# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Before You Begin</strong></td>
<td>10</td>
</tr>
<tr>
<td>Get Help</td>
<td>10</td>
</tr>
<tr>
<td>The Polycom Community</td>
<td>10</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>11</td>
</tr>
<tr>
<td>RealPresence OTX Studio Monitor Lifts</td>
<td>11</td>
</tr>
<tr>
<td>Automatically Controlling Monitor Lifts</td>
<td>11</td>
</tr>
<tr>
<td>Manually Controlling Monitor Lifts</td>
<td>11</td>
</tr>
<tr>
<td>Controlling the Monitor Lifts from the Web Interface</td>
<td>11</td>
</tr>
<tr>
<td>Power On Self Test (POST)</td>
<td>12</td>
</tr>
<tr>
<td>Obtaining the Network Parameters</td>
<td>12</td>
</tr>
<tr>
<td><strong>Placing Calls and Managing Contacts</strong></td>
<td>13</td>
</tr>
<tr>
<td>Viewing the Home Page</td>
<td>13</td>
</tr>
<tr>
<td>Placing a Call</td>
<td>13</td>
</tr>
<tr>
<td>Calling a Favorites Contact</td>
<td>13</td>
</tr>
<tr>
<td>Placing a Call Manually</td>
<td>13</td>
</tr>
<tr>
<td>Calling a Speed Dial Contact</td>
<td>14</td>
</tr>
<tr>
<td>Placing an Audio-Only Call from Web Interface</td>
<td>14</td>
</tr>
<tr>
<td>Using Directories</td>
<td>14</td>
</tr>
<tr>
<td>Directory Capacity</td>
<td>14</td>
</tr>
<tr>
<td>Managing Favorites</td>
<td>15</td>
</tr>
<tr>
<td>Creating a New Favorite Contact</td>
<td>15</td>
</tr>
<tr>
<td>Creating a Favorites Group</td>
<td>15</td>
</tr>
<tr>
<td>Editing a Favorites Group</td>
<td>15</td>
</tr>
<tr>
<td>Deleting a Favorites Contact or Group</td>
<td>16</td>
</tr>
<tr>
<td>Adding a Speed Dial Contact</td>
<td>16</td>
</tr>
<tr>
<td>Removing a Speed Dial Contact</td>
<td>16</td>
</tr>
<tr>
<td>Types of Favorites Contacts</td>
<td>16</td>
</tr>
<tr>
<td><strong>Configuring the Admin Settings</strong></td>
<td>18</td>
</tr>
<tr>
<td>General Settings</td>
<td>18</td>
</tr>
<tr>
<td>Contact and Location Information</td>
<td>18</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>System Contact</td>
<td>18</td>
</tr>
<tr>
<td>Location</td>
<td>19</td>
</tr>
<tr>
<td>System Settings</td>
<td>19</td>
</tr>
<tr>
<td>System Name</td>
<td>19</td>
</tr>
<tr>
<td>Call Settings</td>
<td>20</td>
</tr>
<tr>
<td>Including an Additional Audio Call</td>
<td>20</td>
</tr>
<tr>
<td>Disabling Audio-Only Calls</td>
<td>21</td>
</tr>
<tr>
<td>Enabling Audio-Only Calls</td>
<td>21</td>
</tr>
<tr>
<td>Audio Dialing Order</td>
<td>21</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>21</td>
</tr>
<tr>
<td>Remote Control, Keypad, and Power Settings</td>
<td>21</td>
</tr>
<tr>
<td>Polycom VisualBoard™ Application</td>
<td>22</td>
</tr>
<tr>
<td>Home Screen Settings</td>
<td>22</td>
</tr>
<tr>
<td>Background Image</td>
<td>22</td>
</tr>
<tr>
<td>Custom System Background</td>
<td>22</td>
</tr>
<tr>
<td>Pairing Settings</td>
<td>22</td>
</tr>
<tr>
<td>Polycom Touch Device</td>
<td>23</td>
</tr>
<tr>
<td>SmartPairing</td>
<td>23</td>
</tr>
<tr>
<td>Date and Time</td>
<td>23</td>
</tr>
<tr>
<td>RS-232 Serial Port Settings</td>
<td>25</td>
</tr>
<tr>
<td>Polycom® Concierge Solution</td>
<td>25</td>
</tr>
<tr>
<td>Adding the System Pairing Code to the RealPresence Touch Home Screen</td>
<td>26</td>
</tr>
<tr>
<td>Checking the Polycom Concierge Service Status</td>
<td>26</td>
</tr>
<tr>
<td>Enabling Software Options</td>
<td>26</td>
</tr>
<tr>
<td>Software Updates</td>
<td>27</td>
</tr>
<tr>
<td>Installing Software Updates</td>
<td>27</td>
</tr>
<tr>
<td>Installing Software Updates Manually</td>
<td>27</td>
</tr>
<tr>
<td>Installing Software with Automatic Updates</td>
<td>27</td>
</tr>
<tr>
<td>Networks</td>
<td>28</td>
</tr>
<tr>
<td>LAN Status Lights</td>
<td>28</td>
</tr>
<tr>
<td>LAN Properties</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the IP Addresses of the Component Codecs</td>
<td>30</td>
</tr>
<tr>
<td>IP Network Settings</td>
<td>31</td>
</tr>
<tr>
<td>Network Quality Setting</td>
<td>31</td>
</tr>
<tr>
<td>H.323 Settings</td>
<td>32</td>
</tr>
<tr>
<td>SIP Settings</td>
<td>33</td>
</tr>
<tr>
<td>SIP Address Naming Convention</td>
<td>35</td>
</tr>
<tr>
<td>Configuring SIP Settings for Integration with the Telepresence Interoperability Protocol (TIP)</td>
<td>36</td>
</tr>
<tr>
<td>RTV and Lync-Hosted Conference Support</td>
<td>36</td>
</tr>
</tbody>
</table>
Polycom, Inc.

Using a Provisioning Service ................................................................. 65
  Enabling or Disabling the Provisioning Service .................................. 66
  Provisioning Service Settings ............................................................ 66
Connecting to the Microsoft Exchange Server Calendaring Service .......... 67
Setting Up the Distributed Media Service .............................................. 68
  There should be a MLA registered to the RMX for applying the proper layouts. 69
Configuring the Distributed Media Service ............................................. 69

Immersive Settings .................................................................................. 70
Room Control Devices .............................................................................. 70

Configuring the Diagnostic Settings ...................................................... 72
  Polycom RealPresence Manageability Instrumentation Solution ............. 72
  Web Interface Diagnostics Screens ......................................................... 72
  System Diagnostics ................................................................................ 72
System Information .................................................................................. 73
  Call Statistics ......................................................................................... 73
  System Status ......................................................................................... 74
Download Logs ......................................................................................... 75
System Log Settings ................................................................................ 75
Restarting the System ............................................................................... 76
Sessions ..................................................................................................... 76
Audio and Video Tests ............................................................................... 77
  Audio Meters ......................................................................................... 77
  Calibrating the Microphone .................................................................. 77

Configuring the Utilities Settings ............................................................ 78
  Managing System Profiles ..................................................................... 78
  Storing a Profile .................................................................................... 78
  Uploading a Profile ............................................................................... 78
  Call Detail Report (CDR) ........................................................................ 79
  Enabling CDR ....................................................................................... 79
  Viewing and Downloading the CDR ....................................................... 79
  Information in the Call Detail Report (CDR) .......................................... 79
  Sending a Message .................................................................................. 82
  Monitoring a Room or Call .................................................................... 83
  Displaying a Closed Caption .................................................................. 83

Security Profile Definitions ....................................................................... 84
  Configuring the Low Security Profile .................................................... 84
Configuring Polycom RealPresence Touch ............................................. 89
   Performing the RealPresence Touch Out-of-Box Setup ............................ 89
   Pairing RealPresence Touch with RealPresence Immersive Studio or RealPresence OTX Studio ................................................................. 89
   Customizing the RealPresence Touch Home Screen ................................. 90
      Choosing Icon Buttons That Display on the RealPresence Touch Home Screen ..... 90
      Customizing the Place a Call Screen Icon Buttons on the RealPresence Touch Device ............................................................... 91
   Changing the Background Image of the Home Screen on the RealPresence Touch Device ............................................................ 91
   Changing to a Custom Background Image on the RealPresence Touch ................ 91
The tables in the document are listed as follows:

- Guidelines for Entering Contact Addresses
- Types of Favorites Contacts
- Optional Contact Information
- Location Settings
- System Call Settings
- Security Profiles and SmartPairing
- System Time Settings
- Time in Call Settings
- LAN Status Lights
- IP Address (IPv4) Settings
- LAN Options
- Network Quality Settings
- H.323 Settings
- SIP Settings
- SIP Address Naming Convention
- Quality of Service Settings
- Dialing Options and Preferred Speeds
- General Audio Settings
- Audio Input Settings
- Audio Output Setting
- Authentication Settings
- Access Settings
- Encryption Settings
- Account Lockout Settings
- Login Credentials
- Password Policy Settings
- Log Management Settings
- Directory Servers Supported in Standard Operating Mode
- Directory Servers Supported by Polycom RealPresence Resource Manager Provisioning
- LDAP Server Settings
- Microsoft Directory Server Settings
- SNMP Settings
- Provisioning Service Settings
- Calendaring Settings
- Multipoint Server Settings
- Room Device Settings
System Log Settings ................................................................. 75
Call Detail Report Information ................................................. 80
Low Security Profile Settings .................................................... 84
Before You Begin

This guide is intended for administrators who need to configure, customize, manage, and troubleshoot Polycom® RealPresence Immersive Studio™ and Polycom® RealPresence® OTX® Studio systems. Refer to this guide after installation of the furniture and video communication systems is complete.

Please read the RealPresence Immersive Studio and RealPresence OTX Studio system documentation before you install or operate the system. Related documents for RealPresence Immersive Studio and RealPresence OTX Studio systems are available from the Polycom Video Documentation Support site. For support or service, please contact your Polycom distributor or go online to Polycom Support.

Get Help

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

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.
Introduction

The Polycom® RealPresence Immersive Studio™ system and Polycom® RealPresence® OTX® Studio system are state-of-the-art visual collaboration tools. With crisp, clean video and crystal-clear sound, Polycom RealPresence Immersive Studio and Polycom RealPresence OTX Studio systems provide natural video conferencing interaction using the most robust video communications technology. If your organization has signed on for Video Network Operations Center (VNOC) services, the VNOC will handle many telepresence conferencing tasks for you.

RealPresence OTX Studio Monitor Lifts

You can raise or lower RealPresence OTX Studio table monitor lifts for optimum conference viewing. The monitor lifts are partially automated and can also be manually controlled.

Automatically Controlling Monitor Lifts

All three monitors automatically raise or lower in the following circumstances:

- When content is started the monitors rise.
- When content is used during a call and the call ends, the monitors lower.
- When the system powers on or during a restart the monitors lower. During initial start-up and restarts all monitor controls are locked.

Manually Controlling Monitor Lifts

After initial start-up, the individual buttons in the RealPresence OTX Studio table toggle the state of the associated lift. Full extension or retraction takes about 15 seconds. If you use the buttons while the monitors are moving, the direction the monitors are traveling reverses. The monitors will only fully stop in the middle of travel during a mechanical collision or a system power failure.

Controlling the Monitor Lifts from the Web Interface

You can raise or lower all three monitors from the web interface.

To raise or lower monitors from the web interface:

» Go to Utilities > Tools > OTX Setup and select Up or Down.
Power On Self Test (POST)

When the power is cycled, the RealPresence Immersive Studio system automatically performs a system health check before initialization. This process is known as a power on self test, or POST. All test results are logged in the system’s memory.

When the POST sequence completes with no severe errors, the RealPresence Immersive Studio system starts normally. If a severe error occurs, the system will not initialize. In that case, contact Polycom technical support.

Obtaining the Network Parameters

To perform some of the configuration tasks in this document, you must obtain the proper network parameters.

To obtain the network parameters:

Obtain the following network parameters from the customer.

- Subnet Mask
- Default Gateway
- IP addresses
  - A block of 20 static IP addresses is required.
  - The base IP should be identified (for example, 10.10.10.x).
  - Define x as an offset (for example, 50).
  - The IP addresses should be assigned as shown in the next table.

### IP Address Map

<table>
<thead>
<tr>
<th>...x+</th>
<th>Device</th>
<th>...x+</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GS 700 (A1)</td>
<td>11</td>
<td>Display1 (D1)</td>
</tr>
<tr>
<td>2</td>
<td>GS 500 (A2)</td>
<td>12</td>
<td>Display2 (D2)</td>
</tr>
<tr>
<td>3</td>
<td>GS 500 (A3)</td>
<td>13</td>
<td>Display3 (D3)</td>
</tr>
<tr>
<td>4</td>
<td>&lt;Reserved&gt;</td>
<td>14</td>
<td>&lt;Reserved&gt;</td>
</tr>
<tr>
<td>5</td>
<td>SoundStructure</td>
<td>15</td>
<td>&lt;Reserved&gt;</td>
</tr>
<tr>
<td>6</td>
<td>Nport</td>
<td>16</td>
<td>Lutron NWK</td>
</tr>
<tr>
<td>7</td>
<td>&lt;Reserved&gt;</td>
<td>17</td>
<td>APC (PWR1)</td>
</tr>
<tr>
<td>8</td>
<td>DisplayMatrix</td>
<td>18</td>
<td>APC (PWR2)</td>
</tr>
<tr>
<td>9</td>
<td>&lt;Reserved&gt;</td>
<td>19</td>
<td>APC (PWR3)</td>
</tr>
<tr>
<td>10</td>
<td>Tablet</td>
<td>20</td>
<td>Ethernet Switch (if required)</td>
</tr>
</tbody>
</table>
Placing Calls and Managing Contacts

This section describes how to place calls and manage contacts in the RealPresence Immersive Studio and RealPresence OTX Studio systems.

Viewing the Home Page

When you select the Place a Call link on the web interface, the default view shows you the operations that you can perform:

- Place a Call
- Speed Dial

Placing a Call

There are several methods for placing a call. Most require that you have stored information about the contacts you want to call. For procedures on storing contact information, refer to Managing Favorites.

Calling a Favorites Contact

You can search for a contact in your Favorites list.

To call a Favorites contact:

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

Placing a Call Manually

You can place a call by dialing manually.

To place a call manually:

2. Enter the number.
3. To enter a password to dial into an H.323 call on a standalone Group Series that is configured to require a password, select Meeting Password, and enter a password in the field that is displayed below the check box.
4. Select Call.
   The call is placed according to the default settings you selected in Admin Settings > Network > Dialing Preferences. You can select options other than the defaults in the two drop-down lists below the text entry field.

**Calling a Speed Dial Contact**

You can make a call by choosing a contact from the Speed Dial list.

**To call a speed dial contact:**
» In the Speed Dial section, select a contact from the list, and select Call.

**Placing an Audio-Only Call from Web Interface**

When the audio-only calls setting is enabled, you can place an audio only call from the web interface.

**To place an audio only call from the Web Interface:**

1. In the web interface, go to Place a Call > Manual Dial > Call Type: Audio.
2. Enter the number and click Call.

**Using Directories**

Storing frequently-used contacts and groups in the directory can help users find calling information quickly and easily. Polycom RealPresence Immersive Studio systems support global groups and Favorites groups.

**Directory Capacity**

RealPresence Immersive Studio systems support up to 2,000 Favorites that users create within Favorites. RealPresence Immersive Studio systems can also support one of the following:

- Up to 200 additional contacts with presence, which appear in Favorites, when registered with Microsoft Lync Server 2013 or Skype for Business Server 2015.
- Up to 200 additional contacts with presence, which appear in Favorites, when registered with Polycom RealPresence Resource Manager.
- An unlimited number of contacts when the RealPresence Immersive Studio system is registered with Microsoft Lync Server 2013 or Skype for Business Server 2015.

Polycom RealPresence Immersive Studio systems support up to 200 Favorites groups that users create within Favorites. If the system is connected to a global directory server, it can also support one of the following:

- Up to 64 additional groups from the Microsoft Lync Server, which appear in the Favorites group.
- Up to 200 additional distribution groups from Polycom RealPresence Resource Manager, which appear in the Global Directory group.
Managing Favorites

You can enter frequently called contacts as Favorites to facilitate dialing. The following table shows how to enter Favorite addresses.

Guidelines for Entering Contact Addresses

<table>
<thead>
<tr>
<th>System or Address Type</th>
<th>Format or Sequence for Entering Addresses, Separated by Semicolons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two screens</td>
<td>Right; Left.</td>
</tr>
<tr>
<td>Three screens</td>
<td>Center; Left; Right.</td>
</tr>
<tr>
<td>Four screens</td>
<td>Center right; Center Left; Far Right; Far Left</td>
</tr>
<tr>
<td>Meeting Room/Bridge</td>
<td>Enter the VMR Number three times for the fastest connection.</td>
</tr>
<tr>
<td>H.323 Address</td>
<td>Enter the H.323 alias or E.164 extension in the H.323 field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Avoid entering an H.323 address and a SIP address in the same Favorite entry.</td>
</tr>
</tbody>
</table>

Creating a New Favorite Contact

You can create a new Favorite contact not currently included in the Directory list.

**To create a new Favorite contact that is not in the Directory list:**

1. Go to Manage Favorites, and select Create New Favorite.
2. Enter the contact call information.
3. Select Save.

Creating a Favorites Group

You can create a new group of Favorites. Dialing from a group is not supported.

**To create a Favorites group:**

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

Editing a Favorites Group

You can edit a Favorites group to add or remove contacts.
To edit a Favorites group:

1. Find the group name in the list of contacts.
2. Next to the group contact name, select Edit Group.
   
   Do one of the following:
   
   ➢ To add contacts to the group, select Add From Directory, enter a contact name, select Search, and then Add to add a contact.
   
   ➢ To remove contacts from the group, select a contact name and select Remove.
3. Repeat the above steps to continue adding or removing contacts.
4. Select Done.

Deleting a Favorites Contact or Group

You can delete a contact or a complete group from Favorites.

To delete a Favorites contact or group:

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

Adding a Speed Dial Contact

You can add a new contact to a Speed Dial list.

To add a speed dial contact:

1. Go to Place a Call > Speed Dial and select Edit.
2. Enter a contact name, and select Search.
3. In the contact you want to add, select Add.
4. To save your changes, select Done.

Removing a Speed Dial Contact

You can remove a contact from a Speed Dial list.

To remove a speed dial contact:

1. Go to Place a Call > Speed Dial and select Edit.
2. In the contact you want to delete, select Remove.
3. To save your changes, select Done.

Types of Favorites Contacts

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

<table>
<thead>
<tr>
<th>Directory Server Registration</th>
<th>Types of Contacts</th>
<th>Presence State Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom GDS</td>
<td>Not supported.</td>
<td></td>
</tr>
</tbody>
</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.  
Administrators can delete these entries from Favorites.  
Administrators can copy these entries to other Favorites and remove them from those groups.  
Non-administrative users cannot edit these entries. | Unknown |
| LDAP by a Polycom RealPresence Resource Manager System | • 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 Polycom RealPresence Resource Manager.  
Administrators can delete these entries from Favorites.  
Administrators can copy these entries to other Favorites and remove them from those groups.  
Non-administrative users cannot edit these entries.  
LDAP directory entries saved as Favorites by the user and stored with the presence service.  
Administrators can delete these entries from Favorites.  
Administrators can copy these entries to other Favorites and remove them from those groups.  
Non-administrative users cannot edit these entries. | Unknown |
| Microsoft                     | Microsoft Lync Server directory entries saved as Contacts by the user in Office Communicator and stored on the Microsoft Lync Server.  
Administrators must create their contact lists using Microsoft Office Communicator on a computer.  
Administrators can copy these entries to other Favorites and remove them from those groups.  
Users cannot edit or delete these entries from Favorites using the Polycom RealPresence Immersive Studio system. | Real-time presence |
Configuring the Admin Settings

General Settings

Some of the information saved in these settings is not used in this release of the RealPresence Immersive Studio or RealPresence OTX Studio.

Contact and Location Information

You can specify contact information for your RealPresence Immersive Studio or RealPresence OTX Studio system so that others know whom to call when they need assistance.

System Contact

You can specify system contact information for your RealPresence Immersive Studio or RealPresence OTX Studio system.

To specify system contact information:

1. Go to Admin Settings > General Settings > My Information > Contact Information.
2. Configure these settings.

Optional Contact Information

<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>For RealPresence Immersive Studio specifies the name of the person who provides technical support. For RealPresence OTX Studio specifies the help desk phone number.</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>
</tbody>
</table>

You can also specify regional settings.
Location
You can specify location settings for your RealPresence Immersive Studio system.

To configure location settings:

1. Go to Admin Settings > General Settings > My Information > Location.
2. Configure these settings.

Location 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. Changing the country automatically adjusts the country code associated with your system.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Displays the country code associated with the country where the system is located.</td>
</tr>
</tbody>
</table>

System Settings
The System Settings screen provides access to high-level options for the entire system.

System Name
The System Name screen enables you to name your system and your center, left, and right server names. When naming the sites, keep the following in mind:

- Do not use site names which are the same or similar (site names with a trailing numeral digit, for instance) for Group Series codecs that are part of Immersive Studio or OTX Studio room systems and for individual endpoints that are not part of Immersive Studio or OTX Studio room systems.
- For individual endpoints, disconnected from a telepresence conference, use the same or similar names as each other and as Immersive Studio or OTX Studio systems, then Polycom MLA sometimes mistakenly identifies the individual endpoints as Immersive Studio, OTX Studio, or ITP systems.
- The TYPE OF ITP field enables Polycom Multipoint Layout Application to find the correct Immersive Studio or OTX Studio room, when the Immersive Studio or OTX Studio room is part of a telepresence conference participants list, but disconnected from the conference.

To configure a system name:

1. Go to Admin Settings > General Settings > System Settings > System Name.
   The first character of a System Name must be a letter or a number. The System Name cannot begin with the dollar sign ($) or underscore (_) character.
2. In the System Name field, enter a name as described below.
   » Enter the <SiteName>[TYPE OF ITP].
     "[TYPE OF ITP]" is optional and specifies the type of ITP room: “RIS” for RealPresence Immersive Studio
     When you assign a system name for the main codec, unique identities for the left and right codecs are automatically generated. The naming convention is as follows.
     <SiteName>[TYPE OF ITP]_M_N where:
Configuring the Admin Settings

- M = number of systems (for RealPresence Immersive Studio, this value is 3)
- N = 1 for the primary system, 2 for the left system, and 3 for the right system

The system name is displayed on the screen for the far site when you are in a call.

3 Select Save.

Call Settings

The call settings screen enables you to determine which settings are available to users when they place and answer calls.

To configure call settings:

1 In the primary codec web UI, go to Admin Settings > General Settings > System Settings > Call Settings.
2 Configure these settings.

System Call Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Time in Call</td>
<td>Enter the maximum number of hours allowed for call length. When that time has expired, you see a message asking whether you want to hang up or stay in the call. If you do not answer within one minute, the call automatically disconnects. If you choose to stay in the call at this time, you will not be prompted again. Selecting Off removes any limit. This setting also applies when you are viewing the Near video screen or showing content, even if you are not in a call. If the maximum time is reached while viewing Near video, the system automatically returns to the Home screen. If content is being shown, the content stops.</td>
</tr>
<tr>
<td>Auto Answer Point-to-Point Video</td>
<td>Sets the answer mode for calls with one site.</td>
</tr>
<tr>
<td></td>
<td>• Yes—Answers calls automatically.</td>
</tr>
<tr>
<td></td>
<td>• No—Enables you to answer calls manually.</td>
</tr>
<tr>
<td></td>
<td>• Do Not Disturb—Disables incoming calls from being processed.</td>
</tr>
<tr>
<td>Enable Flashing Incoming Call Notification</td>
<td>Select check box to enable flashing for incoming calls.</td>
</tr>
<tr>
<td>Preferred ‘Place a Call’ Navigation</td>
<td>Sets the preferred method to place a call.</td>
</tr>
<tr>
<td></td>
<td>• Dial Pad</td>
</tr>
<tr>
<td></td>
<td>• Contacts</td>
</tr>
</tbody>
</table>

Including an Additional Audio Call

You can add an audio-only call to a video conference from your system.

Keep in mind the following points:

- When the multipoint option is disabled, the system supports one video call and one audio-only call.
● Audio-only calls can be encrypted and unencrypted independently from video calls. An audio call cannot join an encrypted video conference.

Disabling Audio-Only Calls
You can disable this setting so audio calls are not supported.

To disable Audio Add In:
1. In the web interface, go to Admin Settings > Network > Dialing Preference > Dialing Options.
2. Clear the Enable Audio Add In checkbox. Click Save.

Enabling Audio-Only Calls
You can enable this setting so audio calls are supported.

To enable Audio Add In:
1. In the web interface, go to Admin Settings > Network > Dialing Preference > Dialing Options.
2. Select Enable Audio Add In. Click Save.

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

To choose Audio Dialing Order:
1. In the web interface, go to Admin Settings > Network > Dialing Preference > Dialing Options > Call Type Order.
2. Choose the preferred Audio Dial Preference 1 and 2 from the following options:
   - IP H.323.
   - SIP.
3. Click Save.

Recent Calls
Generating a Call Detail Report is supported in the RealPresence Immersive Studio system. Note that Clear Recent Calls is not supported.

To enable generating a Call Detail Report:
1. Go to Admin Settings > General Settings > System Settings > Recent Calls.
2. Select Call Detail Report.

Remote Control, Keypad, and Power Settings
These functions are not supported in the RealPresence Immersive Studio system.
Polycom VisualBoard™ Application

The Polycom VisualBoard™ application allows you to show and annotate content in real time from Polycom RealPresence Group systems by using a touch display.

To enable the VisualBoard application:

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

Home Screen Settings

Background Image

The RealPresence Immersive Studio system and the OTX Studio system displays a blank wallpaper; however, three optional wallpaper images are available from the web interface.

To change the background image:

1. Go to **Admin Settings > General Settings > Home Screen Settings > Wall Paper**.
2. Select the image that you want to use. The selected image is displayed on the main monitor and on the tablet.

Custom System Background

The RealPresence Immersive Telepresence Studio system, the OTX Studio system, and the RealPresence Touch device allow you to upload a background image in addition to letting you select wallpaper. You can upload an image to display as the background of all monitors on a multi-screen system.

Use the following image guidelines:

- Less than 15 MB
- JPEG file format
- Pixel size of 1920 x 1080 (width by height) for custom tiled wallpaper, displayed on each ITP screen.
- Pixel size of 5760 x 1080 (width by height) for custom panoramic wallpaper, displayed across all ITP screens.

To upload a custom background to the system:

1. Go to **Admin Settings > General Settings > Home Screen Settings > Wall Paper > Background**.
2. Browse to the desired image file and click **Choose File > Upload**.
3. Select the image that you want to use and click **Save**.
   
The custom image displays on the main monitor or monitors.

Pairing Settings

Specify pairing settings to enable touch devices to pair with the system.
Polycom Touch Device
Select **Enable Polycom Touch Device** to enable the touch device to operate the system.

**SmartPairing**
SmartPairing allows you to detect and pair a RealPresence Immersive Studio or RealPresence OTX Studio system from the RealPresence Mobile application on an Android or Apple iPad tablet. After you pair the application and the RealPresence Immersive Studio or RealPresence OTX Studio system, you can use the RealPresence Mobile application to send content from the RealPresence Mobile application to the RealPresence Immersive Studio or RealPresence OTX Studio system.

Be aware that Telnet must be enabled before you can use SmartPairing. Because Telnet is disabled by default in all Security Profiles, SmartPairing is also disabled by default. The Telnet enable setting 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: 1 Enable Telnet. 2 Send API command or use web interface.</td>
</tr>
</tbody>
</table>

**To configure SmartPairing:**
1. In the 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>
</table>
| SmartPairing Mode    | Specifies the method used to pair with the RealPresence Immersive Studio system, if SmartPairing is enabled:  
  • Disabled  
  • Automatic  
  • Manual |
| Signal Volume        | Specifies the relative signal strength of the ultrasonic signal within the loudspeaker audio output signal. |

**Note:**
Each paired device is displayed in **Diagnostics > System > Sessions**.

**Date and Time**
System Time settings enable you to specify how date and time values are displayed.
To configure date and time settings:

1. Go to Admin Settings > General Settings > Date and Time > System Time.
2. Configure these settings.

**System Time 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>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>Time Zone</td>
<td>Specifies the time difference between Greenwich Mean Time (GMT) 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 and optional secondary time servers to use when Time Server is set to Manual. The system uses the secondary time server if the primary time server does not respond.</td>
</tr>
<tr>
<td>Secondary Time Server Address</td>
<td></td>
</tr>
<tr>
<td>Current Date</td>
<td>If Time Server is set to Off, these settings are configurable.</td>
</tr>
<tr>
<td>Current Time</td>
<td></td>
</tr>
</tbody>
</table>

You can also choose whether and how to display the time spent in a call.

**To configure Time in Call settings:**

*Note:*
Time in Call settings are displayed on the web interface.

1. Go to Admin Settings > General Settings > Date and Time > Time in Call.
2. Configure these settings.

**Time in Call Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Time in Call</td>
<td>Specifies the time display in a call:</td>
</tr>
<tr>
<td></td>
<td>• Elapsed Time—Displays the amount of time in the call.</td>
</tr>
<tr>
<td></td>
<td>• System Time—Displays the system time on the screen during a call.</td>
</tr>
<tr>
<td></td>
<td>• Off—Time is not displayed.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

### Time in Call Settings

<table>
<thead>
<tr>
<th>When to Show</th>
<th>Specifies when the time should be shown:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Start of the call only</strong>—Displays only when the call begins</td>
</tr>
<tr>
<td></td>
<td>• <strong>Entire call</strong>—Displays continuously throughout the call</td>
</tr>
<tr>
<td></td>
<td>• <strong>Once per hour</strong>—Displays at the beginning of the hour for one minute</td>
</tr>
<tr>
<td></td>
<td>• <strong>Twice per hour</strong>—Displays at the beginning of the hour and midway through the hour for one minute</td>
</tr>
</tbody>
</table>

| Show Countdown Before Next Meeting | When enabled, it displays a timer that counts down to the next scheduled meeting 10 minutes before that meeting. If a timer is already showing, the countdown timer replaces it 10 minutes before the next scheduled meeting. |

### RS-232 Serial Port Settings

This option is not supported in this release of the RealPresence Immersive Studio or RealPresence OTX Studio system.

### Polycom® Concierge Solution

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

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

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

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

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

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

Adding the System Pairing Code to the RealPresence Touch Home Screen

To display a pairing code on the RealPresence Touch device home screen, you must enable a setting in the RealPresence Immersive Studio or OTX Studio system web interface.

To add the system pairing code to the home screen:

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

The pairing code for the RealPresence Immersive Studio or OTX Studio system displays on the bottom of the RealPresence Touch device’s home screen.

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

Checking the Polycom Concierge Service Status

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

To check the status of the Polycom Concierge service:

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

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

Enabling Software Options

Some of the features of a RealPresence Immersive Studio system are optional. To activate these features, you must enter a key code using the provided license.

Go to Admin Settings > General Settings > Options to enter the key code.

Enable the following options on the primary system:

- **Telepresence Interoperability Protocol (TIP).** This option provides the best possible telepresence experience when interoperating with Cisco TelePresence® rooms equipment.

- **Skype for Business Interoperability License.** This option enhances the video experience by enabling the use of the Microsoft RTV video codec, which provides higher resolutions during video calls when integrated with Microsoft Lync Server.
  
  - Centralized Conferencing Control Protocol (CCCP) enables seamless participation in multipoint video conferences hosted on Lync's audio/video server.
  
  - IPv6 is supported in Lync 2013, Skype for Business Server 2015, and Skype for Business 2015 client environments with IPv6 networks.

  For information about integrating with Microsoft Lync Server, refer to the Polycom Unified Communications Deployment Guide for Microsoft Environments.
Configuring the Admin Settings

- **Advanced Video 1080p License.** This option makes 1080p video and content available to RealPresence Immersive Telepresence systems.
- **RealPresence Immersive Studio.** This option identifies the Polycom video conferencing system that you are using.

Software Updates

You can update your Polycom RealPresence Immersive Studio system by going to support.polycom.com, navigating to **Documents and Downloads > Telepresence and Video**, and then downloading and installing the appropriate software.

You can also have your system automatically check for and apply software updates. If your organization uses a management system for provisioning endpoints, your Polycom RealPresence Immersive Studio system might get software updates automatically.

Installing Software Updates

To install software updates:

1. Go to **Admin Settings > General Settings > Software Updates > Software Server.**
2. Enter the address of the server on which the software is loaded.
3. Select **Check for Software Updates.**
4. When an available update is displayed, select **Start Update.**

Installing Software Updates Manually

To install software updates manually:

1. Go to **Admin Settings > General Settings > Software Updates > Manual Software Updates.**
2. Browse to locate the software update package on your PC and select **Start Transfer** to download it to the Group Series codec and start the update.
3. Repeat steps 1 and 2 for the left and right Group Series codecs.

Installing Software with Automatic Updates

To configure the system to check for software updates:

1. Go to **Admin Settings > General Settings > Software Updates > Automatic Software Updates.**
2. Select **Automatically Check for and Apply Software Updates.**
3. Accept the license agreement.
4. In the **Start Time** field, specify the hour, minute, and AM/PM settings to start checking for updates.
5. In the **Duration** field, specify how long the system should wait to determine whether updates are available

Refer to the **Polycom RealPresence Immersive Telepresence (ITP) Release Notes** information about the latest software version, including version dependencies.
Networks

Before you begin configuring the network options, you must make sure your network is ready for video conferencing.

Polycom also offers contract high-definition readiness services. For more information, contact your Polycom distributor.

LAN Status Lights

The LAN connector on the RealPresence Group systems has two lights to indicate connection status and traffic.

### LAN Status Lights

<table>
<thead>
<tr>
<th>Indicator Light</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left light off</td>
<td>No 1000Base-T connection.</td>
</tr>
<tr>
<td>Left light green</td>
<td>1000Base-T connection.</td>
</tr>
<tr>
<td>Right light off</td>
<td>No 10/100 Base-T connection and no network traffic with 1000 Base-T connection.</td>
</tr>
<tr>
<td>Right light on</td>
<td>10/100 Base-T connection and blinks with network traffic.</td>
</tr>
<tr>
<td>Right light blinking</td>
<td>Network traffic.</td>
</tr>
</tbody>
</table>

LAN Properties

You can configure LAN properties for the RealPresence Immersive Studio. LAN properties are controlled individually by the three systems that are part of the RealPresence Immersive Studio setup. You must configure each system individually.

**To configure RealPresence Immersive Studio LAN properties:**

1. In the primary codec web UI, go to Admin Settings > Network > LAN Properties.
2. Configure the following IP Address (IPv4) settings on the LAN Properties screen. A static IPv4 address is required for each codec.

### IP Address (IPv4) Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
3 The DNS Server address fields are populated automatically when the IPv4 Address is automatically obtained. If the IPv4 address is not obtained automatically, enter the DNS Server addresses.

4 Configure the following **LAN Options** settings.

### LAN Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Name</strong></td>
<td>Indicates the system’s DNS name.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Displays the domain name currently assigned to the system. If the system does not automatically obtain a domain name, enter one here.</td>
</tr>
<tr>
<td><strong>Autonegotiation</strong></td>
<td>Specifies whether the network switch should automatically negotiate the LAN speed and duplex mode. If this setting is enabled, the <strong>LAN Speed</strong> and <strong>Duplex Mode</strong> settings become read only. Polycom and IEEE802.3 recommend 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 that you choose.</td>
</tr>
<tr>
<td><strong>Duplex Mode</strong></td>
<td>Specifies the duplex mode to use. Note that the switch must support the Duplex mode that you choose.</td>
</tr>
<tr>
<td><strong>Ignore Redirect Messages</strong></td>
<td>Enables the RealPresence Group system to ignore redirect messages from network routers. A redirect message tells the endpoint to use a different router than the one it is using.</td>
</tr>
<tr>
<td><strong>ICMP Transmission Rate Limit (millisecond)</strong></td>
<td>Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 signifies that the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled. This setting applies only to ”error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies.</td>
</tr>
<tr>
<td><strong>Generate Destination Unreachable Messages</strong></td>
<td>Generates a Destination Unreachable message if a packet cannot be delivered to its destination for reasons other than network congestion.</td>
</tr>
<tr>
<td><strong>Respond to Broadcast and Multicast Echo Requests</strong></td>
<td>Sends an Echo Reply message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the RealPresence Group system.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

Configuring the IP Addresses of the Component Codecs

The following procedures describe how to change the IP addresses of the main and secondary codecs while they are not in Immersive mode. To take the system out of immersive mode, go to the Immersive page in the primary codec web UI and change this system from Primary to Standalone.

Changing the IP Address of the Primary Codec

To change the IP address of the primary codec:

1. In the primary codec web UI, go to Admin Settings > Network > LAN Properties for the primary codec.
2. In the IP Address (IPv4) section, in the IP Address field, specify how the system obtains an IP address.
   - Obtain IP Address Automatically—Select this option if the system gets an IP address from the DHCP server on the LAN.
   - Enter IP Address Manually—Select this option if the IP address will not be assigned automatically.
     1. For the manual IP address option, enter the new information in the Your IP Address is, Default Gateway, and Subnet Mask fields.
     2. Save the changes.

After you changed the IP address of the primary codec, the secondary codecs might start the reboot cycle because they have lost connection with the primary codec. In addition, the primary display shows black video.

3. Go to Admin Settings > Immersive.
4. In the Left Static IP Address and Right Static IP Address fields, enter the updated IP addresses for the left and right secondary codecs respectively.

### LAN Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 DAD Transmit Count</td>
<td>Specifies the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The RealPresence Immersive Studio 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.</td>
</tr>
<tr>
<td>Enable PC LAN Port</td>
<td>The setting appears only for the RealPresence Immersive Studio main system. Specifies whether the PC LAN port is enabled on the back of the system. Disable this setting for increased security.</td>
</tr>
<tr>
<td>Enable EAP/802.1X</td>
<td>Specifies whether EAP/802.1X network access is enabled. RealPresence Group systems support the following authentication protocols:</td>
</tr>
<tr>
<td></td>
<td>• EAP-MD5</td>
</tr>
<tr>
<td></td>
<td>• EAP-PEAPv0 (MSCHAPv2)</td>
</tr>
<tr>
<td></td>
<td>• EAP-TTLS</td>
</tr>
<tr>
<td></td>
<td>• EAP-TLS</td>
</tr>
<tr>
<td>Enable 802.1p/Q</td>
<td>Specifies whether VLAN and link layer priorities are enabled.</td>
</tr>
</tbody>
</table>
5 Enter **Admin ID** and **Password** credentials if you use them.

6 Select **Connect**. All codecs reboot.

### Changing the IP Address of the Secondary Codec

**To change the IP address of a secondary codec:**

1. In the secondary codec web UI, go to **Admin Settings > Network > LAN Properties** for the secondary codec.

2. In the **IP Address (IPv4)** section, in the **IP Address** field, specify how the system obtains an IP address.
   - **Obtain IP Address Automatically**—Select this option if the system gets an IP address from the DHCP server on the LAN.
   - **Enter IP Address Manually**—Select this option if the IP address will not be assigned automatically.
     1. For the manual IP address option, enter the new information in the **Your IP Address is**, **Default Gateway**, and **Subnet Mask** fields.
     2. Save the changes.

     After you change the IP address of the secondary codec, the codec might start the reboot cycle because it has lost the SSH connection to the primary codec. In addition, the main display shows black video.

3. Go to **Admin Settings > Immersive** for the primary codec.

4. Select the **RealPresence Immersive Studio** or **RealPresence OTX Studio** for the **System Type**.

5. In the **Left Static IP Address** or **Right Static IP Address** field, enter the updated IP address for the applicable secondary codec.

6. Enter **Admin ID** and **Password** credentials if you use them.

7. Select **Connect**. All codecs reboot.

8. As needed, repeat steps 1 through 7 for the remaining secondary codec.

### IP Network Settings

You can configure IP network settings by going to **Admin Settings > Network > IP Network**.

### Network Quality Setting

Use this group of settings to specify how your RealPresence Immersive Studio responds to quality issues.
Configuring the Admin Settings

H.323 Settings

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

To configure H.323 settings, in the web interface go to Admin Settings > Network > IP Network > SIP.

H.323 Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP H.323</td>
<td>Enables 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 <strong>H.323 Name</strong> is the same as the <strong>System Name</strong>, and is automatically generated in the same way.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

SIP Settings

If your network supports the Session Initiation Protocol (SIP), you can use SIP to connect IP calls. The SIP protocol has been widely adapted for voice over IP communications and basic video conferencing; however, many of the advanced 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.

To specify SIP Settings:

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

H.323 Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 Extension (E.164) (for Left, Main, and Right Codecs)</td>
<td>Enables users to 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.</td>
</tr>
<tr>
<td>Use Gatekeeper</td>
<td>Select this setting to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN.</td>
</tr>
<tr>
<td>• Off—Calls do not use a gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>• Auto—System attempts to automatically find an available gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>▲ Current Gatekeeper IP Address—Displays the IP address that the gatekeeper is currently using.</td>
<td></td>
</tr>
<tr>
<td>▲ Primary Gatekeeper IP Address—Displays the gatekeeper’s IP address. The primary gatekeeper IP address contains the IPv4 address with which the system registers. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the RealPresence Group System registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the RealPresence Group System unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>• Specify—Calls use the specified gatekeeper. This option must be selected to enable H.235 Annex D Authentication.</td>
<td></td>
</tr>
<tr>
<td>▲ Require Authentication—Enables support for H.235 Annex D Authentication. When H.235 Annex D Authentication is enabled, the H.323 gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>User Name—When authentication is enabled, specifies the user name for authentication with H.235 Annex D.</td>
<td></td>
</tr>
<tr>
<td>Enter Password—When authentication is enabled, specifies the password for authentication with H.235 Annex D.</td>
<td></td>
</tr>
</tbody>
</table>
## SIP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Enables the SIP settings to be displayed and configured.</td>
</tr>
<tr>
<td>Enable AS-SIP</td>
<td>Not supported.</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>, the Transport Protocol, Registrar Server, and Proxy Server settings cannot be edited. If you select <strong>Specify</strong>, those settings are editable.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Indicates the protocol the system uses for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>The SIP network infrastructure within which your RealPresence Immersive Studio operates determines which protocol is required. <strong>Auto</strong> enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. <strong>TCP</strong> provides reliable transport via TCP for SIP signaling. <strong>UDP</strong> provides best-effort transport via UDP for SIP signaling. <strong>TLS</strong> provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.</td>
</tr>
<tr>
<td>Sign-in Address (for Left, Main, and Right Codecs)</td>
<td>Specifies the SIP address or SIP name of the system, for example, <a href="mailto:vineyarditp3@abc.com">vineyarditp3@abc.com</a>. If you leave this field blank, the system’s IP address is used for authentication. Refer to <strong>SIP Address Naming Convention</strong> for details on the recommended naming convention for SIP addresses.</td>
</tr>
<tr>
<td>User Name (for Left, Main, and Right Codecs)</td>
<td>Specifies the name to use for authentication when registering with a SIP Registrar Server, for example, <a href="mailto:msmith@company.com">msmith@company.com</a>. If the SIP proxy requires authentication, this field and the password cannot be blank.</td>
</tr>
<tr>
<td>Password (for Left, Main, and Right Codecs)</td>
<td>Specifies the password that authenticates the system to the Registrar Server.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

**SIP Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar Server</td>
<td>Specifies the IP address or DNS name of the SIP Registrar Server.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specifies the DNS name or IP address of the SIP Proxy Server.</td>
</tr>
</tbody>
</table>

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

**SIP Address Naming Convention**

Polycom recommends using the following naming conventions for SIP addresses, but it is not required. The advantage of using this naming convention is that a Polycom Immersive endpoint (RPX, OTX, ATX, Immersive Studio, OTX Studio) can dial a call using a single SIP address such as vineyarditp3@abc.com and it will automatically dial the other addresses, ~vineyard2@abc.com and ~vineyard3@abc.com. This naming convention can be used for deployment with any type of SIP infrastructure.

**SIP Address Naming Convention**

<table>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main codec</td>
<td>&lt;name&gt;itp&lt;number_of_codecs&gt;@&lt;domain&gt;</td>
<td><a href="mailto:vineyarditp3@abc.com">vineyarditp3@abc.com</a></td>
</tr>
<tr>
<td>Right codec</td>
<td>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyard2@abc.com">vineyard2@abc.com</a></td>
</tr>
<tr>
<td>Left codec</td>
<td>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyard3@abc.com">vineyard3@abc.com</a></td>
</tr>
</tbody>
</table>
Configuring SIP Settings for Integration with Microsoft Servers

Because Polycom RealPresence Immersive Studio systems run in dynamic management mode, they cannot be simultaneously registered with Lync Server and the presence service provided by the Polycom RealPresence Resource Manager system.

RealPresence Immersive Studio systems can obtain presence services from only one source: Lync Server, or the presence service provided by the RealPresence Resource Manager system. Polycom supports the following features in Microsoft Lync Server 2013 and Skype for Business Server 2015:

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

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

If your organization deploys multiple Lync Server pools, a Polycom RealPresence Immersive Studio system must be registered to the same pool to which the system's user account is assigned.

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

When SIP is enabled on a RealPresence Immersive Studio system that has the TIP option, the system can interoperate with TIP endpoints. Note that the Immersive Studio and OTX Studio systems do not support a TIP call to other Polycom equipment, whether an end point or RMX.SIP (TIP) calls must connect at a call speed of 1 Mbps per screen or higher.

- Only TIP version 7 is supported.
- In a TIP call, only XGA content at 5 fps is supported. The following content sources are not supported in TIP calls:
  - USB content from the Polycom Touch Control
  - People+Content™ IP

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

RTV and Lync-Hosted Conference Support

To use RTV in a Lync-hosted conference, you must have the RTV option key enabled on your RealPresence Immersive Studio system.

For more information about configuring your Lync Server video settings for RTV, refer to the Polycom Unified Communications Deployment Guide for Microsoft Environments.

Specifying Quality of Service

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

Lost Packet Recovery and Dynamic Bandwidth

You can handle video quality issues by selecting the Enable Lost Packet Recovery (LPR) setting, the Dynamic Bandwidth setting, or both settings.

Polycom, Inc.
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.

To configure quality of service settings:

1. Go to Admin Settings > Network > IP Network > Network Quality.
2. Configure these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Service</strong></td>
<td>Specifies your service type and lets you choose how to set the priority of IP packets sent to the system for video, audio, and far-end camera control:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Precedence</strong>—Represents the priority of IP packets sent to the system. The value can be between 0 and 5.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DiffServ</strong>—Represents a priority level between 0 and 63.</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>Specifies the IP Precedence or Diffserv value for video RTP traffic and associated RTCP traffic.</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>Specifies the IP Precedence or Diffserv value for audio RTP traffic and associated RTCP traffic.</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Specifies the IP Precedence or Diffserv value for control traffic on any of the following channels:</td>
</tr>
<tr>
<td></td>
<td>• H.323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control</td>
</tr>
<tr>
<td></td>
<td>• SIP—SIP Signaling, Far End Camera Control, Binary Floor Control Protocol (BFCP)</td>
</tr>
<tr>
<td><strong>OA&amp;M</strong></td>
<td>Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC.</td>
</tr>
<tr>
<td><strong>Maximum Transmission Unit Size</strong></td>
<td>Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or select a maximize size.</td>
</tr>
<tr>
<td><strong>Maximum Transmission Unit Size Bytes</strong></td>
<td>Specifies the MTU size, in bytes, used in IP calls. If the video becomes blocky or network errors occur, packets might be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets might be too small; increase the MTU.</td>
</tr>
<tr>
<td><strong>Enable Lost Packet Recovery</strong></td>
<td>Enables the system to use LPR (Lost Packet Recovery) if packet loss occurs.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

Configuring Dialing Preferences

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

SVC-Based Conferencing

SVC-based conferences are not supported in this release of the RealPresence Immersive Studio system.

To specify dialing preferences:

1. Go to Admin Settings > Network > Dialing Preference.
2. Configure these settings.

Dialing Options and Preferred Speeds

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalable Video Coding Preference</td>
<td>AVC Only is supported in this release.</td>
</tr>
<tr>
<td>Enable H.239</td>
<td>Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far sites you will call.</td>
</tr>
<tr>
<td>Call Type Order</td>
<td>The default value is Video.</td>
</tr>
<tr>
<td>Video Dialing Order</td>
<td>Specifies how the system places video calls to directory entries that have more than one type of number. It also specifies how the system places video calls when the call type selection is either unavailable or set to Auto. If a call attempt does not connect, the system tries to place the call using the next call type in the list.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

Audio/Video Settings

Avoid changing the following settings unless advised by Polycom Technical Support.

Monitors

Do not change the default settings for the monitors.

Sleep

You can specify the period of inactivity before the system goes to sleep.

To configure when the system goes to sleep:

1. In the primary codec web UI, go to Admin Settings > Audio/Video > Sleep.
2. In the Display field, select Black.
3. In the Time before system goes to sleep field, select an option:
   - Off—The system will not go to sleep after a period of inactivity.
   - An idle period.
4. To mute the microphone while in sleep mode, enable the check box next to Enable Mic Mute in Sleep Mode.
5. Go to Admin Settings > Audio/Video > Sleep. If the Display field does not indicate No Signal, select No Signal from the drop down menu. Click Save.

Using Sleep Settings to Prevent Monitor Burn-In

Monitors used with Polycom RealPresence Immersive Studio systems provide display settings to help prevent image burn-in. 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:
  - 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.

Dialing Options and Preferred Speeds

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Speed for Placed Calls: IP Calls</td>
<td>Determines the speed to use for calls from this system.</td>
</tr>
<tr>
<td></td>
<td>If the far-site system does not support the selected speed, the system</td>
</tr>
<tr>
<td></td>
<td>automatically negotiates a lower speed.</td>
</tr>
<tr>
<td>Maximum Speed for Received Calls: IP Calls</td>
<td>Enables you to restrict the bandwidth used when receiving IP calls.</td>
</tr>
<tr>
<td></td>
<td>If the far site attempts to call the system at a higher speed than selected</td>
</tr>
<tr>
<td></td>
<td>here, the call is renegotiated at the speed specified in this field.</td>
</tr>
</tbody>
</table>

Polycom, Inc.
Video Inputs

To configure video input settings:

1. Go to Admin Settings > Audio/Video > Video Inputs.
   Note the three tabs, labeled Left, Main, and Right, that control video input details for the left, main, and right systems.

2. If necessary, select a Power Frequency setting. The Power Frequency setting specifies the power line frequency for your system.
   In most cases, the system defaults to the correct power line frequency, based on the video standard used in the country where the system is located. This setting enables you to adapt the system in areas where the power line frequency does not match the video standard used. You might need to change this setting to avoid flicker from the fluorescent lights in your conference room.

Audio

Avoid changing the following settings unless advised by Polycom Technical Support.

To configure the audio settings:

1. Go to Admin Settings > Audio/Video > Audio.
2. Configure the following settings.

General Audio Settings

<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 ring tone and user alert tones.</td>
</tr>
<tr>
<td>Ringtone</td>
<td>Specifies the ring tone used for incoming calls.</td>
</tr>
<tr>
<td>User Alert Tones</td>
<td>Specifies the tone used for user alerts.</td>
</tr>
<tr>
<td>Mute Auto Answer Calls</td>
<td>Specifies whether to mute incoming calls.</td>
</tr>
<tr>
<td></td>
<td>Incoming calls are muted by default until you press the mute button on the</td>
</tr>
<tr>
<td></td>
<td>microphone or on the remote control.</td>
</tr>
<tr>
<td>Transmission Audio Gain (dB)</td>
<td>Specifies the audio level, in decibels, at which to transmit sound.</td>
</tr>
<tr>
<td></td>
<td>Unless otherwise advised, Polycom suggests setting this value to 0 dB.</td>
</tr>
</tbody>
</table>

Audio Input Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the type of input for connected components.</td>
</tr>
<tr>
<td>Audio Input Level</td>
<td>Sets the audio input level for each connection.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

3.5mm Audio Input Selection (RealPresence OTX Studio Only)

You can enable 3.5mm audio input from the RealPresence Group Series 3.5mm audio port using the RealPresence OTX Studio web interface. 3.5mm audio input is only active under the following conditions.

- The RealPresence Group system is in an active call.
- Content sharing is active.
- HDMI or VGA video input is active.

When audio is part of active HDMI or VGA content, the 3.5mm audio input mixes in with the HDMI or VGA audio input.

Enabling 3.5mm Audio Input for Content Sharing (RealPresence OTX Studio Only)

You can enable audio input for content sharing on a RealPresence OTX Studio system.

To enable 3.5mm audio input for content sharing:

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

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

Security Settings

The security profile your RealPresence Immersive Studio system uses provides the basis for secure access within the system and determines how users can operate the system.

Security Profiles

This release of the RealPresence Immersive Studio system supports the Low security profile. You can customize some of the settings within this security profile as needed.

To view the security profile:

2. Select the Low (default) security profile.

The Low security profile configures the system with no mandated security controls, although you can enable all controls as needed.
3. Select **Next**.
4. Follow the prompts in the **Security Profile Change** wizard.

### Global Security

#### External Authentication

RealPresence Immersive Studio systems support two roles for accessing the system, an admin role and a user role. Admins can perform administrator activities such as changing configuration, as well as user activities such as placing and answering calls. Users can perform only user-type activities.

The systems provide two local accounts, one for the user role (by default named *user*) and one for the admin role (by default named *admin*). The IDs and passwords for these local accounts are stored on the RealPresence Immersive Studio system itself.

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

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

When External Authentication is enabled in PKI environments where Always Validate Peer Certificates from Server is enabled on the RealPresence Immersive Studio system, make sure to configure the Active Directory Server Address on the RealPresence Immersive Studio endpoint using the address information that is in the Active Directory Server’s identity certificate. This is important in enabling the RealPresence Immersive Studio system to successfully validate the Active Directory Server’s identity certificate.

As an example, if the Active Directory Server’s identity certificate contains its DNS name only, and no specific IP address, configuring the Active Directory Server Address on the RealPresence Immersive Studio system using the server’s IP address will result in certificate validation failure, and consequently authentication failure. The RealPresence Immersive Studio system configuration would have to specify the server by DNS name in this case to successfully match the server certificate data.


**Note:**
The RealPresence Immersive Studio system local user account is disabled when **Enable Active Directory External Authentication** is enabled. The admin account is active and usable.

### To enable external authentication:

1. Go to **Admin Settings > Security > Global Security > Authentication**.
2. Configure these settings.
Configuring the Admin Settings

Access Settings in this section enable you to configure remote usage of the RealPresence Immersive Studio system, such as by using the web, a serial port, or Telnet. A session is an instance of a user connected to the system through one of these interfaces. Sessions include an indication of how you are logged on to the RealPresence Immersive Studio system, such as the local interface, web interface, Telnet, or serial API.

To configure access settings:

2. Configure the following settings. Your security profile might affect the availability of some settings.

### Authentication Settings

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

**Note:** 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.

Access

Settings in this section enable you to configure remote usage of the RealPresence Immersive Studio system, such as by using the web, a serial port, or Telnet. A session is an instance of a user connected to the system through one of these interfaces. Sessions include an indication of how you are logged on to the RealPresence Immersive Studio system, such as the local interface, web interface, Telnet, or serial API.
### Access Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Network Intrusion Detection System (NIDS)</td>
<td>Activates the ability to log entries to the security log when the system detects a possible network intrusion. This setting is enabled or disabled by default based on the security profile, but can be changed.</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Specifies whether to allow remote access to the system by using the web interface.</td>
</tr>
<tr>
<td>Allow Access to User Settings</td>
<td>Specifies whether the User Settings screen is accessible to users through the local interface.</td>
</tr>
<tr>
<td>Restrict to HTTPS</td>
<td>Specifies that the web server is accessible only over a secure HTTPS port. Enabling this setting closes the HTTP port and so disables redirects of sessions from HTTP to HTTPS (all access must be initiated as HTTPS).</td>
</tr>
<tr>
<td>Web Access Port (HTTP)</td>
<td>Specifies the port to use when accessing the system using the Polycom RealPresence Immersive Studio system web interface using HTTP.</td>
</tr>
<tr>
<td></td>
<td>If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the Polycom RealPresence Immersive Studio system web interface to access the system. This makes unauthorized access more difficult.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Restrict to HTTPS</strong> is enabled, the <strong>Web Access Port</strong> setting is unavailable.</td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>Specifies whether to allow remote access to the system by Telnet.</td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>Not supported. Do not enable SNMP.</td>
</tr>
<tr>
<td>API Port</td>
<td>Specifies the port for API access. Select port 23 or 24.</td>
</tr>
<tr>
<td></td>
<td>If you set the API port to port 23, the diagnostics port changes to port 24.</td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>For information about this setting, refer to <a href="#">Account Lockout</a>.</td>
</tr>
<tr>
<td>Enable SSH Access</td>
<td>Specifies whether to allow SSH access.</td>
</tr>
<tr>
<td>Enable Diagnostics Port Idle Session Timeout</td>
<td>Specifies whether to allow the diagnostics port to time out at the configured time interval or not. The timeout setting is set under Idle <strong>Session Timeout</strong> in <strong>Minutes</strong>.</td>
</tr>
<tr>
<td>Enable API Port Idle Session Timeout</td>
<td>Specifies whether to allow the API port to time out at the configured time interval or not. The timeout setting is set under Idle <strong>Session Timeout</strong> in <strong>Minutes</strong>.</td>
</tr>
<tr>
<td>Enable Whitelist</td>
<td>Specifies whether the system web interface ports accept connections only from specified IP addresses.</td>
</tr>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>Specifies the number of minutes your web interface session can be idle before the session times out.</td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>Specifies the maximum number of users who can be logged in to and using your system through Telnet or the web interface at the same time.</td>
</tr>
</tbody>
</table>
Encryption Settings

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

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

RealPresence Immersive Studio systems provide the following AES cryptographic algorithms to ensure flexibility when negotiating secure media transport:

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

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

To enable encryption:

2. Configure these settings.
Configuring the Admin Settings

Encryption Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Require AES Encryption for Calls AES Encryption in local interface | Specifies how to encrypt calls with other sites that support AES encryption.  
  - **Off**—AES Encryption is disabled.  
  - **When Available**—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call do not support it.  
  - **Required for Video Calls Only**—AES Encryption is used for all video endpoints in the call. Video endpoints must support AES Encryption to participate in the call.  
  - **Required for All Calls**—AES Encryption is used for all video endpoints in the call. All endpoints must support AES Encryption to participate in the call. |
| Require FIPS 140 Cryptography | Enables the exclusive use of the FIPS 140-2-validated software cryptography module for cryptographic functions. Also disables all "weak" protocols and ciphers, including:  
  - SSLv2  
  - SSLv3  
  - Non-FIPS 140-2 approved TLS cipher suites |

Local Account Settings

Account Lockout

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

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

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

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

- Local interface
- Web interface
- Telnet interface
To configure the account lockout feature:

1. Go to **Admin Settings > Security > Local Accounts > Account Lockout**.
2. Configure these settings for the appropriate account on the Account Lockout page. You can configure account lock for the admin account, user account, or both accounts.

### Account Lockout Settings

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

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

A RealPresence Immersive Studio system web interface is configured with these settings:

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

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

A user fails to log in to the **Admin** account three times on the web interface. 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 three times on the web interface. 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 three times on the web interface. 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.

### Login and Credentials

To configure local access to the system:

1. Go to **Admin Settings > Security > Local Accounts > Login Credentials**.
2 Configure the following settings for each system in your RealPresence Immersive Studio setup.

### Login Credentials

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin ID</strong></td>
<td>Specifies the ID for the administrator account. The default Admin ID is <code>admin</code>. Admin IDs are not case sensitive.</td>
</tr>
<tr>
<td><strong>Admin Room Password</strong></td>
<td>Specifies the password for the local administrator account used when logging in to the system locally.</td>
</tr>
<tr>
<td></td>
<td>When this password is set, you must enter it to configure the system Admin Settings using the remote control. The password cannot contain spaces or more than 40 characters. Passwords are case sensitive. The default Admin Room Password is the 14-digit system serial number from the System Information screen or the back of the system.</td>
</tr>
<tr>
<td><strong>Use Room Password for Remote Access</strong></td>
<td>Specifies whether the room password used for local login is also used for the remote login. When this setting is disabled, the remote access password settings are displayed.</td>
</tr>
<tr>
<td><strong>Admin Remote Access Password</strong></td>
<td>Specifies the password for the local administrator account used when logging in to the system remotely using the web interface or a telnet session. When this password is set, you must enter it to update the software or manage the system from a computer. The password cannot contain spaces or more than 40 characters.</td>
</tr>
<tr>
<td><strong>Require User Login for System Access</strong></td>
<td>Not Supported</td>
</tr>
<tr>
<td><strong>User ID</strong></td>
<td>Not Supported</td>
</tr>
<tr>
<td><strong>User Room Password</strong></td>
<td>Not Supported</td>
</tr>
<tr>
<td><strong>User Remote Access Password</strong></td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

### Password Requirements

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

**To configure password requirements:**

1. Go to Admin Settings > Security > Local Accounts > Password Requirements.
2. Configure the following settings.
Configuring the Admin Settings

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

### Managing Certificates and Revocation

If your organization has deployed a public key infrastructure (PKI) for securing connections between devices on your network, Polycom recommends that you have a strong understanding of certificate management and how it applies to Polycom RealPresence Immersive Studio before you integrate this system with the PKI.
The RealPresence Immersive Studio system can use certificates to authenticate network connections to and from the Polycom RealPresence Immersive Studio system. Other web applications also use certificates, as you might notice when you navigate the Internet. The system uses configuration and management techniques typical of PKI to manage certificates, certificate signing requests, and revocation checking. ANSI X.509 standards regulate the characteristics of certificates and revocation.

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

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

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

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

**Generating Certificate Signing Requests (CSRs)**

The RealPresence Immersive Studio system enables you to install one client and one server certificate for identification of the RealPresence Immersive Studio system to network peers. In order to obtain these certificates you must first generate a Certificate Signing Request (CSR) for each certificate. This request, also known as an unsigned certificate, must be submitted to a CA so that it can be signed, after which the certificate can be installed on the RealPresence Immersive Studio system. Whether you need to generate a client-type CSR, a server-type CSR, or both depends on which features and services you intend to use, and whether your network environment supports certificate-based authentication for those services. In most cases, both certificates are needed.

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

- RealPresence Resource Manager system Provisioning
- RealPresence Resource Manager system Monitoring
- RealPresence Resource Manager system LDAP Directory
- RealPresence Resource Manager system Presence
- Calendaring
- SIP
- 802.1X
The RealPresence Immersive Studio system web server uses the server-type CSR and resulting certificate whenever an administrator attempts to connect to the RealPresence Immersive Studio 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 enabling the browser to connect to the system. The browser’s user needs the server certificate if he or she wants to be certain about the identity of the RealPresence Immersive Studio system he or she is connecting to. Settings in the web browser typically control the validation of the server certificate, but you can also validate the certificate manually.

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

**Only a single outstanding CSR of either type can exist at a time.**

After the CSR is generated, it is important to get it signed and installed before attempting to generate a different CSR of the same type.

For example, if you generate a client CSR and then, prior to having it signed and installed on the RealPresence Immersive Studio system, another client CSR is generated, the previous CSR is discarded and invalidated, and any attempt to install a signed version of it will result in an error.

**To create a CSR:**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Algorithm</td>
<td>Specifies the hash algorithm for the CSR. You may select SHA-256 or keep the default SHA-1.</td>
</tr>
</tbody>
</table>
| Common Name (CN)         | Specifies the name that the system assigns to the CSR. Polycom recommends the following guidelines for configuring the Common Name:  
  • For systems registered in DNS, use the Fully Qualified Domain Name (FQDN) of the system.  
  • For systems not registered in DNS, use the IP address of the system. |
| Organizational Unit (OU) | Specifies the unit of business defined by your organization. If you want the signed certificate to include more than one OU field, download and edit the CSR manually. |
| Organization (O)         | Specifies your organization's name.                                         |
| City or Locality (L)     | Specifies the city where your organization is located.                      |
| State or Province (ST)   | Specifies the state or province where your organization is located.         |
| Country (C)              | Displays the country selected in **Admin Settings > General Settings > My Information**. |
Configuring the Admin Settings

After you create the CSR, the system displays a message indicating that the CSR has been created. 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.

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

To add a signed certificate on the Certificates page:

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

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

Security certificate error message

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

Configuring Certificate Validation Settings

Certificates are authorized externally when they are signed by the CA. The certificates can be automatically validated when they are used to establish an authenticated network connection. To perform this validation, the RealPresence Immersive Studio system must have certificates installed for all CAs that are part of the trust chain. A trust chain is the hierarchy of CAs that have issued certificates from the device being authenticated, through the intermediate CAs that have issued certificates to the various CAs, leading back to a root CA, which is a known trusted CA. The following sections describe how to install and manage these certificates.
A certificate exchange is between a server and a client, both of which are peers. When a user is accessing the RealPresence Immersive Studio system web interface, the RealPresence Immersive Studio system is the server and the web browser is the client application. In other situations, such as when the RealPresence Immersive Studio system connects to LDAP directory services, the RealPresence Immersive Studio system is the client and the LDAP directory server is the server.

**To configure certificate usage:**

1. Go to **Admin Settings > Security > Certificates > Certificate Options**.
2. Configure these settings on the Certificates screen and click **Save**.

### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Peer Certificate Chain Depth</strong></td>
<td>Specifies how many links a certificate chain can have. The term <em>peer certificate</em> refers to any certificate sent by the far-end host to the RealPresence Immersive Studio system when a network connection is being established between the two systems.</td>
</tr>
<tr>
<td><strong>Always Validate Peer Certificates from Browser</strong></td>
<td>Not supported.</td>
</tr>
<tr>
<td><strong>Always Validate Peer Certificates from Server</strong></td>
<td>Controls whether the RealPresence Immersive Studio system requires the remote server to present a valid certificate when connecting to it for services such as those listed for client-type CSRs in Generating Certificate Signing Requests (CSRs) (provisioning, directory, SIP, and so forth).</td>
</tr>
</tbody>
</table>

**Configuring Certificate Revocation Settings**

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

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

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

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

**Using Certificate Revocation Lists**

**To use Certificate Revocation Lists (CRLs):**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Revocation Method</strong></td>
<td>Select the CRL method.</td>
</tr>
<tr>
<td>**Allow Incomplete</td>
<td>When this field is enabled, a certificate in the chain is verified without a revocation status check if no corresponding CRL for the issuing CA is installed. The RealPresence Immersive Studio system assumes that the lack of a CRL means the certificate is not revoked. If a CRL is installed, the system performs a revocation check when validating the certificate.</td>
</tr>
<tr>
<td><strong>Revocation Checks</strong></td>
<td></td>
</tr>
<tr>
<td>Add CRL</td>
<td>1 Click <strong>Browse</strong> to search for and select a CRL.</td>
</tr>
<tr>
<td></td>
<td>2 Click <strong>Open</strong> to add the CRL to the list.</td>
</tr>
</tbody>
</table>

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

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

If the Always Validate Peer Certificates from Browsers setting is enabled and the expired CRL is for a CA that is part of the trust chain for the client certificate sent by your browser, you will no longer be able to connect to the RealPresence Immersive Studio system web interface because the revocation check will always fail. In this case, unless the RealPresence Immersive Studio system web interface can be accessed by a user whose client certificate’s trust chain does not include the CA whose CRL is expired, you must delete all certificates and CRLS from the system and then reinstall them. See the *RealPresence Server Address Configuration in PKI-Enabled Environments* for more information.

**Using Online Certificate Status Protocol**

If you use OCSP, you might need to install one or more additional CA certificates on the RealPresence Immersive Studio system, for validation of the OCSP response messages.

**To use Online Certificate Status Protocol (OCSP):**

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

Certificates and Security Profiles within a Provisioned System

When your RealPresence Immersive Studio 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 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.

RealPresence Server Address Configuration in PKI-Enabled Environments

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

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

**Security Banners**

Security banners are not supported.

**Log Management**

The RealPresence Immersive Studio system log files comprise the following information:

- System logs
- Call Detail Report (CDR)
- Configuration profile

You can download logs by using the Polycom RealPresence Immersive Studio system web interface. The date and time of system log entries for RealPresence Immersive Studio systems are shown in GMT. When the log fills up past the threshold, the following actions are triggered:

- Transfers the log to the USB device if Transfer Frequency is set to “Auto at Threshold”
- Creates a log entry indicating that the threshold has been reached
- Displays an alert on the home screen
- Displays an indicator on the System Status screen

**Viewing the Log File Status**

**To view the log file status:**

1. Go to **Diagnostics > System > System Status**.
2. Select the More Info link for **Log Threshold** for each system in your RealPresence Immersive Studio setup.
   - When the Log Threshold system status indicator is red, automatic log transfers cannot be completed and data can be lost.

**Configuring Log Management**

**To configure log management:**

1. Go to **Admin Settings > Security > Log Management**.
2. Configure these settings.
Configuring the Admin Settings

Log Management Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Percent Filled</td>
<td>Displays how full the log file is as a percentage of the total size.</td>
</tr>
<tr>
<td>Percent Filled Threshold</td>
<td>Specifies a threshold for the percent filled value. Reaching the threshold triggers an alarm, creates a log entry, and transfers the log if Transfer Frequency is set to Auto at Threshold. Off disables logging threshold notifications.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Specifies the name to give the folder for log transfers. System Name and Timestamp — Folder name is the system name and the timestamp of the log transfer, in the date and time format specified on the Location screen. For example, if the system name is “Marketing”, the folder name could be marketing_MMddyyyyymmssSSS. Timestamp — Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example yyyyMMddhhmmssSSS. Custom — Optional folder name for manual log transfers.</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 logs are transferred: 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 being transferred, new events overwrite the oldest events. Auto at Threshold — The transfer starts automatically when the Percent Filled Threshold is reached.</td>
</tr>
</tbody>
</table>

System Log Files

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

To set up system logging, you need to perform the following tasks:

- Configuring System Log Management
- Configuring System Log Level and Remote Logging

After setting up system logging, you can retrieve a system log file. For details on how to get log files, refer to Retrieving Log Files.

Configuring System Log Management

When the system log fills up past the threshold, the following actions are triggered:

- Transfers the log to the USB device if Transfer Frequency is set to “Auto at Threshold”
- Creates a log entry indicating that the threshold has been reached
- Displays an alert on the home screen
- Displays an indicator on the System Status screen

To view the log file status, do one of the following:

- In the local interface, go to Settings > System Information > Status > Log Management.
Configuring the Admin Settings

- In the web interface, go to Diagnostics > System > System Status and select the More Info link for Log Threshold.

  Note: When the Log Threshold system status indicator is red, automatic log transfers cannot be completed and data may be lost. You must manually transfer the logs to a USB storage device.

To configure system log management:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Percent Filled</td>
<td>Displays how full the log file is, as a percentage of the total size.</td>
</tr>
<tr>
<td>Percent Filled Threshold</td>
<td>Specifies a threshold for the percent filled value. Reaching the threshold triggers an alarm, creates a log entry, and transfers the log if Transfer Frequency is set to Auto at Threshold. Off disables logging threshold notifications.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Specifies the name to give the folder 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, in the date and time format specified on the Location screen. For example, if the system name is “Marketing”, the folder name could be marketing_MMddyyyymmssSSS.</td>
</tr>
<tr>
<td></td>
<td>• Timestamp—Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example yyyyMMddhhmmssSSS.</td>
</tr>
<tr>
<td></td>
<td>• Custom—Elective 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 logs are transferred: Manual—The transfer starts when you click the Start Log Transfer button, which is visible only on the local interface. If the log fills before being transferred, new events overwrite the oldest events. Auto at Threshold—The transfer starts automatically when the Percent Filled Threshold is reached.</td>
</tr>
</tbody>
</table>

Configuring System Log Level and Remote Logging

The system log captures devices and server events in a consistent manner. You determine the log level, whether to enable remote logging, and whether to log additional SIP or H.323 details.

To configure system log settings:

1. In the web interface, go to Diagnostics > System > System Log Settings.
2. Configure these settings.
Retrieving Log Files

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

You might find log files useful when troubleshooting. You can generate log files for the RealPresence Immersive Studio or RealPresence OTX Studio system. This section explains how to retrieve those log files:

- Downloading System Log Files
Configuring the Admin Settings

- Transferring System Log Files

**Downloading System Log Files**

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

> **Note:** The date and time of system log entries for RealPresence Immersive Studio and RealPresence OTX Studio systems are shown in GMT.

**To download a system log in the web interface:**

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

**Transferring System Log Files**

You can transfer a RealPresence Immersive Studio or RealPresence OTX Studio system log in the local interface.

**To transfer a system log in the local interface:**

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

**Configuring Servers**

This section shows how to set up various servers in your RealPresence Immersive Studio or RealPresence OTX Studio system.

**Setting Up a Directory Server**

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

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

Directory Servers Supported in Standard Operating Mode

<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>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: • H.323 IP address (raw IPv4 address, DNS name, H.323 dialed digits, H.323 ID, or H.323 extension) • SIP address (SIP URI) • ISDN number • Phone number *</td>
</tr>
<tr>
<td>Microsoft Lync Server 2013 and 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:
  • +Country Code.Area Code.Number

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

Directory Servers Supported by Polycom RealPresence Resource Manager Provisioning

<table>
<thead>
<tr>
<th>Directory Servers Supported</th>
<th>Authentication Protocol</th>
<th>Global Directory Groups</th>
<th>Entry Calling Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP by a Polycom RealPresence Resource Manager system</td>
<td>NTLM v2 only</td>
<td>Pre-defined groups from the LDAP directory are shown in Polycom RealPresence Immersive Studio system's directory</td>
<td>Might include: • H.323 dialed digits, H.323 ID, or H.323 extension • Phone number * • SIP address</td>
</tr>
<tr>
<td>Microsoft Lync Server 2013 and Skype for Business Server 2015</td>
<td>NTLM v1 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:
  • +Country Code.Area Code.Number
Configuring the LDAP Directory Server

To configure the LDAP directory server:

1. Go to Admin Settings > Servers > Directory Servers and select the LDAP Server Type.
2. Configure these settings.

LDAP Server Settings

<table>
<thead>
<tr>
<th>LDAP Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>Specifies the address of the LDAP directory server. With Automatic Provisioning, this setting is configured by the server and appears as read only.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specifies the port used to connect to the LDAP server. With Automatic Provisioning, this setting is configured by the server and appears as read only.</td>
</tr>
<tr>
<td>Base DN (Distinguished Name)</td>
<td>Specifies the top level of the LDAP directory where searches will begin. With Automatic Provisioning, this setting is configured by the server and appears as read only.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the protocol used for authentication with the LDAP server: NTLM, BASIC, or Anonymous.</td>
</tr>
<tr>
<td>Use SSL (Secure Socket Layer)</td>
<td>Enables SSL for securing data flow to and from the LDAP server.</td>
</tr>
<tr>
<td>Bind DN (Distinguished Name)</td>
<td>The user ID of the person allowed to search the LDAP directory, which must be in a standard DN format such as cn=user,dc=example,dc=com.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name for authentication with the LDAP server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the user name for authentication with LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password for authentication with the LDAP server.</td>
</tr>
</tbody>
</table>

Microsoft Directory Server Settings

To configure the Microsoft Lync Server and Skype for Business Server directory settings:

1. Go to Admin Settings > Network > IP > SIP Settings.
2. Configure the SIP settings as described in SIP Settings.
3. Go to Admin Settings > Servers > Directory Servers and select Microsoft for the Server Type.
4. Configure these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Status</td>
<td>Specifies whether the system is successfully registered with the Microsoft Lync Server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the Domain Name entered on the SIP Settings screen.</td>
</tr>
</tbody>
</table>
Setting Up SNMP

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

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

SNMP features specific to version 3 include the following:

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

Downloading MIBs

In order to enable your SNMP management console application to resolve SNMP traps and display human readable text descriptions for those traps, you need to install Polycom MIBs (Management Information Base) on the computer you intend to use as your network management station. The MIBs are available for download from the Polycom RealPresence Immersive Studio system web interface.

To download MIBs:

1. Go to Admin Settings > Servers > SNMP.
2. Select the Download MIB link.

Configuring for SNMP Management

To configure the system for SNMP Management:

1. Go to Admin Settings > Servers > SNMP.
2 Configure these settings for each system in your RealPresence Immersive Studio setup.

### SNMP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Enables administrators to manage the system remotely using SNMP.</td>
</tr>
<tr>
<td>Version1</td>
<td>Enables the use of the SNMPv1 protocol.</td>
</tr>
<tr>
<td>Version2c</td>
<td>Enables the use of the SNMPv2c protocol.</td>
</tr>
<tr>
<td>Version3</td>
<td>Enables the use of the SNMPv3 protocol. You must select this setting to use the subsequent settings that apply only to SNMPv3.</td>
</tr>
<tr>
<td>Read-Only Community</td>
<td>Specifies the SNMP management community in which you want to enable this system. The default community is <code>public</code>. <strong>Note:</strong> Polycom does not support SNMP write operations for configuration and provisioning; the read-only community string is used for both read operations and outgoing SNMP traps.</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Specifies the name of the person responsible for remote management of this system.</td>
</tr>
<tr>
<td>Location Name</td>
<td>Specifies the location of the system.</td>
</tr>
<tr>
<td>System Description</td>
<td>Specifies the type of video conferencing device.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the SNMPv3 User Security Model (USM) account name that will be used 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>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 type of SNMPv3 cryptography privacy algorithm used:</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. This setting might be needed for matching the configuration of an SNMP console application. The Engine ID is automatically generated, but you can create your own ID between 10 and 32 hexadecimal digits. Each group of 2 hex digits can be separated by a colon character (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (therefore, <code>:F:</code> is equivalent to <code>:0f:</code>). The ID cannot be all zeros or all Fs.</td>
</tr>
<tr>
<td>Listening Port</td>
<td>Specifies the port number SNMP uses to listen for messages. The default listening port is 161.</td>
</tr>
</tbody>
</table>
Configuring the Admin Settings

Using a Provisioning Service

If your organization uses the Polycom RealPresence Resource Manager system, you can manage Polycom RealPresence Immersive Studio systems in dynamic management mode. In dynamic management mode, the following might be true:

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

### SNMP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transport Protocol       | Specifies the transport protocol used:  
  • TCP  
  • UDP |
| Destination Address1, 2, 3 | Specifies the IP addresses of the computers you intend to use as your network management station and to which SNMP traps will be sent.  
Each address row has four settings:  
  • IP Address—Accepts IPv4 and IPv6 addresses, host names, and FQDNs)  
  • Message Type—Trap, Inform  
  • SNMP protocol version—v1, v2c, v3  
  • Port—Default is 162  
Disabling the check box next to the Port setting disables the corresponding Destination Address. |
Enabling or Disabling the Provisioning Service
To register the Polycom RealPresence Immersive Studio system with the Polycom RealPresence Resource Manager system, enter the registration information and attempt to register by going to Admin Settings in the Polycom RealPresence Immersive Studio system web interface.

To enable a provisioning service:
1. Go to Admin Settings > Servers > Provisioning Service.
2. Select the Enable Provisioning setting.
3. Enter the Domain, User Name, Password, and Server Address for automatic provisioning.
   Multiple Polycom RealPresence Immersive Studio systems can be registered to a single user.
4. Select Register or Update. The system tries to register with the Polycom RealPresence Resource Manager system using NTLM authentication.

To disable a provisioning service:
1. Go to Admin Settings > Servers > Provisioning Service.
2. Disable the Enable Provisioning setting.

Provisioning Service Settings
If automatic provisioning is enabled but the system does not register successfully with the provisioning service, you might need to change the Domain, User Name, Password, or Server Address used for registration. For example, users might be required to periodically reset passwords used to log into the network from a computer. If such a network password is also used as the provisioning service password, you must update it on the Polycom RealPresence Immersive Studio system, too.

To avoid unintentionally locking a user out of network access in this case, RealPresence Immersive Studio systems will not automatically retry registration until you update the settings and register manually on the Provisioning Service page.

To configure the provisioning service settings:
1. Go to Admin Settings > Servers > Provisioning Service.
2. Configure these settings.

Provisioning Service Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specifies the domain for registering to the provisioning service.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the endpoint’s user name for registering to the provisioning service.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password that registers the system to the provisioning service.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specifies the address of the Polycom RealPresence Resource Manager system running the provisioning service.</td>
</tr>
</tbody>
</table>
Connecting to the Microsoft Exchange Server Calendaring Service

Polycom RealPresence Immersive Studio systems can connect to Microsoft Exchange Server 2010 or 2013 and retrieve calendar information. Connecting to a calendaring service enables the system to:

- Display the day’s scheduled meetings, along with details about each.
- Hide or show details about meetings marked Private, depending on the configuration of the system.
- Display a meeting reminder before each scheduled meeting, along with a reminder tone.

To configure Calendaring properties:

1. Go to **Admin Settings > Servers > Calendaring Service**.
2. Configure these settings.

Calendaring Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Calendaring Service</td>
<td>Enables the system to connect to the Microsoft Exchange Server 2010 or 2013 and retrieve calendar information.</td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td>Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access Server. If your organization has multiple Client Access Servers behind a network load balancer, this is the FQDN of the server’s Virtual IP Address. If required, an IP address can be used instead of an FQDN, but Polycom recommends using the same FQDN that is used for Outlook clients.</td>
</tr>
<tr>
<td>Secure Connection Protocol</td>
<td>Specifies the secure connection protocol.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specifies the domain for registering to the Microsoft Exchange Server 2010 or 2013, in either NETBIOS or DNS notation, for example, either company.local or COMPANY.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the user name for registering to the Microsoft Exchange Server 2010 or 2013, with no domain information included. This can be the system’s name or an individual's name.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the system's password for registering with the Microsoft Exchange Server 2010 or 2013.</td>
</tr>
<tr>
<td>Email</td>
<td>Specifies the Outlook mailbox this system should monitor for calendar information. This should match the Primary SMTP Address for the account in Microsoft Exchange Server 2010 or 2013, which is displayed as the value of the mail attribute in the account properties.</td>
</tr>
<tr>
<td>Meeting Reminder Time In Minutes</td>
<td>Specifies the number of minutes before a meeting to display a reminder.</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>
Setting Up the Distributed Media Service

By default, the RealPresence Immersive Studio system supports the Polycom RealPresence Distributed Media Application™ (DMA). RealPresence DMA enables multipoint conferences.

To set up the Distributed Media Service:

1. Go to the admin interface of RMX and configure DMA as the H323 gatekeeper and SIP server.
2. Login to the DMA web interface with a user account having Administrator privileges.
3. Configure MCU in DMA:
   a. In the DMA menu, go to Network > MCU > MCUs and press Add on the ACTIONS pane to add the details of the MCU (RMX) that you want to use for your conferencing needs.
   b. After filling in the details of the MCU (RMX), press OK. Make sure that the MCU state shows as "Connected to .. MCU" and "In service" as indicated by the status indicators in the first column of the table displayed in Network > MCU > MCUs.
4. Configure MCU pool:
   a. Go to Network > MCU > MCU Pools and press Add on the ACTIONS pane to add a MCU Pool.
   b. Name the pool and select the MCU that was added previously in step 3 and move it to the Selected MCUs section. Press OK.
5. Configure MCU pool order:
   a. Go to Network > MCU > MCU Pool Orders and press Add on the ACTIONS pane to add a MCU Pool order.
   b. Name the pool order and select the MCU pool that was added previously in step 4 and move it to the Selected MCU pools section. Press OK.
6. Configure the conference template:
   a. Go to Admin > Conference Manager > Conference Templates and press Add on the ACTIONS pane to add a conference template.
   b. Name the template and configure the rest of the settings as required. The resolution, video quality, line rate, etc that is applied to the conference depends on the configuration in the conference template.
7. Configure a DMA user:
   a. In the menu, go to User > Users and press Add on the ACTIONS pane to add a user.
   b. Configure the userid and password. You can also configure the class of service and bit rate. No special roles (Administrator/Auditor,Provisioner) are required for this DMA user.
8. Create a conference room:
   a. Select the user that you created in step 7 and press Manage conference rooms on the ACTIONS pane.
   The Conference Rooms window appears.
b Add a conference room by pressing Add.
The Add Conference Room window opens.

c Provide or generate a Room id (conference room number). Enable the conference template and select the conference template that was created in step 6.

d Enable MCU pool order and select the MCU pool order that was created in step 5.

9 Verify the above configuration:
Dial in to the conference room created above from the Immersive Studio or OTX Studio endpoint by dialing the dial-in number of the conference room. If this succeeds (codec should be able to enter the conference), then the configuration is correct.

Notes: Distributed Media Service
• These instructions do not cover all configuration items related to setting up a conference room in DMA. Refer to the DMA documentation for detailed instructions on setting up MCUs, pools, conference templates, etc.
• All the endpoints (conference initiator and conference participants) should be registered to DMA as H323 and/or SIP endpoints. This may not be required on the conference participants if you are using only an IP address to perform blast dialing.
• The DMA should have the RealPresence API license installed in it to use the meeting composer feature. This can be checked in Admin > Local Cluster > Licenses > Active License. If the Licensed capabilities field shows RealPresence Platform API, then the license is installed.

There should be a MLA registered to the RMX for applying the proper layouts.

Configuring the Distributed Media Service
To use the Meeting Composer functionality in RealPresence Immersive Studio or RealPresence OTX Studio, you must enable and configure Distributed Media Service.

To configure Distributed Media Service:

1 Login to the web UI of RealPresence Immersive Studio or RealPresence OTX Studio as admin.
2 Go to Admin Settings > Servers > Distributed Media Service.
3 Select the Enable Multipoint Server check box.
4 Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Meeting Room</td>
<td>Specifies the DMA conference room number/ID to use for conferencing activities, created in step 8.</td>
</tr>
<tr>
<td>(VMR) Number</td>
<td></td>
</tr>
<tr>
<td>Server Address</td>
<td>Specifies the DMA server that hosts the conference room/VMR.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specifies the domain of the DMA user who owns the conference room. It should be the same as the domain displayed in the DMA admin web interface in User &gt; Users in the room item for the user created in step 7.</td>
</tr>
</tbody>
</table>
Multipoint Server Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specifies the User ID of the DMA user, created in step 7, who owns the conference room. No special roles (Administrator/Auditor/Provisioner) are required for this DMA user. This user must own the VMR (conference room) entered in VMR Number. The user name value entered should be the same as the User ID displayed in the DMA admin web interface in User &gt; Users for the user created in step 7.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password of the DMA user, created in step 7, who owns the DMA conference room.</td>
</tr>
</tbody>
</table>

**Note: DMA username, domain, and password**
The username, domain, and password in the Distributed Media Service page should match the User Id, Domain, and password shown in the User > Users section of the DMA admin web interface.

5 When you complete the Multipoint Server settings, press **Save** to save the details and perform validation of the values entered in the text boxes.

<table>
<thead>
<tr>
<th>Configuration Status</th>
<th>Validation</th>
<th>Registration Status Field</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Success</td>
<td>Online</td>
<td>An error message appears with the cause of the validation failure, for example:</td>
</tr>
<tr>
<td>Incorrect</td>
<td>Failure</td>
<td>Offline</td>
<td>• wrong username, password, or domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• insufficient resources in the configured RMX MCU</td>
</tr>
</tbody>
</table>

**Immersive Settings**

Immersive settings include the IP address of the secondary codecs in the RealPresence Immersive Studio setup. For information about configuring the Immersive settings, refer to Configuring the IP Addresses of the Component Codecs.

**Room Control Devices**

Control of the room features is built into the RealPresence Immersive Studio system, eliminating the need for an external control system.

To view the status, IP address, and port number used for room control devices:

1. Go to Admin Settings > Room Control Devices.
2. Select the device for which you want to see the settings.

The settings for each device are described below.
### Room Device Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Specifies the state of the connection. The states are <strong>Connected</strong>, <strong>Not Connected</strong>, and <strong>Unknown</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the device that is being controlled.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Specifies the port number for TCPIP connection of the device that is being controlled.</td>
</tr>
</tbody>
</table>
Configuring the Diagnostic Settings

Polycom RealPresence Immersive Studio systems provide various screens that enable you to review information about calls made by the system, review network usage and performance, perform audio and video tests, and send system messages.

Polycom RealPresence Manageability Instrumentation Solution

The Polycom® RealPresence® Manageability Instrumentation solution simplifies management of Polycom RealPresence video collaboration services. RealPresence Manageability Instrumentation now enables you to collect, store, and export data in a consistent format across all Polycom endpoints, and hardware and software infrastructure systems. Polycom video and collaboration environments and infrastructure that include the Manageability Instrumentation solution capabilities are easier to monitor, operate, and secure.

RealPresence Manageability Instrumentation equips your Polycom devices with an embedded capability that enhances your ability to monitor them:

The Polycom Unified System logging Syslog transport format provides a system log message format compliant with RFC 5424 that enables you to log device events locally and remotely in a standardized way. Monitoring system logs is especially useful for troubleshooting and security purposes.

For detailed information on using the Manageability Instrumentation solution with your Polycom products, see the Polycom RealPresence Manageability Instrumentation Solution Guide.

Web Interface Diagnostics Screens

Read this section to learn how to find diagnostic information in the web interface.

To access the Diagnostics screens using the Polycom RealPresence Immersive Studio system web interface:

1. In your web browser address line, enter the RealPresence Immersive Studio or RealPresence OTX Studio system’s IP address.
2. Enter the Admin ID as the user name (default is admin), and enter the Admin Remote Access Password, if one is set.
3. Click Diagnostics from any page in the web interface.

System Diagnostics

You can find some system information by clicking the System link in the blue bar at the top of the page.
The web interface’s Diagnostics page has the following groups of settings in addition to the Send a Message application:

- System
- Audio and Video Tests

**System Diagnostics**

<table>
<thead>
<tr>
<th>Diagnostic Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Statistics</td>
<td>Displays information about the call in progress. To view more information about a specific stream, navigate to the desired stream and select <strong>More Info</strong>. From an individual stream view you can select <strong>Next Stream</strong> to view the next stream in the stream list.</td>
</tr>
<tr>
<td>System Status</td>
<td>Displays system status information.</td>
</tr>
<tr>
<td>Download Logs</td>
<td>Enables you to save system log information for each codec using separate web UI on each codec.</td>
</tr>
</tbody>
</table>
| System Log Settings | • Specifies the Log Level to use.  
• Enables Remote Logging, H.323 Trace, and SIP Trace.  
• Specifies the Remote Log Server Address.  
• Allows you to Send Diagnostics and Usage Data to Polycom, and get information about the Polycom Improvement Program. |
| Restart System    | Instructs the system to restart (system reboot). Restarting the RealPresence OTX Studio takes four minutes to complete. The system is not fully functional until the restart completes. During the restart the RealPresence Touch unpairs and repairs and the monitor lifts lower. |
| Sessions          | View information about everyone logged in to the RealPresence Immersive Studio system.                                                        |

**System Information**

You can find system information by clicking the **System** link in the blue bar at the top of the page.

**Call Statistics**

To display call statistics (in a call):

» Go to **Diagnostics > System > Call Statistics**.

  Displays information about the call in progress. Streams associated with the participant are displayed beneath the participant information in the order center, left, and right. If the system is not in a call, the page displays **The System is not currently in a call.**

  Select **More Info** to display the following detailed information:

  **Participant information**
  - Participant Name
  - Participant Number
  - Participant System
  - Call Type
Configuring the Diagnostic Settings

- Call Speed
- Encryption

**Participant Streams**

- Stream ID; possible stream IDs include Audio TX, Audio RX, Video TX, Video RX, Content TX, and Content RX
- Stream quality indicator; possible colors are green, yellow, and red.
- Protocol
- Format
- Rate Used
- Frame Rate
- Packets Lost
- % Packet Loss
- Jitter
- Encryption type, key exchange algorithm type, and key exchange check code (if the encryption option is enabled and the call is encrypted)
- Error concealment type, such as lost packet recovery (LPR), retransmission, or dynamic bandwidth allocation (DBA)

**System Status**

**To display system status:**

» Go to **Diagnostics > System > System Status**.

Displays the following system status information. When the status information for three systems is shown, the order is primary system, left system, and right system.

- Auto-Answer Point-to-Point Video
- Remote Control
- Audio Devices
- VisualBoard
- Global Directory Server
- Presence Service
- IP Network
- Gatekeeper
- SIP Registrar Server
- Log Threshold
- Meeting Password
- Calendaring Service
- Distributed Media Service
- People Display
- Content Display
Polycom, Inc.  75

Configuring the Diagnostic Settings

- Display Switcher
- Lighting Controller
- SoundStructure
- VisualBoard Display

Select More Info beside each topic for additional detail and links to configuration screens.

Downloading Logs

To download logs:

1. Go to Diagnostics > System > Download Logs.
2. Select Download system log, and then specify a location on your computer to save the file.

System Log Settings

The system log captures devices and server events in a consistent manner within a log. The log can assist you when troubleshooting system issues. Log settings apply to all three systems in your RealPresence Immersive Studio setup.

To configure system log settings:

1. In your web browser address line, enter the RealPresence Immersive Studio system’s IP address.
2. Enter the Admin ID as the user name (default is admin), and enter the Admin Remote Access Password, if one is set.
3. Go to Diagnostics > System > System Log Settings.
4. Configure these settings.

System Log Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>Sets the minimum log level of messages stored in the Polycom RealPresence Immersive Studio system’s flash memory. DEBUG logs all messages. WARNING logs the fewest number of messages. Polycom recommends leaving this setting at the default value of DEBUG.</td>
</tr>
<tr>
<td>Enable Remote Logging</td>
<td>Specifies whether remote logging is enabled. Enabling this setting causes the Polycom RealPresence Immersive Studio system to send each log message to the specified server in addition to logging it locally. The system immediately begins forwarding its log messages when you select Save. Encryption is not supported for remote logging, so Polycom recommends remote logging only for secure, local networks.</td>
</tr>
<tr>
<td>Remote Log Server Address</td>
<td>Specifies the server address and port.</td>
</tr>
</tbody>
</table>
System Log Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Remote Log Server Transport Protocol | Specifies the type of transport protocol:  
  • UDP  
  • TCP  
  • TLS (secure connection) |
| Enable H.323 Trace          | Logs additional H.323 connectivity information.                             |
| Enable SIP Trace            | Logs additional SIP connectivity information.                               |
| Send Diagnostics and Usage Data to Polycom | Sends crash log server information to Polycom to help us analyze and improve the product. Click the Polycom Improvement Program button to view information about how your data is used. |

Caution: Do not enable the following settings unless advised to do so by Polycom Support:
- Enable H.323 Trace
- Enable SIP Trace
- Send Diagnostics and Usage Data to Polycom

<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. Select the Polycom Improvement Program button to view information about how your data is used.</td>
</tr>
</tbody>
</table>

5 Select **Download system log**, and then specify a location on your computer to save the file.

Restarting the System

To restart the system:

  » In the primary codec web UI, go to **Diagnostics > System > Restart System**.

Sessions

You can use the sessions list to see information about everyone logged in to a RealPresence Immersive Studio system including:
- Type of connection, for example, Web
- User ID associated with the session, typically Admin or User
- Remote IP address, the addresses of people logged in to the system from their computers
To view the Sessions List:

» Go to Diagnostics > System > Sessions.

Audio and Video Tests

Audio Meters

Audio meters measure the strength of audio signals from content audio and recording outputs (HDMI1, HDMI2, HDMI3, component, and Recording Out).

The Audio Meters indicate peak signal levels. Set signal levels so that you see peaks between +3dB and +7dB with normal speech and program material. Occasional peaks of +12dB to +16dB with loud transient noises are considered acceptable. A meter reading of +20dB corresponds to 0dBFS in the RealPresence Immersive Studio system audio. A signal at this level is likely clipping the audio system.

Meters function only when the associated input is enabled. Currently, the microphone meters function is only available from the SoundStructure Studio software.

To use audio meters:

» Go to Diagnostics > Audio and Video Tests > Audio Meter.

Calibrating the Microphone

Microphone calibration is required before making TIP calls. The Microphone Calibration Screen does not provide any indication of whether the calibration process has been performed for any given seat. Carefully track the seats as you perform the calibration so no seat is omitted.

To calibrate the microphones:

1 In the primary codec web user interface, go to Diagnostics > Audio and Video Tests > Microphone Calibration.

   The Microphone Calibration screen displays. The screen displays a representation of the furniture in the room with circles representing the seating locations.

2 Sit in any of the seats at the table. It may be convenient to start at the far right or left seat and work your way around the table(s).

3 On the Microphone Calibration screen, select the circle corresponding to your current seated location. A message box showing progress appears.

4 Face the monitors and speak normally. After a few seconds, a successful calibration message appears.

   If calibration fails, a calibration failure message appears. Close the message and try again. If you are unable to achieve a successful calibration, verify proper microphone installation and try again. Contact Polycom Support to verify proper installation, if necessary.

5 Close the message box.

6 Repeat steps 2 through 5 for all seating locations.
Configuring the Utilities Settings

In the web interface, you can configure, manage, and monitor Polycom RealPresence Immersive Studio systems from a computer. You can also use Polycom RealPresence Resource Manager, or the API commands.

Managing System Profiles

Administrators managing systems that support multiple applications can change system settings using profiles. You can store a RealPresence Immersive Studio system profile on a computer as a .profile file. The number of profiles you can save is unlimited. Polycom recommends using profiles only as a way to back up system settings. Attempting to edit a stored profile or upload it to more than one system on the network 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.

Storing a Profile

You can download and store a profile from the Profile Center.

To store a profile:

1. Go to Utilities > Services > Profile Center.
2. Select Download.
3. Save the file to a location on your computer.

Uploading a Profile

You can upload a Settings Profile from your system to the Profile Center.

To upload a profile:

1. Reset the Polycom RealPresence Immersive Studio system to restore default settings.
2. Go to **Utilities > Services > Profile Center**.
3. Next to **Upload Settings Profile**, select **Browse**, and navigate to the location of the profile `.csv` file on your computer.
4. Select **Open** to upload the `.csv` file to your system.

### Call Detail Report (CDR)

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

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

Polycom recommends that you download the report periodically to prevent its growing to an unmanageable size. If you consider that 150 calls result in a CDR of approximately 50 KB, you might set up a schedule to download and save the CDR after about every 1000–2000 calls just to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads.

### Enabling CDR

In order to use the CDR, you must first enable it.

**To enable CDR:**

» Go to **Admin Settings > General Settings > System Settings > Recent Calls** and enable the **Call Detail Report** check box.

### Viewing and Downloading the CDR

You can open or save the CDR file on your computer.

**To view and download the CDR:**

1. Go to **Utilities > Services > Call Detail Report (CDR)**.
2. Select **Most Recent Call Report**.
   - A report for each system and an aggregated report are delivered in a compressed file.
3. Specify whether to open or save the file on your computer.

### Information in the Call Detail Report (CDR)

The following table describes the data fields in the Call Detail Reports.
### Call Detail Report Information

<table>
<thead>
<tr>
<th>Data</th>
<th>Description for Individual System Report</th>
<th>Description for Aggregated Report</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>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Start Date</td>
<td>The call start date, in the format dd-mm-yyyy.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The call start time, in the 24-hour format hh:mm:ss.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>End Date</td>
<td>The call end date.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>End Time</td>
<td>The call end time.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call Duration</td>
<td>The length of the call.</td>
<td>Same as primary system.</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>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Remote System Name</td>
<td>The system name of the far site.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call Number 1</td>
<td><strong>Outgoing calls:</strong> The number dialed from the first call field, not necessarily the transport address. <strong>Incoming calls:</strong> The caller ID information from the first number received from a far site.</td>
<td>Combined addresses separated by a semicolon.</td>
</tr>
<tr>
<td>Call Number 2</td>
<td><strong>Outgoing calls:</strong> The number dialed from the second call field, not necessarily the transport address. <strong>Incoming calls:</strong> The caller ID information from the second number received from a far site.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call Number 2 (If applicable for call)</td>
<td></td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Transport Type</td>
<td>The type of call, either H.323 (IP) or SIP.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call Rate</td>
<td>The bandwidth negotiated with the far site.</td>
<td>Sum of the call rates of the individual calls.</td>
</tr>
<tr>
<td>System Manufacturer</td>
<td>The name of the system manufacturer, model, and software version, if they can be determined.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call Direction</td>
<td><strong>In</strong> for calls received. <strong>Out</strong> for calls placed from the RealPresence Immersive Studio system.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Conference ID</td>
<td>A identification 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>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Call ID</td>
<td>Identifies individual calls within the same conference.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Total H.320 Channels Used</td>
<td>0 (zero) indicates that the call did not connect. 1 indicates a connected call.</td>
<td>The total number of codecs used in the call.</td>
</tr>
</tbody>
</table>
### Call Detail Report Information

<table>
<thead>
<tr>
<th>Data</th>
<th>Description for Individual System Report</th>
<th>Description for Aggregated Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Alias</td>
<td>The alias of the far site.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Endpoint Additional Alias</td>
<td>An additional alias of the far site.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>View Name</td>
<td>Names the web or local interface used in the call.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>User ID</td>
<td>Lists the ID of the user who placed the call.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Endpoint Transport Address</td>
<td>The actual address of the far site, not necessarily the address dialed.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Audio Protocol (Tx)</td>
<td>The audio protocol transmitted to the far site, such as G.728 or G.722.1.</td>
<td>Same as primary system.</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>
<td>Same as primary system.</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>
<td>Same as primary system.</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>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Video Format (Tx)</td>
<td>The video format transmitted to the far site, such as CIF or SIF.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Video Format (Rx)</td>
<td>The video format received from the far site, such as CIF or SIF.</td>
<td>Same as primary system.</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>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Q.850 Cause Code</td>
<td>The standard Q.850 cause code showing how the call ended.</td>
<td>Same as primary system.</td>
</tr>
<tr>
<td>Total H.320 Errors</td>
<td>The number of H.320 errors experienced during the call.</td>
<td>Same as primary system.</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 H.323 call.</td>
<td>Average of the individual call numbers.</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 H.323 call.</td>
<td>Average of the individual call numbers.</td>
</tr>
<tr>
<td>Average Packets Lost (Tx)</td>
<td>The number of packets transmitted that were lost during an H.323 call.</td>
<td>Sum of packets that were lost in the individual calls.</td>
</tr>
</tbody>
</table>
Sending a Message

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

To send a near-site message:

1. Go to Utilities > Send a Message.
2. In the Send a Message field, enter the text. You can enter up to 100 characters.
3. Select Send.

The message is displayed for 15 seconds on the screen of the system that you are managing.
Monitoring a Room or Call

The remote monitoring feature enables administrators to view the room where the system is installed. Camera controls and presets are not supported in this release of RealPresence Immersive Studio.

To monitor a room or a call using the web interface:

» Go to Utilities > Tools > Remote Monitoring.

Displaying a Closed Caption

The closed caption feature is not supported in this release of the RealPresence Immersive Studio system.
Security Profile Definitions

Configuring the Low Security Profile

The Low Security Profile is supported in this release of the RealPresence Immersive Studio. The following table shows the default values for specific Admin settings.

Low Security Profile Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Low Settings</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Default Value</td>
</tr>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Answer Point to Point Video</td>
<td>Checkbox</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto Answer Multipoint Video</td>
<td>Checkbox</td>
<td>Disabled</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>Enabled</td>
</tr>
<tr>
<td>Pairing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartPairing Mode</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Checkbox</td>
<td>Enabled</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Auto TLS TCP UDP</td>
<td>Auto</td>
</tr>
<tr>
<td>Dialing Preference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalable Video Coding Preference (H.264)</td>
<td>AVC Only</td>
<td>AVC Only</td>
</tr>
</tbody>
</table>
### Low Security Profile Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Low Range</th>
<th>Default Value</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<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><strong>Security Profile</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Profile</td>
<td>Maximum</td>
<td>Low</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>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Authentication</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</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>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Restrict to HTTPS</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Web access port (http)</td>
<td>16-bit integer</td>
<td>80</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Note:</strong> You cannot select this setting if the <strong>Restrict to HTTPS</strong> setting is enabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Remote Access: Telnet</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</td>
<td>1,2,3,5,10,20,30,45 minutes, 1,2,4,8 hours</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>10-50</td>
<td>25</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Video Display on Web</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Low Security Profile Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Low</th>
<th>Default Value</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require AES Encryption for Calls</td>
<td>Off When Available Required-Video Calls Required-All Calls</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require FIPS 140 Cryptography</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Local Accounts</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Lockout</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock Admin Account After Failed Logins</td>
<td>Off,2-10</td>
<td>Off</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</td>
<td>Off,[1..24] hours</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock User Account After Failed Logins</td>
<td>Off,2-10</td>
<td>Off</td>
<td>Yes</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>
</tr>
<tr>
<td>Reset User Account Lock Counter After</td>
<td>Off,[1..24] hours</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Login Credentials</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>Disabled</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Password Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin (Room, Remote), User (Room, Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>Off,1-16</td>
<td>Off</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>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>
<tr>
<td>Remote Access (Admin Remote, User Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Off,1-16,32</td>
<td>Off</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Low Security Profile Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Low</th>
<th>Default Value</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Lowercase</td>
<td>Off,1,2,All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase</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>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### User (Room), Admin (Room)

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Off,1-16,32</th>
<th>Off</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Lowercase</td>
<td>Off,1,2,All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase</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>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Meeting

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Off,1-20,32</th>
<th>Off</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Lowercase</td>
<td>Off,1,2,All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase</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>Off</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>Minimum Length</td>
<td>1-16,32</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Lowercase</td>
<td>Off,1,2,All</td>
<td>Off</td>
<td>Yes</td>
</tr>
<tr>
<td>Require Uppercase</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>
</tbody>
</table>
## Low Security Profile Settings

<table>
<thead>
<tr>
<th>Admin Settings Area</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
</tr>
<tr>
<td>Reject Previous Password</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 Consecutive Repeated Characters</td>
<td>Off,1-4</td>
</tr>
<tr>
<td>Can contain ID or Its Reverse Form</td>
<td>Checkbox</td>
</tr>
</tbody>
</table>

### Security Banner

<table>
<thead>
<tr>
<th>Enable Security Banner</th>
<th>Checkbox</th>
<th>Disabled</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner Text</td>
<td>DoD</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>
</tbody>
</table>

### Certificates

#### Certificate Options

<table>
<thead>
<tr>
<th>Certificate Validation (Web Server)</th>
<th>Checkbox</th>
<th>Disabled</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Validation (Client Apps)</td>
<td>Checkbox</td>
<td>Disabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Revocation

<table>
<thead>
<tr>
<th>Revocation Method</th>
<th>OCSP</th>
<th>CRL</th>
<th>OCSP</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>Checkbox</td>
<td>Enabled</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Servers

#### Directory Servers

<table>
<thead>
<tr>
<th>XMPP</th>
<th>Provisioned-only</th>
<th>Disabled</th>
<th>Yes (via provisioning)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Off Microsoft Polycom GDS LDAP</td>
<td>Off</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** The Microsoft selection means Microsoft Lync Server 2010 or 2013, depending on what is installed.

### Calendaring Service

<table>
<thead>
<tr>
<th>Enable Calendaring Service</th>
<th>Checkbox</th>
<th>Disabled</th>
<th>Yes</th>
</tr>
</thead>
</table>
Performing the RealPresence Touch Out-of-Box Setup

You can perform the RealPresence Touch out-of-box setup by ensuring that the RealPresence Touch is connected and navigating through three simple screens.

To perform the RealPresence Touch out-of-box setup:

1. If the RealPresence Touch is not connected, connect it to the Ethernet cable specified for use by Polycom. If this is the first time the device has been powered on, the language screen will display automatically.
2. On the language screen, touch the language you want to use and touch Next.
3. On the password screen the administrator password is automatically set to your system serial number. Polycom recommends that you create a new, custom administrator password. To create a new administrator password, touch Create New Password. In the Password field, type in your new password. In the Confirm Password field type in your new password again. Touch Save.
4. On the Network Settings screen type in the network parameters. For information about obtaining network parameters refer to Obtaining the Network Parameters.
5. The RealPresence Touch pairing screen automatically displays.

Pairing RealPresence Touch with RealPresence Immersive Studio or RealPresence OTX Studio.

You can easily pair your RealPresence Touch with RealPresence Immersive Studio or RealPresence OTX Studio room systems.

To pair the RealPresence Touch:

1. Touch Manually Pair.
2. In the Device Address field, enter the IP address.
3. In the Admin ID field, enter the administrator user name.
4. In the Password field, enter the administrator password.
5. Touch Pair.
6. You may be prompted that an update is available. Touch Update and the update begins. After a few minutes, the Home screen appears.
Customizing the RealPresence Touch Home Screen

You can use the RealPresence Group 700 system web interface to configure how information is displayed on the Home screen of the RealPresence Touch device. These settings are included in the RealPresence Group System settings profile, and included in bundled provisioning when using RealPresence Resource Manager. For more information about RealPresence Group systems settings refer to the Polycom RealPresence Group Series Administrator Guide available at support.polycom.com.

To configure the RealPresence Touch Home Screen using the web interface:

1. In the web interface, go to Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration.
2. Configure the settings on the Home Screen Settings page that are described in the following sections.

Choosing Icon Buttons That Display on the RealPresence Touch Home Screen

By default, two icon buttons appear in the lower center of the Home screen; users see the Place a Call and Show Content icons. However, you can customize the number of screens and Home screen icons in a preferred order. Once you customize the Home screen configuration, users can scroll through one to three Home Screens, with up to three icons on each screen.

To display the Home screen icons:

1. In the web user interface, go to Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration.
2. Under Configure Home Screen, click Configure Home Screen Options.
3. At Home screen 1 > Button 1, select one to three icon buttons to appear per screen in your preferred order. You can select from the following icon buttons:
   - None (no icon)
   - Place a Call
   - Show Content
   - Keypad
   - Contacts
   - System Information
   - User Settings
   - Administration
4. If you want to include more than one Home screen, continue selecting icon buttons for Home Screen 2 and Home Screen 3 until all screens are configured. For example, Home Screen 1 > Button 1 > Recent Call Button 2 > Place a Call > Button 3 > Contacts.
5. To save your selections, click Save.

Your new selections display on the RealPresence Touch Home screens.
Customizing the Place a Call Screen Icon Buttons on the RealPresence Touch Device

You can customize the Place a Call screen to display certain icon buttons. Since there are two ways to place a call by default, after you tap the Place a Call button, both options display on the screen. You can customize one of the icon buttons to be the default. The other Place a Call icon button continues to display at the top of the screen.

To customize the Place A Call screen icon buttons:

1. In the web interface, go to Admin Settings > General Settings > Pairing > RealPresence Touch Home Screen Configuration.
2. Under Configure Home Screen, click Place A Call Screen.
3. Under Select Preferred Sub Menu, choose from the following:
   - Keypad
   - Contacts
4. Click Save.
   
   Your new selection displays on the RealPresence Touch Home screens.

Changing the Background Image of the Home Screen on the RealPresence Touch Device

The RealPresence Touch Home screen displays a blank wallpaper, however, three optional wallpaper images are available from the web interface.

To change the background image:

1. In the web interface, go to Admin Settings > General Settings > Home Screen Settings > Wallpaper.
2. Select the image that you want to use.
   
   The selected image is displayed on the main monitor and on the RealPresence Touch.

Changing to a Custom Background Image on the RealPresence Touch

You can match the RealPresence Touch device background to the RealPresence Immersive Telepresence or RealPresence OTX Studio system background by selecting the default option. Without a custom image loaded, the image from the primary system screen displays as the RealPresence Touch device background when paired with the system. When the default option is selected, the system background will display on the RealPresence Touch device.

For a custom image on the RealPresence Touch device separate from the system background, use the following image guidelines.

- Less than 5 MB
- Pixel size of 1920 x 1280 or 1280 x 800 (width by height)
- JPEG file format
To upload a custom background to the RealPresence Touch device:

1. Go to Admin Settings > General Settings > Home Screen Settings > RealPresence Touch Background.
2. Browse to the desired image file and click Choose File > Upload.
3. Select the image that you want to use and click Save.
   The image displays on the RealPresence Touch device home screen.