ADMINISTRATOR GUIDE

6.1.0 | February 2017 | 3725-66892-005A

Polycom® RealPresence Immersive Telepresence (ITP)

6001 America Center Drive
San Jose, CA 95002
USA

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

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

Contents

Before You Begin

Topics:

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

Note: In this document, when you see " RealPresence ITP " systems, the content applies to RealPresence Immersive Studio, RealPresence Immersive Studio Flex, and RealPresence OTX Studio systems. If content applies to specific products only, the product names are included.

Please read the RealPresence ITP system documentation before you install or operate the system. Related documents for RealPresence ITP systems are available from **Documents and Downloads** at Polycom Support.

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.

Polycom Partner and Solution Resources

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

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Microsoft Office Communications Server, Microsoft Lync Server 2013, Skype for Business Server 2015, or Office 365 integrations. For additional information and details, refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

The Polycom Community

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

Getting Started with ITP

Topics:

The RealPresence Immersive Studio, RealPresence Immersive Studio Flex, and RealPresence OTX Studio systems are state-of-the-art visual collaboration tools. With crisp, clean video and crystal-clear sound, RealPresence ITP 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.

Control the Monitor Lifts from the Web Interface

You can raise or lower RealPresence OTX Studio table monitor lifts for optimum conference viewing. You can raise or lower all three monitors from the web interface.

Procedure

» Go to **Utilities** > **Tools** > **OTX Setup** and select **Up** or **Down**.

Obtaining the Network Parameters

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

...x+	Device	...x+	Device
1	Group Series 700 (A1)	11	Display1 (D1)
2	Group Series 500 (A2)	12	Display2 (D2)
3	Group Series 500 (A3)	13	Display3 (D3)
4	<Reserved>	14	<Reserved>
5	SoundStructure	15	<Reserved>
6	Nport	16	Lutron NWK
7	<Reserved>	17	APC (PWR1)
8	DisplayMatrix	18	APC (PWR2)
9	<Reserved>	19	APC (PWR3)
10	Tablet	20	Ethernet Switch (if required)

Using a Provisioning Service

Topics:

A provisioning service prepares and equips your network to provide services to its users.

Enable a Provisioning Service

To register the RealPresence ITP system with the Polycom RealPresence Resource Manager system, enter the registration information and attempt to register by going to **Admin Settings** in the RealPresence ITP system web interface. Multiple RealPresence ITP systems can be registered to a single user.

Procedure

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.
4. Select **Register or Update**.

   The system tries to register with the Polycom RealPresence Resource Manager system using NTLM authentication.

Configure a Provisioning Service

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

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

Procedure

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

Provisioning Service Settings

Setting	Description
Domain	Specifies the domain for registering to the provisioning service.

Setting	Description
User Name	Specifies the endpoint's user name for registering to the provisioning service.
Password	Specifies the password that registers the system to the provisioning service.
Server Address	Specifies the address of the Polycom RealPresence Resource Manager system running the provisioning service.

Set Up the Distributed Media Service

By default, the RealPresence ITP systems supports the Polycom® RealPresence® Distributed Media Application™ (DMA®). RealPresence DMA enables multipoint conferences.

Procedure

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.

      The Add MCU Pool window appears.
   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.

      The Add MCU Pool Order window appears.
   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.

The Add Conference Template window appears.

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.

The Add User window appears.

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 by dialing in to the conference room created above from the RealPresence ITP endpoint by dialing the dial-in number of the conference room.

If the codec enters the conference, then the configuration is correct.

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.

Configure the Distributed Media Service

By default, the RealPresence ITP system supports the Polycom RealPresence Distributed Media Application™ (DMA). RealPresence DMA enables multipoint conferences. Refer to the DMA documentation for detailed instructions on setting up the service, including MCUs, pools, conference templates, etc.

Keep the following in mind:

- All the endpoints (conference initiator and conference participants) should be registered to DMA as H323 and/or SIP endpoints. This may not be required of the conference participants if you are using only an IP address to perform blast dialing.
- The DMA must 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 an MLA registered to the RMX for applying the proper layouts.

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

Procedure

1. Login to the web interface of the RealPresence ITP system as admin.
2. Go to **Admin Settings** > **Servers** > **Distributed Media Service**.
3. Select the **Enable Multipoint Server** check box.
4. Configure the following settings:

Multipoint Server Settings

Setting	Description
Virtual Meeting Room (VMR) Number	Specifies the DMA conference room number/ID to use for conferencing activities, created in step 8.
Server Address	Specifies the DMA server that hosts the conference room/VMR.
Domain	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** > **Users** in the room item for the user created in step 7.
User Name	Specifies the User ID of the DMA user, created in step , 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** > **Users** for the user created in step 7.
Password	Specifies the password of the DMA user, created in step 7, who owns the DMA conference room.

Note: 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.

Configuration Status	Validation	Registration Status Field	Notes
Correct	Success	Online	

Configuration Status	Validation	Registration Status Field	Notes
Incorrect	Failure	Offline	An error message appears with the cause of the validation failure, for example: • wrong username, password, or domain • insufficient resources in the configured RMX MCU

Certificates and Security Profiles within a Provisioned System

When your RealPresence ITP 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.

- 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.

SNMP Condition Reports

Topics:

RealPresence ITP systems support SNMP (Simple Network Management Protocol) versions 1, 2c, and 3.

A RealPresence ITP system sends SNMP reports to indicate conditions, including the following:

- Standard MIB information communicated by individual codecs independently
- Polycom MIB information communicated only by the primary codec and consisting of only primary codec information
- All alert conditions found on the system
- Details of jitter, latency, and packet loss
- 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

Download MIBs for SNMP Management

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

Procedure

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

Configure SNMP Management

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

Procedure

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

Setting	Description
Enable SNMP	Allows administrators to manage the system remotely using SNMP.
Enable Legacy Notifications	Supports sending notifications that are compatible with the legacy MIB.
Enable New Notifications	Supports sending notifications that are compatible with the new MIB.
Version1	Enables the use of the SNMPv1 protocol.
Version2c	Enables the use of the SNMPv2c protocol.
Version3	Enables the use of the SNMPv3 protocol. You must select this setting to use the subsequent settings that apply only to SNMPv3.
Read-Only Community	Specifies the SNMP management community in which you want to enable this system. The default community is `public`. **Note:** Polycom does not support SNMP write operations for configuration and provisioning; the read-only community string is used for both read operations and outgoing SNMP traps.
Contact Name	Specifies the name of the person responsible for remote management of this system.
Location Name	Specifies the location of the system.
System Description	Specifies the type of video conferencing device.
User Name	Specifies the SNMPv3 User Security Model (USM) account name that will be used for SNMPv3 message transactions. The maximum length is 64 characters.
Authentication Algorithm	Specifies the type of SNMPv3 authentication algorithm used: • SHA • MD5
Authentication Password	Specifies the SNMPv3 authentication password. The maximum length is 48 characters.

Setting	Description
Privacy Algorithm	Specifies the type of SNMPv3 cryptography privacy algorithm used: • CFB-AES128 • CBC-DES
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.
Engine ID	Specifies the unique ID of the SNMPv3 engine. This setting might be needed for matching the configuration of an SNMP console application. The Engine ID is automatically generated, but you can create your own ID, as long as it's between 10 and 32 hexadecimal digits. Each group of 2 hex digits can be separated by a colon character (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (therefore, ***:F:*** is equivalent to ***:0f:***). The ID cannot be all zeros or all Fs.
Listening Port	Specifies the port number SNMP uses to listen for messages. The default listening port is 161.
Transport Protocol	Specifies the transport protocol used: • TCP • UDP
Destination Address1 **Destination Address2** **Destination Address3**	Specifies the IP addresses of the computers you intend to use as your network management station and to which SNMP traps will be sent. Each address row has four settings: 1 IP Address (accepts IPv4 and IPv6 addresses, host names, and FQDNs) 2 Message Type (Trap, Inform) 3 SNMP protocol version (v1, v2c, v3) 4 Port (the default is 162) Disabling the **Port** setting disables the corresponding Destination Address.

Configuring General System Settings

Topics:

This section provides information on how to configure general system settings for RealPresence ITP :

Name the System

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 RealPresence ITP room systems and for individual endpoints that are not part of RealPresence ITP room systems.
- For individual endpoints, disconnected from a telepresence conference, use the same or similar names as each other and as RealPresence ITP systems, then Polycom MLA sometimes mistakenly identifies the individual endpoints as Immersive Studio, Immersive Studio Flex, OTX Studio, or ITP systems.
- The TYPE OF ITP field enables Polycom Multipoint Layout Application to find the correct RealPresence ITP room, when the RealPresence ITP room is part of a telepresence conference participants list, but disconnected from the conference.

Procedure

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.
3. 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:

   - 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.
4. Click **Save**.

Set the Date and Time

System Time settings enable you to specify how date and time values are displayed.

Procedure

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

System Time Settings

Setting	Description
Date Format	Specifies how the date is displayed in the interface.
Time Format	Specifies how the time is displayed in the interface.
Auto Adjust for Daylight Saving Time	Specifies the daylight saving time setting. When you enable this setting, the system clock automatically changes for daylight saving time.
Time Zone	Specifies the time difference between Greenwich Mean Time (GMT) and your location.
Time Server	Specifies whether the connection to a time server is automatic or manual for system time settings. You can also select **Off** to enter the date and time yourself.
Primary Time Server Address **Secondary Time Server Address**	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.
Current DateCurrent Time	If **Time Server** is set to **Off**, these settings are configurable.

Configuring Network Settings

Topics:

Configure LAN Properties

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

Procedure

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

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

Setting	Description
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here.

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

Setting	Description
Host Name	Indicates the system's DNS name.
Domain Name	Displays the domain name currently assigned to the system. If the system does not automatically obtain a domain name, enter one here.
Autonegotiation	Specifies whether the network switch should automatically negotiate the LAN speed and duplex mode. If this setting is enabled, the **LAN Speed** and **Duplex Mode** settings become read only. Polycom and IEEE802.3 recommend that you use autonegotiation to avoid network issues.
LAN Speed	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.
Duplex Mode	Specifies the duplex mode to use. Note that the switch must support the Duplex mode that you choose.
Ignore Redirect Messages	Enables the RealPresence ITP 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.

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

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.

Exit Immersive Mode

In order to change the codec IP addresses, you must exit Immersive Mode.

Procedure

1. Go to the Immersive page in the primary codec web user interface.
2. Change the system from Primary to Standalone.

Change the IP Address of the Primary Codec

Follow these procedures to change the IP address of the Primary codec.

Procedure

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

   All codecs reboot.

Change the IP Address of the Secondary Codecs

Follow these procedures to change the IP address of the Secondary codecs.

Procedure

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, RealPresence Immersive Studio Flex**, 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.

Configure Network Quality Settings

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

Procedure

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

Network Quality Settings

Setting	Description
Automatically Adjust People or Content Bandwidth	Specifies whether the system should automatically adjust the bandwidth necessary for the People stream or Content stream depending on the relative complexity of the people video, content video, or both. This setting is not available if you select a **Quality Preference**.

Setting	Description
Quality Preference	Specifies which stream has precedence when attempting to improve network quality issues: • Both (People and Content Streams) • People Streams • Content Streams This setting is not available when the **Automatically Adjust People/Content Bandwidth** setting is enabled.

Configure 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.

Procedure

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

SIP Settings

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

Setting	Description
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure within which your RealPresence Immersive Studio operates determines which protocol is required. **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. **TCP** provides reliable transport via TCP for SIP signaling. **UDP** provides best-effort transport via UDP for SIP signaling. **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.
Sign-in Address (for Left, Main, and Right Codecs)	Specifies the SIP address or SIP name of the system, for example, vineyarditp3@abc.com. If you leave this field blank, the system's IP address is used for authentication. .
User Name (for Left, Main, and Right Codecs)	Specifies the name to use for authentication when registering with a SIP Registrar Server, for example, msmith@company.com. If the SIP proxy requires authentication, this field and the password cannot be blank.
Password (for Left, Main, and Right Codecs)	Specifies the password that authenticates the system to the Registrar Server.

Setting	Description
Registrar Server	Specifies the IP address or DNS name of the SIP Registrar Server. • In a Microsoft Lync Server 2013 or Skype for Business Server 2015 environment, specify the IP address or DNS name of the Lync Server server. • If registering a remote RealPresence Immersive Studio with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role. By default for TCP, the SIP signaling is sent to port 5060 on the registrar server. By default for TLS, the SIP signaling is sent to port 5061 on the registrar server. Enter the IP address and port using the following format: <IP_Address>:<Port> <*IP_Address*> can be an IPv4 address or a DNS hostname such as `servername.company.com:6050`. Hostnames can resolve to IPv4 addresses. **Syntax Examples:** • To use the default port for the protocol you have selected: 10.11.12.13 • To specify a different TCP or UDP port: 10.11.12.13:5071
Proxy Server	Specifies the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you leave both the SIP Registrar Server and Proxy Server fields blank, no Proxy Server is used. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server. The syntax used for this field is the same as for the Registrar Server field.
Registrar Server Type	If the registering server is Lync, select **Microsoft**. Otherwise, select **Unknown**.

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

Related Links
SIP Address Naming Convention on page 25

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, RealPresence Immersive Studio, RealPresence Immersive Studio Flex, RealPresence 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

Codec	Format	Example
Main codec	<name>itp<number_of_codecs>@<domain>	vineyarditp3@abc.com
Right codec	~<name><codec_number>@<domain>	~vineyard2@abc.com
Left codec	~<name><codec_number>@<domain>	~vineyard3@abc.com

Related Links
Configure SIP Settings on page 22

Configuring SIP Settings for Integration with Microsoft Servers

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

Because Polycom RealPresence ITP 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 ITP 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 for Microsoft Environments Solution Deployment Guide*.

If your organization deploys multiple Lync Server pools, a Polycom RealPresence ITP 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 ITP system that has the TIP option, the system can interoperate with TIP endpoints. Note that the RealPresence ITP 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 for Cisco Environments Solution Deployment Guide*.

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

RTV and Lync-Hosted Conference Support

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

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

Specify Quality of Service

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

Procedure

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

Quality of Service Settings

Setting	Description
Type of Service	Specifies your service type and lets you choose how to set the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedence**—Represents the priority of IP packets sent to the system. The value can be between 0 and 5. • **DiffServ**—Represents a priority level between 0 and 63.

Setting	Description
Video	Specifies the IP Precedence or Diffserv value for video RTP traffic and associated RTCP traffic.
Audio	Specifies the IP Precedence or Diffserv value for audio RTP traffic and associated RTCP traffic.
Control	Specifies the IP Precedence or Diffserv value for control traffic on any of the following channels: • 323—H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control • SIP—SIP Signaling, Far End Camera Control, Binary Floor Control Protocol (BFCP)
OA&M	Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC.
Maximum Transmission Unit Size	Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or select a maximize size.
Maximum Transmission Unit Size Bytes	Specifies the MTU size, in bytes, used in IP calls. If the video becomes blocky or network errors occur, packets might be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets might be too small; increase the MTU.
Enable Lost Packet Recovery	Enables the system to use LPR (Lost Packet Recovery) if packet loss occurs.
Enable RSVP	Enables the system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.
Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum line speed for a call.
Maximum Transmit Bandwidth	Specifies the maximum transmit line speed between 64 kbps and the system's maximum line rate.
Maximum Receive Bandwidth	Specifies the maximum receive line speed between 64 kbps and the system's maximum line rate.

Configure Servers

This section shows how to set up various servers in your RealPresence ITP system.

Setting Up a Directory Server in Standard Operating Mode

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.

Directory Servers Supported in Standard Operating Mode

Directory Servers Supported	Authentication Protocols	Global Directory Groups	Entry Calling Information
LDAP with H.350 or Active Directory	Any of the following: • NTLM v2 only • Basic • Anonymous	Not Supported	Might include: • 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 *
Microsoft Lync Server 2013 and Skype for Business Server 2015	NTLM v2 only	Contact groups but not distribution lists	Might include SIP address (SIP URI)
* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats: • +Country Code.Area Code.Number • +Country Code.(National Direct Dial Prefix).Area Code.Number			

Setting Up a Directory Server with RealPresence Resource Manager Provisioning

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 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

Directory Servers Supported	Authentication Protocol	Global Directory Groups	Entry Calling Information
LDAP by a Polycom RealPresence Resource Manager system	NTLM v2 only	Pre-defined groups from the LDAP directory are shown in Polycom RealPresence ITP system's directory	Might include: ▪ H.323 dialed digits, H.323 ID, or H.323 extension ▪ Phone number * ▪ SIP address
Microsoft Lync Server 2013 and Skype for Business Server 2015	NTLM v1 only	Contact groups but not distribution lists	Might include SIP address (SIP URI)
* To successfully call a phone number from the LDAP directory, the phone number must be stored in one of the following formats: ▪ +Country Code.Area Code.Number ▪ +Country Code.(National Direct Dial Prefix).Area Code.Number			

Configure the Skype for Business Directory Server

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

Procedure

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.

Microsoft Directory Server Settings

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

Immersive Settings

Immersive settings include the IP address of the secondary codecs in the RealPresence Immersive Studio setup.

Room Control Devices

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

Procedure

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

Setting	Description
Status	Specifies the state of the connection. The states are **Connected**, **Not Connected**, and **Unknown**.
IP Address	Specifies the IP address of the device that is being controlled.
Port Number	Specifies the port number for TCPIP connection of the device that is being controlled.

Securing the System

Topics:

Configure the System for Use with a Firewall or NAT

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

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

Procedure

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

Firewall Settings

Setting	Description
Fixed Ports	Lets you specify whether to define the TCP and UDP ports. • If the firewall is not H.323 compatible, enable this setting. The RealPresence ITP system assigns a range of ports starting with the TCP and UDP ports you specify. The system defaults to a range beginning with port 3230 for both TCP and UDP. **Note**: You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic. • If the firewall is H.323 compatible or the system is not behind a firewall, disable this setting. For IP you need 2 TCP and 8 UDP ports per connection. For SIP you need TCP port 5060 and 8 UDP ports per connection. **Note:** Because RealPresence ITP supports ICE, the range of fixed UDP ports is 112. The system cycles through the available ports from call to call. After the system restarts, the first call begins with the first port number, either 49152 or 3230. Subsequent calls start with the last port used, for example, the first call uses ports 3230 to 3236, the second call uses ports 3236 to 3242, the third call uses ports 3242 through 3248, and so on.
TCP Ports **UDP Ports**	Specifies the beginning value for the range of TCP and UDP ports used by the system. The system automatically sets the range of ports based on the beginning value you set. **Note**: You must also open the firewall's TCP port 1720 to allow H.323 traffic.
Enable H.460 Firewall Traversal	Enables the system to use H.460-based firewall traversal for IP calls.

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

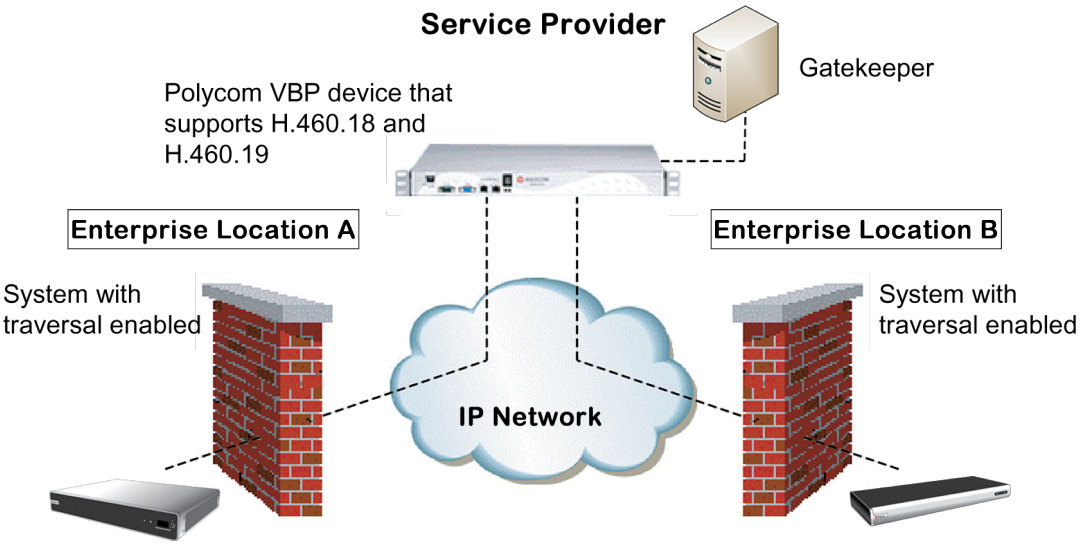
In environments set up behind a firewall, firewall administrators can choose to limit access to TCP connections only. Although TCP is an accurate and reliable method of data delivery that incorporates error-checking, it is not a fast method. For this reason, real-time media streams often use UDP, which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

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

H.460 NAT Firewall Traversal

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

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



Procedure

1. Enable firewall traversal.
   a) Go to **Admin Settings** > **Network** > **IP Network** > **Firewall**.
   b) Select **Enable H.460 Firewall Traversal**.
2. Register the system to an external Polycom VBP device that supports the H.460.18 and H.460.19 standards.
3. Make sure that firewalls being traversed allow the RealPresence ITP system behind them to open outbound TCP and UDP connections.
   - Firewalls with a stricter rule set should allow the RealPresence ITP system to open at least the following outbound TCP and UDP ports:
     - (TCP)
     - 14085-15084 (TCP)
     - (UDP)
     - 16386-25386 (UDP)

- Firewalls should permit inbound traffic to TCP and UDP ports that have been opened earlier in the outbound direction.

External Authentication

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

The RealPresence ITP 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 ITP 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 ITP system, make sure to configure the Active Directory Server Address on the RealPresence ITP endpoint using the address information that is in the Active Directory Server's identity certificate. This is important in enabling the RealPresence ITP 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 ITP system using the server's IP address will result in certificate validation failure, and consequently authentication failure. The RealPresence ITP system configuration would have to specify the server by DNS name in this case to successfully match the server certificate data.

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

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

Configure Access Settings

Settings in this section enable you to configure remote usage of the RealPresence ITP 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 ITP system, such as the local interface, web interface, Telnet, or serial API.

Procedure

1. Go to **Admin Settings** > **Security** > **Global Security** > **Access**.
2. Configure the following settings.

Your security profile might affect the availability of some settings.

Access Settings

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

Setting	Description
Enable Diagnostics Port Idle Session Timeout	Specifies whether to allow the diagnostics port to time out at the configured time interval or not. The timeout setting is set under Idle **Session Timeout in Minutes**.
Enable API Port Idle Session Timeout	Specifies whether to allow the API port to time out at the configured time interval or not. The timeout setting is set under Idle **Session Timeout in** **Minutes**.
Enable Whitelist	Specifies whether the system web interface ports accept connections only from specified IP addresses.
Idle Session Timeout in Minutes	Specifies the number of minutes your web interface session can be idle before the session times out.
Maximum Number of Active Sessions	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.

Set 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.

Procedure

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

Password Policy Settings

Setting	Description
Minimum Length	Specifies the minimum number of characters required for a valid password.
Require Lowercase Letters	Specifies whether a valid password must contain one or more lowercase letters.
Require Uppercase Letters	Specifies whether a valid password must contain one or more uppercase letters.
Require Numbers	Specifies whether a valid password must contain one or more numbers.

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

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

Encryption Settings

AES encryption is a standard feature on all Polycom RealPresence ITP 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 ITP 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 ITP 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.

Enable Encryption

To use the AES encryption feature, you must first enable encryption.

Procedure

1. Go to **Admin Settings** > **Security** > **Global Security** > **Encryption**.
2. Configure these settings.

Encryption Settings

Setting	Description
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 TPS cipher suites

Configure Local Access

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

Procedure

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

Login Credentials

Setting	Description
Admin ID	Specifies the ID for the administrator account. The default Admin ID is **admin**. Admin IDs are not case sensitive.

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

Create a CSR

RealPresence ITP systems can generate requests for certificates (CSRs) that are then sent to a certificate authority (CA) for offical issuance. The CA is the trusted entity that issues, or signs, digital certificates for others.

Procedure

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

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

Setting	Description
Hash Algorithm	Specifies the hash algorithm for the CSR. You may select SHA-256 or keep the default SHA-1.
Common Name (CN)	Specifies the name that the system assigns to the CSR. Polycom recommends the following guidelines for configuring the Common Name: • For systems registered in DNS, use the Fully Qualified Domain Name (FQDN) of the system. • For systems not registered in DNS, use the IP address of the system.
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.**

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.

Configure Certificate Validation Settings

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

connects to LDAP directory services, the RealPresence ITP system is the client and the LDAP directory server is the server.

Procedure

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

Setting	Description
Maximum Peer Certificate Chain Depth	Specifies how many links a certificate chain can have. The term *peer certificate* refers to any certificate sent by the far-end host to the RealPresence ITP system when a network connection is being established between the two systems.
Always Validate Peer Certificates from Browser	Not supported.
Always Validate Peer Certificates from Server	Controls whether the RealPresence ITP 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 **Certificate Signing Requests (CSRs)** (provisioning, directory, SIP, and so forth).

Monitor 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 ITP .

Procedure

» Go to **Utilities** > **Tools** > **Remote Monitoring**.

View the Sessions List

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

Procedure

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

View the Security Profile

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

Procedure

1. Go to **Admin Settings** > **Security** > **Global Security**.
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.

Low Security Profile Definition

The Low Security Profile is supported on the RealPresence ITP system. The following table shows the default values for specific Admin settings.

Low Security Profile Settings

Admin Settings Area	Low		
	Range	Default Value	Configurable
General Settings			
System Settings			
Auto Answer Point to Point Video	Checkbox	Disabled	Yes
Auto Answer Multipoint Video	Checkbox	Disabled	Yes
Call Detail Report	Checkbox	Enabled	Yes
Enable Recent Calls	Checkbox	Enabled	Yes
Pairing			
SmartPairing Mode	DisabledAutomatic Manual	Disabled	Yes
Network			
IP Network			
Enable SIP	Checkbox	Enabled	Yes
Transport Protocol	AutoTLS TCP UDP	Auto	Yes

Admin Settings Area	Low		
	Range	Default Value	Configurable
Dialing Preference			
Scalable Video Coding Preference (H.264)	AVC Only	AVC Only	Yes
Security			
Global Security			
Security Profile			
Security Profile	MaximumHigh Medium Low	Low	Yes
Authentication			
Active Directory Authentication	Checkbox	Disabled	Yes
Access			
Enable Network Intrusion Detection System (NIDS)	Checkbox	Disabled	Yes
Enable Web Access	Checkbox	Enabled	Yes
Restrict to HTTPS	Checkbox	Disabled	Yes
Web access port (http) **Note:** You cannot select this setting if the **Restrict to HTTPS** setting is enabled.	16-bit integer	80	Yes
Enable Remote Access: Telnet	Checkbox	Disabled	Yes
Lock Port after Failed Logins	Off,2-10	Off	Yes
Port Lock Duration	1,2,3,5,10, 20,30 minutes, 1,2,4,8 hours	1 minute	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable
	Reset Port Lock Counter After	Off,[1..24] hours	Off	Yes
	Enable Whitelist	Checkbox	Disabled	Yes
	Idle Session Timeout	1,2,3,5,10, 20,30,45 minutes, 1,2,4,8 hours	10	Yes
	Maximum Number of Active Sessions	10-50	25	Yes
	Allow Video Display on Web	Checkbox	Disabled	Yes
Encryption				
	Require AES Encryption for Calls	OffWhen Available Required-Video Calls Required-All Calls	Off	Yes
	Require FIPS 140 Cryptography	Checkbox	Disabled	Yes
Local Accounts				
Account Lockout				
	Lock Admin Account After Failed Logins	Off,2-10	Off	Yes
	Admin Account Lock Duration	1,2,3,5 minutes	1	Yes
	Reset Admin Account Lock Counter After	Off,[1..24] hours	Off	Yes
	Lock User Account After Failed Logins	Off,2-10	Off	Yes
	User Account Lock Duration	1,2,3,5,10, 20,30 minutes, 1,2,4,8 hours	1 minute	Yes

Admin Settings Area	Low		
	Range	Default Value	Configurable
Reset User Account Lock Counter After	Off,[1..24] hours	Off	Yes
Login Credentials			
Use Room Password for Remote Access	Checkbox	Enabled	Yes
Require User Login for System Access	Checkbox	Disabled	Yes
Password Requirements			
Admin (Room, Remote), User (Room, Remote)			
Reject Previous Passwords	Off,1-16	Off	Yes
Minimum Password Age in Days	Off, 1,5,10,15,20,30	Off	Yes
Maximum Password Age in Days	Off, 30,60,90,100,110, 120,130,140,150,160, 170,180	Off	Yes
Minimum Changed Characters	Off,1-4,All	Off	Yes
Password Expiration Warning	Off,1-7	Off	Yes
Remote Access (Admin Remote, User Remote)			
Minimum Length	Off,1-16,32	Off	Yes
Require Lowercase	Off,1,2,All	Off	Yes
Require Uppercase	Off,1,2,All	Off	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable
	Require Numbers	Off,1,2,All	Off	Yes
	Require Special Characters	Off,1,2,All	Off	Yes
	Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
	Can contain ID or Its Reverse Form	Checkbox	Enabled	Yes
User (Room), Admin (Room)				
	Minimum Length	Off,1-16,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	Off,1,2,All	Off	Yes
	Require Numbers	Off,1,2,All	Off	Yes
	Require Special Characters	Off,1,2,All	Off	Yes
	Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
	Can contain ID or Its Reverse Form	Checkbox	Enabled	Yes
Meeting				

Admin Settings Area		Low		
		Range	Default Value	Configurable
	Minimum Length	Off,1-20,32	Off	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	Off,1,2,All	Off	Yes
	Require Numbers	Off,1,2,All	Off	Yes
	Require Special Characters	Off,1,2,All	Off	Yes
	Reject Previous Passwords	Off,1-16	Off	Yes
	Minimum Password Age in Days	Off, 1,5,10,15,20,30	Off	Yes
	Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
	Minimum Length	1-16,32	1	Yes
	Require Lowercase	Off,1,2,All	Off	Yes
	Require Uppercase	Off,1,2,All	Off	Yes
	Require Numbers	Off,1,2,All	Off	Yes
	Require Special Characters	Off,1,2,All	Off	Yes
	Reject Previous Passwords	Off,1-16	Off	Yes

Admin Settings Area		Low		
		Range	Default Value	Configurable
	Minimum Password Age in Days	Off, 1,5,10,15,20,30	Off	Yes
	Maximum Consecutive Repeated Characters	Off,1-4	Off	Yes
	Can contain ID or Its Reverse Form	Checkbox	Disabled	Yes
Security Banner				
Enable Security Banner		Checkbox	Disabled	Yes
Banner Text		DoDCustom	Custom	Yes
Local System Banner Text		Unicode characters, 2048 bytes max	Null (no text)	Yes
Remote System Banner Text		Unicode characters, 2048 bytes max	Null (no text)	Yes
Certificates				
Certificate Options				
	Certificate Validation (Web Server)	Checkbox	Disabled	Yes
	Certificate Validation (Client Apps)	Checkbox	Disabled	Yes
Revocation				
	Revocation Method	OCSPCRL	OCSP	Yes
	Allow Incomplete Revocation Checks	Checkbox	Enabled	Yes

Admin Settings Area	Low		
	Range	Default Value	Configurable
Servers			
Directory Servers			
XMPP	Provisioned-only	Disabled	Yes (via provisioning)
Service Type **Note:** the *Microsoft* selection means Microsoft Lync Server 2010 or 2013, depending on what is installed.	OffMicrosoft Polycom GDS LDAP	Off	Yes
Calendaring Service			
Enable Calendaring Service	Checkbox	Disabled	Yes

Audio Settings

Topics:

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

Configure Audio Settings

Procedure

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

General Audio Settings

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

Audio Input Settings

Setting	Description
Type	Displays the type of input for connected components.
Audio Input Level	Sets the audio input level for each connection.

Audio Output Setting

Setting	Description
Master Audio Volume	Sets the main audio output volume level that goes to the speakers.

3.5mm Audio Input Selection in a RealPresence OTX Studio System

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. 3.5 mm audio input is then heard from the RealPresence Group system speakers and from all far-end sites.

- 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.

Enable 3.5mm Audio Input in a RealPresence OTX Studio System

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

Procedure

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.

Set Up 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 ITP 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.

Procedure

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

Calibrate the Microphones

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.

Procedure

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.

Video Settings

Topics:

Do not change the default settings for the monitors. Avoid changing the following settings unless advised by Polycom Technical Support.

Note the three tabs, labeled Left, Main, and Right, that represent the left, main, and right systems.

Prevent Monitor Burn-In

Monitors used with RealPresence ITP 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.

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

Procedure

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**.

Configure Video Inputs

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

Procedure

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.
3. 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.

Configure Camera Sleep Mode

There are two Camera Sleep Mode options for your RealPresence ITP system.

Procedure

1. Go to **Admin Settings** > **Audio/Video** > **Video Inputs** > **General Camera Settings** > **Camera Sleep Mode**.
2. Select one of the following settings:
   - **Save Energy:** The camera goes into Standby mode to save resources.
   - **Fast Wake Up:** The camera wakes faster. This mode is recommended when the user is not concerned about power consumption and does not want to see the blue screen when the system wakes up.

Call Settings

Topics:

You can determine which call settings are available to users when they place and answer calls.

Set Time in Call

You can configure the Time in Call setting so that users can view their time in a call.

Procedure

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

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

Time in Call Settings

Setting	Description
Show Time in Call	Specifies the time display in a call: • **Elapsed Time**—Displays the amount of time in the call. • **System Time**—Displays the system time on the screen during a call. • **Off**—Time is not displayed.

Setting	Description
When to Show	Specifies when the time should be shown: • **Start of the call only**—Displays only when the call begins • **Entire call**—Displays continuously throughout the call • **Once per hour**—Displays at the beginning of the hour for one minute • **Twice per hour**—Displays at the beginning of the hour and midway through the hour for one minute
Show Countdown Before Next Meeting	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.

Set the Maximum Time in a Call

You can enable user to choose the maximum number of hours that are allowed for the call length. When a call reaches the set time, users will see a message asking whether they want to end or stay on the call. If an action is not indicated within a minute, the call is automatically disconnected. If the user decides to stay on the call, another prompt does not display.

This setting also applies when users are viewing the Near video screen or showing content, even if they 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.

Procedure

1. In the primary codec web UI, navigate to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings.**
2. For **Maximum Time in a Call**, do one of the following:
   - Enter the maximum number of hours allowed for call length.
   - Select **Off** to remove any time limit.

Set the Preferred Method for Placing Calls

You can set the dial pad or the Contacts screen as the preferred method for placing calls.

Procedure

1. In the primary codec web UI, go to **Admin Settings** > **General Settings** > **System Settings** > **Call Settings.**
2. Select **Dial Pad** or **Contacts**.

Setting Up Audio-Only Calls

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.

Enable Audio-Only Calls

You can enable this setting so audio calls are supported.

Procedure

1. In the web interface, go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options**.
2. Select **Enable Audio Add In**.

   Click **Save**.

Disable Audio-Only Calls

You can disable this setting so audio calls are not supported.

Procedure

1. In the web interface, go to **Admin Settings** > **Network** > **Dialing Preference** > **Dialing Options.**
2. Clear the **Enable Audio Add In** check box.

   Click **Save**.

Select the Call Type Order for Audio-Only Order Calls

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

Procedure

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
   - 323
   - SIP
3. Click **Save**.

Configure 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.

Note: SVC-based conferences are not supported.

Procedure

1. Go to **Admin Settings** > **Network** > **Dialing Preference**.
2. Configure the settings in the following table.

Dialing Options and Preferred Speeds

Setting	Description
Scalable Video Coding Preference	**AVC Only** is supported in this release.
Enable H.239	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.
Call Type Order	The default value is **Video**.
Video Dialing Order	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.
Preferred Speed for Placed Calls: **IP Calls**	Determines the speed to use for calls from this system. If the far-site system does not support the selected speed, the system automatically negotiates a lower speed.
Maximum Speed for Received Calls: **IP Calls**	Enables you to restrict the bandwidth used when receiving IP calls. If the far site attempts to call the system at a higher speed than selected here, the call is renegotiated at the speed specified in this field.

Enable Calling the Help Desk

You can enable a button on the RealPresence Touch device so that users can place an audio-only call to the help desk.

Procedure

1. In the RealPresence Group Series system web interface, go to **Admin Settings**> **General Settings** > **Pairing** >**RealPresence Touch Home Screen Configuration**.
2. Under **Configure Home Screen**, select **Configure Home Screen Options**.
3. At **Home screen 1 > Button 1**, select **Call Help Desk**.

   The Call Help Desk button displays on the RealPresence Touch home screen.

4. Go to **Admin Settings > General Settings > My Information > Contact Information**.
5. In the **Help Desk Number** field, enter the audio number or address for the **Call Help Desk** button. You cannot edit this field during an active help desk call. For RealPresence OTX Studio systems, select the **POTS/SSTR** check box.

Supported Call Types for Help Desk

From a RealPresence Touch device, you can place a call to the help desk using the following call types:

- Audio-only SIP
- Audio-only H.323
- For RealPresence OTX Studio systems: Public Switched Telephone Network (PSTN) number

In the following circumstances, call escalation is rejected and the help desk feature is not supported:

- In a Polycom RealPresence Collaboration Server (RMX) SVC conference, you cannot add an audio call to the conference from a RealPresence Group system.
- In a Microsoft CCCP conference, you cannot add a H.323 audio-only call to the conference from a RealPresence Group system.

Enabling Mobile Devices as Controllers

Topics:

In addition to enabling users to control the RealPresence ITP systems with RealPresence Touch, you can also enable users to control the systems with their personal mobile devices.

Pairing Settings

Specify pairing settings to enable touch devices to pair with the system.

Polycom Touch Device

Before your users can control the system with the RealPresence Touch device, you must enable the device on the system's web interface. Once the device is enabled, you can pair it to the system.

1. Select **Enable Polycom Touch Device** to enable the touch device to operate the system.
2. Go to **Diagnostics** > **System** > **Sessions** to view the paired devices.

Calling

Topics:

There are several methods for placing a call. Most require that you have stored information about the contacts you want to call.

Place a Call

You can place a call by dialing manually.

Procedure

1. Select **Manual Dial**.
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.

Call a Speed Dial Contact

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

Procedure

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

Place an Audio-Only Call

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

Procedure

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

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

System Maintenance

Topics:

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

Enable 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.

Procedure

1. Go to **Admin Settings** > **General Settings** > **Options** and enter the key code.
2. 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*.
   - **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.

Upgrade System Software

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

Upgrade Software from a Web Server

If your organization uses a management system for provisioning endpoints, you can enter the server address where software updates are stored to update the system.

Procedure

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**.

Upgrade Software from a Computer

You can download the latest software onto a Windows computer and transfer the update to the RealPresence Immersive Studio system.

Procedure

1. Go to **Admin Settings** > **General Settings** > **Software Updates** > **Manual Software Updates**.
2. Browse to locate the software update package on your computer 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.

Enable Automatic Software Updates

You can set the system to automatically check for and apply software updates. If your organization uses a management system for provisioning endpoints, the RealPresence ITP system can get software updates automatically.

Procedure

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* for information about the latest software version, including version dependencies.

View the Log File Status

You can view the log file status for your system in the system local or web interface.

Procedure

» Do one of the following:

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

Troubleshooting

Topics:

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.

Access System Diagnostics

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

Procedure

1. In your web browser address line, enter the RealPresence ITP 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

Diagnostic Screen	Description
Call Statistics	Displays information about the call in progress. To view more information about a specific stream, navigate to the desired stream and select **More Info**. From an individual stream view you can select **Next Stream** to view the next stream in the stream list.
System Status	Displays system status information.
Download Logs	Enables you to save system log information for each codec using separate web UI on each codec.
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.

Display Call Statistics

You might need to view call statistics on the system local interface to do some troubleshooting for users. You can only view call statistics during a call.

Procedure

» 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
- 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)

Display System Status

You can view the status of the primary, left, and right systems.

Procedure

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

Displays the following system status information. When the status information for three systems in 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
- Display Switcher
- Lighting Controller
- SoundStructure
- VisualBoard Display

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

Download Logs

You can download logs to a specified location on your computer.

Procedure

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

Configure 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.

Procedure

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

Setting	Description
Log Level	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`.

Setting	Description
Enable Remote Logging	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.
Remote Log Server Address	Specifies the server address and port.
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

Setting	Description
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. Select the **Polycom Improvement Program** button to view information about how your data is used.

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

Restart the System

You can restart the system from the web UI.

Procedure

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

Generate the CDR

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

Procedure

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

Information in the Call Detail Report (CDR)

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

Call Detail Report Information

Data	Description for Individual System Report	Description for Aggregated Report
Row ID	Each call is logged on the first available row. A call is a connection to a single site, so there might be more than one call in a conference.	Same as primary system.
Start Date	The call start date, in the format dd-mm-yyyy.	Same as primary system.
Start Time	The call start time, in the 24-hour format hh:mm:ss.	Same as primary system.

Data	Description for Individual System Report	Description for Aggregated Report
End Date	The call end date.	Same as primary system.
End Time	The call end time.	Same as primary system.
Call Duration	The length of the call.	Same as primary system.
Account Number	If **Require Account Number to Dial** is enabled on the system, the value entered by the user is displayed in this field.	Same as primary system.
Remote System Name	The system name of the far site.	Same as primary system.
Call Number 1	Outgoing calls: The number dialed from the first call field, not necessarily the transport address. Incoming calls: The caller ID information from the first number received from a far site.	Combined addresses separated by a semicolon.
Call Number 2 **(If applicable for call)**	Outgoing calls: The number dialed from the second call field, not necessarily the transport address. Incoming calls: The caller ID information from the second number received from a far site.	Same as primary system.
Transport Type	The type of call, either H.323 (IP) or SIP.	Same as primary system.
Call Rate	The bandwidth negotiated with the far site.	Sum of the call rates of the individual calls.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.	Same as primary system.
Call Direction	**In** for calls received. **Out** for calls placed from the RealPresence Immersive Studio system.	Same as primary system.
Conference ID	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.	Same as primary system. Shown as 0 (zero) in this release.

Data	Description for Individual System Report	Description for Aggregated Report
Call ID	Identifies individual calls within the same conference.	Same as primary system.
Total H.320 Channels Used	0 (zero) indicates that the call did not connect. 1 indicates a connected call.	The total number of codecs used in the call.
Endpoint Alias	The alias of the far site.	Same as primary system.
Endpoint Additional Alias	An additional alias of the far site.	Same as primary system.
View Name	Names the web or local interface used in the call.	Same as primary system.
User ID	Lists the ID of the user who placed the call.	Same as primary system.
Endpoint Transport Address	The actual address of the far site, not necessarily the address dialed.	Same as primary system.
Audio Protocol (Tx)	The audio protocol transmitted to the far site, such as G.728 or G. 722.1.	Same as primary system.
Audio Protocol (Rx)	The audio protocol received from the far site, such as G.728 or G. 722.	Same as primary system.
Video Protocol (Tx)	The video protocol transmitted to the far site, such as H.263 or H. 264.	Same as primary system.
Video Protocol (Rx)	The video protocol received from the far site, such as H.261 or H. 263.	Same as primary system.
Video Format (Tx)	The video format transmitted to the far site, such as CIF or SIF.	Same as primary system.
Video Format (Rx)	The video format received from the far site, such as CIF or SIF.	Same as primary system.
Disconnect Local ID and Disconnect Reason	The identity of the user who initiated the call and the reason the call was disconnected.	Same as primary system.
Q.850 Cause Code	The standard Q.850 cause code showing how the call ended.	Same as primary system.
Total H.320 Errors	The number of H.320 errors experienced during the call.	Same as primary system. This value should be 0 (zero).

Data	Description for Individual System Report	Description for Aggregated Report
Average Percent of Packet Loss (Tx)	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.	Average of the individual call numbers.
Average Percent of Packet Loss (Rx)	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.	Average of the individual call numbers.
Average Packets Lost (Tx)	The number of packets transmitted that were lost during an H.323 call.	Sum of packets that were lost in the individual calls.
Average Packets Lost (Rx)	The number of packets from the far site that were lost during an H.323 call.	Sum of packets that were lost in the individual calls.
Average Latency (Tx)	The average latency of packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.	Average of the individual call numbers.
Average Latency (Rx)	The average latency of packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.	Average of the individual call numbers.
Maximum Latency (Tx)	The maximum latency for packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.	Maximum of the individual call numbers.
Maximum Latency (Rx)	The maximum latency for packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.	Maximum of the individual call numbers.
Average Jitter (Tx)	The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.	Average of the individual call numbers.

Data	Description for Individual System Report	Description for Aggregated Report
Average Jitter (Rx)	The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.	Average of the individual call numbers.
Maximum Jitter (Tx)	The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.	Maximum of the individual call numbers.
Maximum Jitter (Rx)	The maximum jitter of packets received during an H.323 call, calculated from sample tests done once per minute.	Maximum of the individual call numbers.
Call Priority	This function is not supported.	

View Room Control Devices

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

Procedure

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

Setting	Description
Status	Specifies the state of the connection. The states are **Connected**, **Not Connected**, and **Unknown**.
IP Address	Specifies the IP address of the device that is being controlled.
Port Number	Specifies the port number for TCPIP connection of the device that is being controlled.