-bit integer</td>
<td>Grayed out (80)</td>
<td>Read only</td>
</tr>
</tbody>
</table>

**Note:** You cannot select this setting if the **Restrict to HTTPS** setting is enabled.
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Telnet Access</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable SSH Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>Off, 2-10</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Port Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes, 1, 2, 4, 8 hours</td>
<td>1 minute</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reset Port Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable Whitelist</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480</td>
<td>10, 15, 20, 25, 30, 35, 40, 45, 50</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>10, 15, 20, 25, 30, 35, 40, 45, 50</td>
<td>25</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require AES Encryption for Calls</td>
<td>Off</td>
<td>When Available</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Disable TLS v1.0</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Local Accounts</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Lockout</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock Admin Account After Failed Logins</td>
<td>Off, 2-10</td>
<td>3</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong></td>
<td><strong>Default Value</strong></td>
<td><strong>Configurable?</strong></td>
<td></td>
</tr>
<tr>
<td>Admin Account Lock Duration</td>
<td>1, 2, 3, 5 minutes</td>
<td>1</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reset Admin Account Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Lock User Account After Failed Logins</td>
<td>Off, 2-10</td>
<td>3</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User Account Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes 1, 2, 4, 8 hours</td>
<td>1 minute</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reset User Account Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Login Credentials**

<table>
<thead>
<tr>
<th></th>
<th><strong>Checkbox</strong></th>
<th><strong>Disabled</strong></th>
<th><strong>Yes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Room Password for Remote Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require User Login for System Access</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Password Requirements**

**Admin (Room, Remote), User (Room, Remote)**

<table>
<thead>
<tr>
<th></th>
<th><strong>Checkbox</strong></th>
<th><strong>Disabled</strong></th>
<th><strong>Yes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>Off, 1-4, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Off, 1-7</td>
<td>Off</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Remote Access (Admin Remote, User Remote)**
<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td></td>
<td>1-16, 32</td>
<td>3</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td></td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td></td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Numbers</td>
<td></td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td></td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td></td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

| User (Room), Admin (Room)                              |                                             | 8-16, 32       | 8             | Yes           |
| Minimum Length                                         |                                             | Off, 1, 2, All | 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                                   | Disabled        | Yes           |

<table>
<thead>
<tr>
<th>Meeting</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-20, 32</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Maximum Consecutive Repeated</td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Characters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> SNMP passwords are</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>applicable only when the system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uses SNMP v3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>8-16, 32</td>
<td>3</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, All</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
<td>Configurable?</td>
<td></td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1-4</td>
<td>Off</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Certificates**

<table>
<thead>
<tr>
<th></th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td></td>
<td>Checkbox</td>
</tr>
</tbody>
</table>

**Revocation**

<table>
<thead>
<tr>
<th></th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td></td>
<td>OCSPCRL</td>
</tr>
<tr>
<td></td>
<td>Checkbox</td>
</tr>
</tbody>
</table>

**Security Banner**

<table>
<thead>
<tr>
<th></th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td></td>
<td>DoDCustom</td>
</tr>
<tr>
<td></td>
<td>Unicode characters, 2048 bytes max</td>
</tr>
</tbody>
</table>

**Servers**

<table>
<thead>
<tr>
<th></th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td></td>
<td>Null (no text)</td>
</tr>
<tr>
<td>Admin Settings Area</td>
<td>Medium</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Server Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Status</td>
<td></td>
</tr>
</tbody>
</table>

**SNMP**

<table>
<thead>
<tr>
<th>SNMP</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version1</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Version2c</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Version3</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Calendaring Service**

<table>
<thead>
<tr>
<th>Calendaring Service</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Calendaring Service</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Recording Service**

<table>
<thead>
<tr>
<th>Recording Service</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Recording Service</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Recording Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diagnostics Area**

<table>
<thead>
<tr>
<th>Diagnostics Area</th>
<th>Medium</th>
<th>Range</th>
<th>Default Value</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Log Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Remote Logging</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Security Profile Default Settings

<table>
<thead>
<tr>
<th>Diagnostics Area</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Remote Log Server</td>
<td>UDP</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>TLS</td>
</tr>
</tbody>
</table>

#### Changing Medium Security Profile Default Values

When you configure the system to use the Medium Security Profile, it forces you to change the following settings from their default values:

- Admin account room password
- User account room password

#### Low Security Profile Default Settings

System security profiles provide varying levels of secure access to your RealPresence Centro system. The following table shows the default values for specific settings when you use the **Low** security profile.

<table>
<thead>
<tr>
<th>Admin Setting</th>
<th>Low Range</th>
<th>Default</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place a Call</td>
<td>Search box</td>
<td>No value</td>
<td>Yes</td>
</tr>
<tr>
<td>Contacts</td>
<td>Search box</td>
<td>No value</td>
<td>Yes</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Search box</td>
<td>No value</td>
<td>Yes</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Entry box</td>
<td>No value</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual Dial</td>
<td>Video</td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audio</td>
<td>Auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td>H.323</td>
<td>Auto</td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
<td>Configurable?</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>Admin Settings &gt; General Settings &gt; My Information</td>
<td>Contact Information</td>
<td>Entry boxes</td>
<td>No value</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Settings &gt; General Settings &gt; System Settings</td>
<td>System Name</td>
<td>Entry box</td>
<td>No value</td>
</tr>
<tr>
<td>Call Settings</td>
<td>Maximum Time in Call</td>
<td>Off, 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hours, 7 hours, 8 hours, 9 hours, 10 hours, 11 hours, 12 hours, 24 hours, 48 hours</td>
<td>8 hours</td>
</tr>
<tr>
<td></td>
<td>Auto Answer Point to Point Video</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Auto Answer Multipoint Video</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Mulitpoint Mode</td>
<td>Auto, Full Screen, Discussion, Presentation</td>
<td>Discussion</td>
</tr>
<tr>
<td></td>
<td>Display Icons in a Call</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Enable Flashing Incoming Call Notification</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Preferred 'Place a Call' Navigation</td>
<td>Keypad</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Automatic Self View Control</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Admin Setting</strong></td>
<td><strong>Low</strong></td>
<td><strong>Range</strong></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Recent Calls</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Checkbox</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Enable Recent Calls</td>
<td>Checkbox</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Maximum Number to Display</td>
<td>25, 50, 75, 100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Admin Settings &gt; General Settings &gt; Home Screen Settings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Calendar</td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Background</td>
<td>Choose Image File</td>
<td>No file selected</td>
<td></td>
</tr>
<tr>
<td>Startup Background</td>
<td>Choose Image File</td>
<td>No file selected</td>
<td></td>
</tr>
<tr>
<td>Kiosk Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Home Screen Icons</td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Address Bar</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Address</td>
<td>None</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>H.323 Extension</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pairing Code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RealPresence Touch Background</strong></td>
<td>Choose image file</td>
<td>Image file not selected</td>
<td></td>
</tr>
<tr>
<td><strong>Skype Mode</strong></td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Pairing &gt; Enable Polycom Touch Device</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: Disabling this setting closes the SSH port.</td>
<td>Checkbox</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>SmartPairing Mode</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
<td>Configurable?</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Serial Ports &gt; Mode</strong></td>
<td>RS-232 Mode</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Note: Some RealPresence Centro systems support only a subset of listed modes.</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Camera Control</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Closed Caption</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pass Thru</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Login Mode</strong></td>
<td>None</td>
<td>Admin Password Only</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>Password only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Username/Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network &gt; IP Network</strong></td>
<td>Enable SIP</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transport Protocol</td>
<td>TLS</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Dialing Preference</strong></td>
<td>SVC then AVC</td>
<td>SVC then AVC</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Dialing Options</strong></td>
<td>SVC then AVC</td>
<td>SVC then AVC</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SVC then AVC</td>
<td>SVC then AVC</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enable H.239</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Enable Audio-Only Calls</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>TIP</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Call Type Order</td>
<td>Video</td>
<td>Video</td>
</tr>
</tbody>
</table>

Polycom, Inc.
<table>
<thead>
<tr>
<th>Admin Setting</th>
<th>Low</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Default</td>
</tr>
<tr>
<td>Video Dialing Order</td>
<td>IP H.323</td>
<td>IP H.323</td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>Auto Dialing Order Preference 1</td>
<td>SIP</td>
<td>SIP</td>
</tr>
<tr>
<td>(only displays if <strong>Enable Audio-Only Calls</strong> checkbox is selected)</td>
<td>H.323</td>
<td></td>
</tr>
<tr>
<td>Auto Dialing Order Preference 2</td>
<td>H.323</td>
<td>H.323</td>
</tr>
<tr>
<td>(only displays if <strong>Enable Audio-Only Calls</strong> checkbox is selected)</td>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td><strong>Audio/Video &gt; Video Inputs &gt; Sleep</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display</td>
<td>No Signal</td>
<td>No Signal</td>
</tr>
<tr>
<td></td>
<td>Black</td>
<td></td>
</tr>
<tr>
<td>Time Before System Goes to Sleep</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 minute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>30 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>60 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 hours</td>
<td></td>
</tr>
<tr>
<td>Enable Mic Mute in Sleep Mode</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>General Camera Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Other Participants in a Call to Control Your Camera</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Enable People+Content IP</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable Camera Preset Snapshot Icons</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom StereoSurround</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Security &gt; Global Security &gt; Security Profile</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Security Profile</strong></td>
<td>Maximum</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Active Directory External</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Network Intrusion Detection System (NIDS)</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Access to User Settings</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Restrict to HTTPS</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Web access port (http) Note:You cannot select this setting if the <strong>Restrict to HTTPS</strong> setting is enabled.</td>
<td>16-bit integer</td>
<td>Grayed out (80)</td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Enable SSH Access</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>Off, 2-10</td>
<td>Off</td>
</tr>
<tr>
<td>Port Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes</td>
<td>1 minute</td>
</tr>
<tr>
<td></td>
<td>1, 2, 4, 8 hours</td>
<td></td>
</tr>
<tr>
<td>Reset Port Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
</tr>
<tr>
<td>Enable Whitelist</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>1, 3, 5, 10, 15, 20, 30, 45, 60, 120, 240, 480</td>
<td>10,15,20,25,30,35,40,45,50</td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>10, 15, 20, 25, 30, 35, 40, 45, 50</td>
<td>25</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Require AES Encryption for Calls</td>
<td>Off</td>
<td>When Available</td>
</tr>
<tr>
<td></td>
<td>Required for Video Calls Only</td>
<td>When Available</td>
</tr>
<tr>
<td></td>
<td>Required for All Video Calls</td>
<td></td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Disable TLS v1.0</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Local Accounts &gt; Account Lockout</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock Admin Account After Failed Logins</td>
<td>Off, 2-10</td>
<td>3</td>
</tr>
<tr>
<td>Admin Account Lock Duration</td>
<td>1, 2, 3, 5 minutes</td>
<td>1</td>
</tr>
<tr>
<td>Reset Admin Account Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
</tr>
<tr>
<td>Lock User Account After Failed Logins</td>
<td>Off, 2-10</td>
<td>3</td>
</tr>
<tr>
<td>User Account Lock Duration</td>
<td>1, 2, 3, 5, 10, 20, 30 minutes</td>
<td>1 minute</td>
</tr>
<tr>
<td></td>
<td>1, 2, 4, 8 hours</td>
<td></td>
</tr>
<tr>
<td>Reset User Account Lock Counter After</td>
<td>Off, [1..24] hours</td>
<td>Off</td>
</tr>
<tr>
<td><strong>Login Credentials</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Room Password for Remote Access</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require User Login for System Access</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Password Requirements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-32</td>
<td>Off</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>Off, 1, 2, 3, 4, all</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1, 2, 3, 4</td>
<td>Off</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Off, 1-7</td>
<td>Off</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Selected</td>
</tr>
<tr>
<td><strong>User Room</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-32</td>
<td>Off</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>Off, 1, 2, 3, 4, all</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1, 2, 3, 4</td>
<td>Off</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Off, 1-7</td>
<td>Off</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Selected</td>
</tr>
<tr>
<td><strong>Meeting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-32</td>
<td>Off</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low</td>
<td>Configurable?</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1, 2, 3, 4</td>
<td>Off</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**Remote Access**

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Default</td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-32</td>
<td>Off</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>Off, 1, 2, 3, 4, all</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1, 2, 3, 4</td>
<td>Off</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Off, 1-7</td>
<td>Off</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Selected</td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low</td>
<td>Configurable?</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>Range</td>
<td>Default</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off, 1-32</td>
<td>Off</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>Off, 1, 2, all</td>
<td>Off</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off, 1-16</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>Off, 1, 5, 10, 15, 20, 30</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>Off, 1, 2, 3, 4</td>
<td>Off</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>none</td>
<td>Off</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>Checkbox</td>
<td>Not Selected</td>
</tr>
<tr>
<td><strong>Certificates &gt; Certificate Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Browser</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Server</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Revocation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revocation Method</td>
<td>OCSPCRL</td>
<td>OCSP</td>
</tr>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Security Banner</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Security Banner</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Banner Text</td>
<td>DodCustom</td>
<td>Custom</td>
</tr>
<tr>
<td>Local System Banner Text</td>
<td>Unicode characters, 2048 bytes max</td>
<td>Null (no text)</td>
</tr>
<tr>
<td>Admin Setting</td>
<td>Low Range</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Remote System Banner Text</td>
<td>Unicode characters, 2048 bytes max</td>
<td>Null (no text)</td>
</tr>
<tr>
<td><strong>Servers &gt; Directory Servers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Type</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>Polycom GDS</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Registration Status</td>
<td>N/A</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version 1</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Version 2c</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Version 3</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Calendaring Service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Calendaring Service</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Recording Service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable RealPresence Recording Suite</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Checkbox</td>
<td>Status text</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Diagnostics &gt; System &gt; System Log Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Remote Logging</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remote Log Server Transport Protocol</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Call Speeds and Resolutions

Topics:

• Point-to-Point Call Speeds
• Multipoint Call Speeds for RealPresence Centro Systems
• High-Profile Call Speeds and Resolutions
• Multipoint Resolutions for High Definition Video for RealPresence Centro Systems
• Resolution and Frame Rates for Content Video

Point-to-Point Call Speeds

The maximum allowable H.323/SIP point-to-point call speed for the RealPresence Centro system is 6144 kbps.

Multipoint Call Speeds for RealPresence Centro Systems

The following table shows the maximum allowable H.323/SIP call speeds for the number of sites in a call. Maximum speeds can be further limited by the communications equipment. Multipoint option keys are required for some of the capabilities shown in the table.

<table>
<thead>
<tr>
<th>Number of Sites in Call</th>
<th>Max Speed for Each Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3072 kbps</td>
</tr>
<tr>
<td>4</td>
<td>2048 kbps</td>
</tr>
<tr>
<td>5</td>
<td>1536 kbps</td>
</tr>
<tr>
<td>6</td>
<td>1152 kbps</td>
</tr>
</tbody>
</table>

High-Profile Call Speeds and Resolutions

The following table includes the H.264 high-profile resolutions and frame rates sent in calls between two RealPresence Centro systems.

Resolutions and frame rates are based on the call speed and the Optimized for setting of your video input.

Due to the complexities of system capabilities and the call types and scenarios in your environment, it isn’t possible to provide the resolutions and frame rates for calls between a system and a different type of...
endpoint or multipoint resource. The systems attempt to provide the highest resolutions and 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.

### Call Speeds and Resolutions in High-Profile Calls

<table>
<thead>
<tr>
<th>Call Speed (kbps)</th>
<th>Motion/Sharpness</th>
<th>Resolution</th>
<th>Max Frame Rate (fps)</th>
<th>Resolution</th>
<th>Max Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;160</td>
<td>Motion</td>
<td>512x288</td>
<td>60</td>
<td>512x288</td>
<td>60</td>
</tr>
<tr>
<td>160-511</td>
<td>Motion</td>
<td>640x368</td>
<td>60</td>
<td>640x368</td>
<td>60</td>
</tr>
<tr>
<td>512-831</td>
<td>Motion</td>
<td>848x480</td>
<td>60</td>
<td>848x480</td>
<td>60</td>
</tr>
<tr>
<td>832-895</td>
<td>Motion</td>
<td>1024x576</td>
<td>60</td>
<td>720x832</td>
<td>60</td>
</tr>
<tr>
<td>896-1727</td>
<td>Motion</td>
<td>1280x720</td>
<td>60</td>
<td>1280x720</td>
<td>60</td>
</tr>
<tr>
<td>&gt;=1728</td>
<td>Motion</td>
<td>1280x720</td>
<td>60</td>
<td>1920x1080</td>
<td>60</td>
</tr>
<tr>
<td>&lt;128</td>
<td>Sharpness</td>
<td>640x368</td>
<td>30</td>
<td>640x368</td>
<td>30</td>
</tr>
<tr>
<td>128-511</td>
<td>Sharpness</td>
<td>1024x576</td>
<td>30</td>
<td>1024x576</td>
<td>30</td>
</tr>
<tr>
<td>512-1023</td>
<td>Sharpness</td>
<td>1280x720</td>
<td>30</td>
<td>1280x720</td>
<td>30</td>
</tr>
<tr>
<td>&gt;=1024</td>
<td>Sharpness</td>
<td>1280x720</td>
<td>30</td>
<td>1920x1080</td>
<td>30</td>
</tr>
</tbody>
</table>

### Multipoint Resolutions for High Definition Video for RealPresence Centro Systems

Polycom offers enhanced high definition (HD) multipoint resolutions, maximizing video quality in multipoint conferences for RealPresence Centro systems. This feature increases the maximum transmitting and receiving video resolutions in multipoint video conferences. During a multipoint video conference, if any endpoints in the video conference do not support high resolution video and transmit lower resolution video, all endpoints receive lower resolution video.
The maximum Multipoint Control Unit (MCU) transmitting and receiving resolutions are specified in the following table. Note that changing from discussion to speaker does not alter the transmit of 960x540 from an endpoint and the receive of 1080p from the endpoints.

RealPresence Centro systems support one endpoint as a host system and up to 5 other endpoints in a 6-way multipoint conference.

<table>
<thead>
<tr>
<th>Number of Endpoints in the Video Conference</th>
<th>Maximum Transmitting Resolutions</th>
<th>Maximum Receiving Resolutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-4 endpoints</td>
<td>1080p, 30fps</td>
<td>960x540p, 30fps</td>
</tr>
<tr>
<td>5-8 endpoints</td>
<td>720p, 30fps</td>
<td>640x368p, 30fps</td>
</tr>
</tbody>
</table>

**Resolution and Frame Rates for Content Video**

The high frame rates with high resolution apply only to point-to-point calls above 832 kbps on RealPresence Centro systems. In addition, you must set Optimized for value of your Camera input to Sharpness. Low frame rates apply if your call does not meet these requirements.

For multipoint calls, the maximum resolution and frame rate for content is 720p @ 30 fps.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Encode Resolution</th>
<th>Sharpness</th>
<th>Motion</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 x 600</td>
<td>800 x 600</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>1024 x 768</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1280 x 720</td>
<td>1280 x 720</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1280 x 768</td>
<td>1280 x 720</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1280 x 1024</td>
<td>1280 x 1024</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1600 x 1200</td>
<td>1280 x 1024</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1680 x 1050</td>
<td>1280 x 720</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>1920 x 1080</td>
<td>1920 x 1080</td>
<td>30</td>
<td>60*</td>
</tr>
</tbody>
</table>

*Available only when the Quality Preference setting on your system is set to Content in Admin Settings > Network > IP Network > Network Quality.*