ADMINISTRATOR GUIDE

8.10 | March 2022 | 3725-74900-000F

Polycom RealPresence Collaboration Server 1800/2000/4000/Virtual Edition

Getting Help
For more information about installing, configuring, and administering Poly/Polycom products or services, go to Poly Support.

Poly
345 Encinal Street
Santa Cruz, California
95060

Contents

Before You Begin

Topics:

The Polycom RealPresence Collaboration Server (RMX) Administrator Guide provides instructions to configure and administer your RealPresence Collaboration Server (RMX) 1800, 2000, 4000, and Virtual Edition multipoint control unit (MCU).

Audience, Purpose, and Required Skills

The primary audience for this guide is system administrators and network engineers who configure, maintain, and support the telecommunications infrastructure and video conferencing environment.

Operators and participants assigned to the chairperson role also find task information in this guide useful.

To perform some of the implementation and maintenance tasks described in this guide, the administrator should have basic technical knowledge and skills in the following disciplines:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment
- Virtual machine environments
- Networking, security certificates, and software configuration

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The Poly Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Poly Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The Poly Partner Network is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- The Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration.

- Poly Lens enables better collaboration for every user in every workspace. It is designed to spotlight the health and efficiency of your spaces and devices by providing actionable insights and simplifying device management.
- With Poly+ you get exclusive premium features, insights and management tools necessary to keep employee devices up, running and ready for action.

Privacy Policy

Poly products and services process customer data in a manner consistent with the Poly Privacy Policy. Please direct comments or questions to privacy@poly.com

Getting Started

Topics:

This section provides information on getting started with your RealPresence Collaboration Server and includes the following chapters:

- Polycom RealPresence Collaboration Server Overview
- Network Configuration
- Customizing the User Interface

Polycom RealPresence Collaboration Server Overview

Topics:

The Polycom RealPresence Collaboration Server (RMX) 1800, 2000, 4000, and Virtual Edition multipoint control units (MCUs) are high performance, scalable MCUs that provide a feature-rich, multipoint audio and video conferencing experience.

Polycom RealPresence Collaboration Server Features and Capabilities

The Polycom RealPresence Collaboration Server supports the following audio and video conferencing features.

Supported Features for Conferencing

Feature Name	Description
Polycom Open Collaboration Network	The Polycom Open Collaboration Network (POCN) enables Poly, Microsoft, and Cisco users, within their own environment, to participate in the same conference running on a Polycom RealPresence Collaboration Server. The Polycom RealPresence Collaboration Server also natively interoperates with Cisco Telepresence Systems and Poly Telepresence and video conferencing endpoints, ensuring optimum quality multiscreen, multipoint calls.
Presence in Microsoft Office Communications, Lync, or Skype for Business	Registration and Presence enables Microsoft Lync or Skype for Business users to see user and meeting room status (Available, Busy, or Offline). Users can connect to these contacts and resources directly from the buddy list.
Cascading Conferences	The Polycom RealPresence Collaboration Server can merge multiple conferences into a single conference. This enables Polycom RealPresence Collaboration Servers to split a larger number of participants and resources. Microsoft Lync or Skype for Business users can also connect (via Polycom RealConnect) to a RealPresence Collaboration Server meeting room to a conference running on the Microsoft AVMCU.

Feature Name	Description
Content Sharing	The Polycom RealPresence Collaboration Server supports sharing of documents, presentations, videos, or other content with conference participants. HD H.264 Content and H.264 Content for Cascading links allow conference participants to receive high-quality content in both standard conferences and cascaded conferences.
Video Preview	The Polycom RealPresence Collaboration Server enables you to preview video and the video quality sent and received by participants and the conference. This enables users to identify possible quality degradation. The Polycom RealPresence Collaboration Server supports H.264 High Profile with video preview.
Indicators	The Polycom RealPresence Collaboration Server offers different types indicators and allows you to design the layout of those indicators on some participant's screens: • Network Quality - Indicates the quality of the video channels • Recording - Indicates that the system is recording the conference • Audio and Video Participants - Identifies the number of audio and video participants in the conference (AVC only)
Auto Scan and Customized Polling in Video Layout	The Polycom RealPresence Collaboration Server enables you to define a single cell in the conference layout to cycle the display of participants that aren't in the conference layout.
Packet Loss Compensation - Polycom LPR and DBA	Polycom Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA) help minimize media quality degradation that can result from packet loss in the network. The Polycom LPR algorithm uses Forward Error Correction (FEC) to create additional packets that contain recovery information. DBA allocates the bandwidth needed to transmit the additional packets.
Lecture Mode	Lecture Mode enables all participants to view the lecturer in full screen while the conference lecturer sees all the other conference participants in the selected layout. When the number of sites or endpoints exceeds the number of video windows in the layout, the system switches among participants every 15 seconds.
Poly NoiseBlock technology	The Polycom RealPresence Collaboration Server automatically detects and mutes AVC endpoints that have a noisy audio channel.

Related Links

Preview a Participant's Video on page 186
Change Position of the Conference Indicators on page 154
Designate a Participant as the Lecturer in an Active Conference on page 185

Required Software Components

This section lists the Required Software Components for RealPresence Collaboration Server.

The required software components for RealPresence Collaboration Server are as follows:

RealPresence Collaboration Server Version	Required Software Components
RealPresence Collaboration Server 1800/2000/4000	• .Net Framework 3.5 SP1 or higher is required and installed automatically. • Internet Explorer to allow the running of Signed ActiveX.
RealPresence Collaboration Server, Virtual Edition	• .Net Framework 2.0 SP1 or higher is required and installed automatically. • Internet Explorer must be enabled to allow the running of Signed ActiveX. If ActiveX installation is blocked, see ActiveX Bypass.

System User Types

RealPresence Collaboration Server users are identified by their role and associated authorization level, which determines the user's capabilities within the system.

RealPresence Collaboration Server users have authorization to access the MCU interface. RealPresence Collaboration Server supports the following user authorization levels:

- Administrator
- Administrator read-only
- Operator
- Chairperson
- Auditor

Note: You can associate user names with servers (machines) to ensure that all users are subject to the same account and password policies, but the system doesn't treat these user names as a distinct user type.

RealPresence Collaboration Server doesn't consider conference participants to be users because they don't interact directly with the system itself. However, you can store conference participant information in the RealPresence Collaboration Server address book for conference scheduling and management purposes.

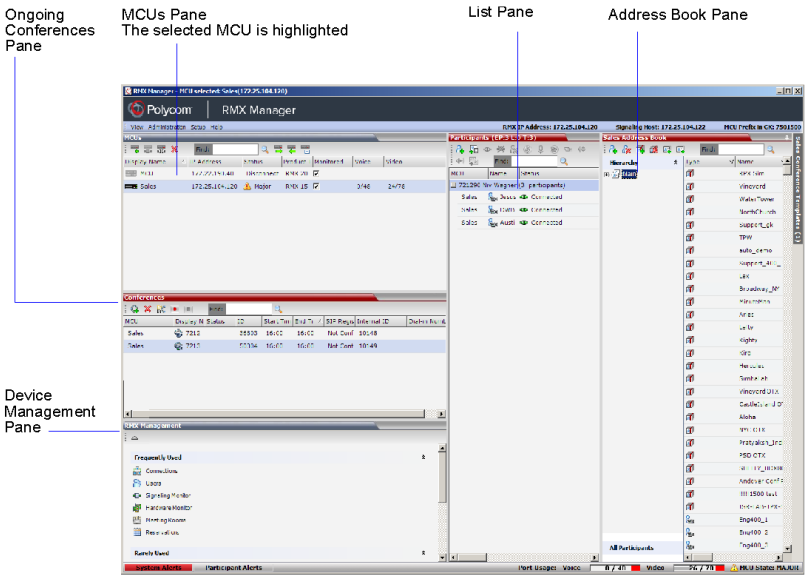
Navigating the System

Manage and monitor the Polycom RealPresence Collaboration Server with either the RMX Manager application or the RMX Web Client using Internet Explorer.

In general, the tasks documented in this guide apply to both RMX Manager and the RMX Web Client, but the document concentrates on the RMX Manager interface.

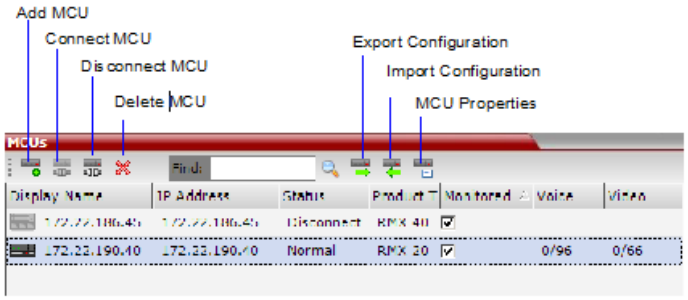
After connecting to a server, you can see the RMX Manager main screen. The RMX Manager main screen and the RMX Web Client main screen are similar except RMX Manager contains an MCU section. This section manages multiple MCUs. RMX Manager displays the Polycom RealPresence Collaboration Server functions based on the authorization level of the user.

The MCU section is available to all users. You can select only one Polycom RealPresence Collaboration Server in the MCU section. It contains the menu items, server management, address book, conference templates, and all properties of that particular MCU.



The MCU Pane

The MCU pane includes the MCU list and an MCU toolbar.



For each listed Polycom RealPresence Collaboration Server, the system displays the following information:

MCU Menu	Description
MCU Display Name	The name of the Polycom RealPresence Collaboration Server and its icon according to its type and connection status.
IP Address	The IP address of the Polycom RealPresence Collaboration Server.
Status	The MCU status: • Connected: The MCU is connected to RMX Manager and can be managed by an RMX Manager user. • Disconnected: The MCU is disconnected from RMX Manager. • Major: The MCU has a major problem. The MCU behavior is affected and proper attention is required.
Product Type	The Polycom RealPresence Collaboration Server type: **RMX 1800/2000/4000/800VE**. Before connecting to the MCU for the first time, the Polycom RealPresence Collaboration Server type is unknown and so **RealPresence Collaboration Server (RMX)** is displayed as a general indication.
Monitored	When selected, indicates that the conferences running on this MCU are automatically added to the conferences list and monitored. To stop monitoring the conferences running on this MCU and the participants, clear the **Monitored** check box.
Video Resources	The number of video resources available for conferencing.
Audio Resources	The number of audio resources available for conferencing.

MCU Icons and States

This section lists the MCU Icons and States.

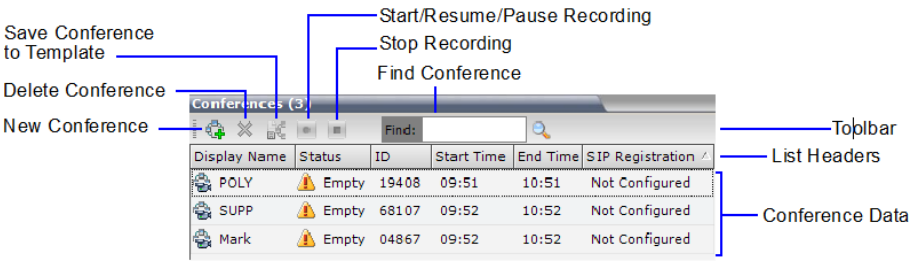
The MCU icons and states are as follows:

MCU Icon	Description
	Polycom RealPresence Collaboration Server (RMX) 2000, disconnected
	Polycom RealPresence Collaboration Server (RMX) 2000, connected
	Polycom RealPresence Collaboration Server (RMX) 4000, disconnected
	Polycom RealPresence Collaboration Server (RMX) 4000, connected
	Polycom RealPresence Collaboration Server 1800, disconnected
	Polycom RealPresence Collaboration Server 1800, connected
	Polycom RealPresence Collaboration Server, Virtual Edition, disconnected
	Polycom RealPresence Collaboration Server, Virtual Edition, connected

Conferences List

The Conferences List includes all the conferences currently running on the MCU along with the Status, Conference ID, Start Time, and End Time data.

The number of ongoing conferences is displayed in the title of the pane.



Conferences List Toolbar Options

This section lists the Conferences List Toolbar Options.

If you're logged in as an operator or administrator, then the toolbar options are as follows:

Conferences List Toolbar Options

Toolbar Option	Permission Role
New Conference	• Operator • Administrator
Delete Conference	• Operator • Administrator
Save Conference to Template	• Operator • Administrator
Start/Resume/Pause Recording	• Operator • Administrator
Stop Recording	• Operator • Administrator
Find Conference	• Operator • Administrator
Chairperson Password	Chairperson only
Refresh	Chairperson only

System Status Bar

The Status Bar is available to operators and administrators to display the system alerts, participant alerts, port usage gauges, and MCU state indicator.

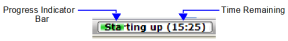
The information included in the status bar varies with the product model.

MCU State Indicator

The MCU State Indicator is available to chairpersons, operators, and administrators.

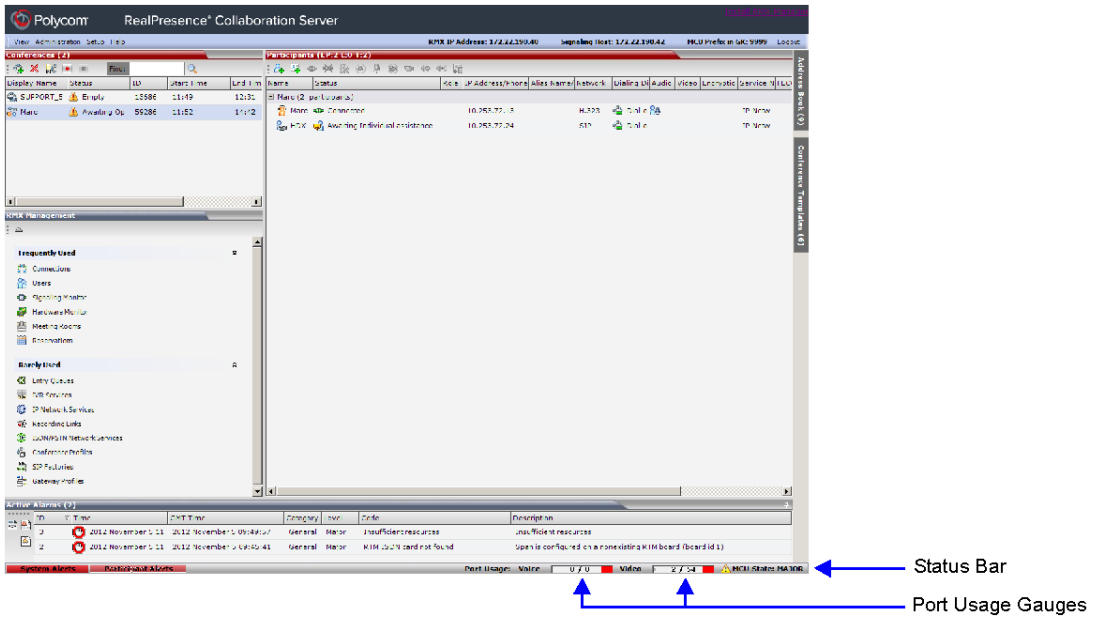
The MCU State indicator displays one of the following:

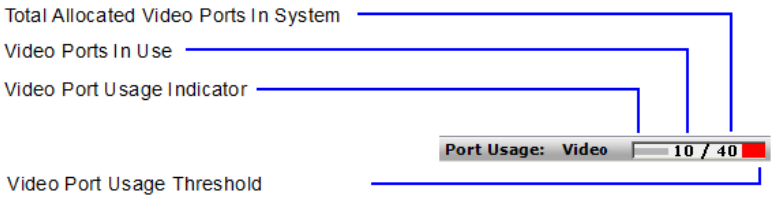
MCU State Indicator

Option	Description
	The MCU is starting up. The time remaining until the system start-up is complete. The Time remaining is displayed within parentheses. The blue progress indicator bar indicates the start-up progress. 
	The MCU is functioning normally.
	The MCU has a major problem. The MCU behavior could be affected and attention is required.

Port Usage Gauges

The Port Usage Gauges are displayed on the status bar at the bottom of the interface.





For Polycom RealPresence Collaboration Server 1800/2000/4000, the Port Usage Gauge displays the following:

- Total number of video or voice ports

  The port information in the system according to the video or voice port configuration. The Audio gauge is displayed only if audio ports are allocated by the administrator, otherwise only the video port gauge is displayed.
- Number of video and voice ports in use
- High port usage threshold

For Polycom RealPresence Collaboration Server, Virtual Edition, the Port Usage Gauge displays the following:

- Total number of video ports in the system
- Number of video ports in use
- High port usage threshold

The basic unit used for reporting resource usage in the Port Gauges is HD720p30. Usage numbers are rounded to the nearest integer.

List Pane

The List Pane displays details of the item selected in the Conferences pane or RMX Management pane.

The title of the pane changes according to the selected item.

Example: When an ongoing conference is selected in the Conferences pane, the list and parameters of the connected participants is displayed.

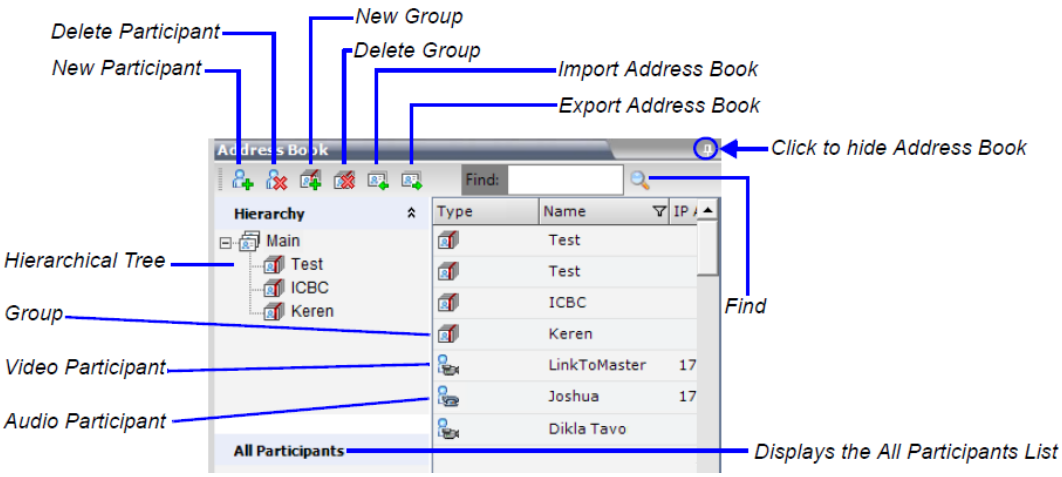
Selecting an item in the RMX Management pane lists the items currently defined.

Example: If the Users item is selected, a list of system users defined for the MCU is displayed.

Address Book

The Address Book is available to chairpersons, operators, and administrators.

The Address Book displays a list of participants and groups that are defined on the MCU. The information in the Address Book can be modified only by an administrator. All system users can view and use the Address Book to assign participants to conferences. The **Quick Search** field displays all the available options in the Address Book.



The **Address Book** has two sections.

- The **Hierarchy** section displays a hierarchy of groups, which provides an easy way to manage a collection of participants and their associated endpoints. For example, if you frequently conduct conferences with the marketing department, create a group called "Marketing Team" that contains the endpoints of all members of the marketing team. Double-clicking a group on the navigation pane displays the group participants and sub-groups in the **List** pane.
- The **All Participants** section displays the single unique entity of all the participants in a single level. When adding a participant to a group, the system adds a link to the participant's unique entity that is stored in the All Participants list. The same participant may be added to many groups at different levels, and all these participant links are associated with the same definition of the participant in the **All Participants** list. If the participant properties are changed in one group, they will be changed in all groups.

The **Participants List** in the Address Book displays the following information for each participant:

Field/Option	Description
Type	Indicates whether the participant is a video ( ) or voice ( ).
Name	Displays the name of the participant.
IP Address/Phone	Enter the IP address of the participant's endpoint. • For H.323 participant, define either the endpoint IP address or alias. • For SIP participant, define either the endpoint IP address or the SIP address. **Note:** This field is removed from the dialog box when the ISDN (audio/video) protocol is selected.
Network	The network communication protocol used by the endpoint to connect to the conference: • H.323 • SIP • ISDN (audio/video)

Field/Option	Description
Dialing Direction	**Dial-in** - The participant dials in to the conference. **Dial-out** - The RealPresence Collaboration Server dials out to the participant.
Encryption	Indicates whether the endpoint uses encryption for its media. The default setting is **Auto**, indicating that the endpoint must connect according to the conference encryption setting.

On first access, the RMX **Address Book** appears on the main **RMX Manager** page. You can hide the Address Book pane by clicking the anchor pin. The Address Book pane closes and a tab appears at the right edge of the screen. If it's hidden, double-click the **Address Book** tab on the right to unhide it.

RMX Management Pane

The RMX Management pane is available to operators and administrators.

The RMX Management pane lists the entities that are to be configured to enable the Polycom RealPresence Collaboration Server to run conferences. Only users with administrators permission can modify these parameters.

The RMX Management pane is divided into two sections:

- **Frequently Used** - Parameters often configured, monitored, or modified.
- **Rarely Used** - Parameters configured during initial system setup and rarely modified afterward.

You can toggle between toolbar and list views in the RMX Management pane, and you can move items within and between the frequently used and rarely used sections by dragging icons of the item to the appropriate position.

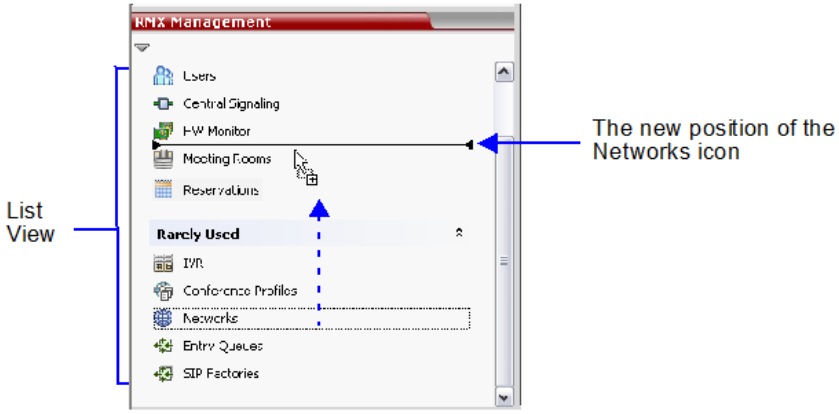
In list view, you can toggle items between the **Frequently Used** and **Rarely Used** sections depending on the operations you most commonly perform and the way you prefer to work with the RMX Web Client. This option doesn't work in toolbar view as all items are represented by icons.

Conference Template Tab

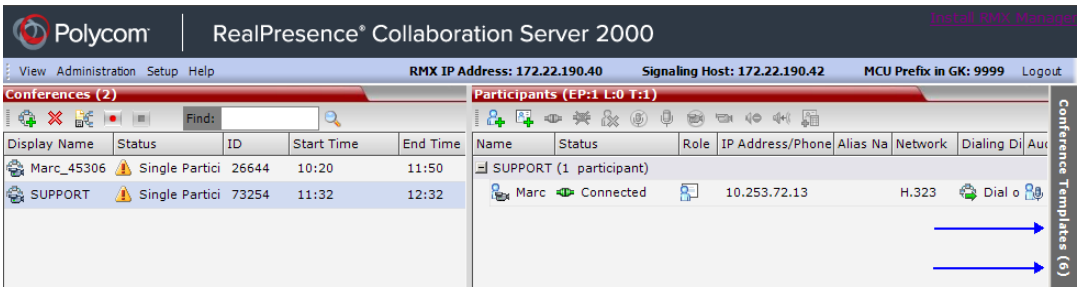
Administrators and operators can create, save, schedule, and activate identical conferences using conference templates.

A conference template does the following:

- Saves the conference profile
- Saves all participant parameters including the Personal Layout and Video Forcing settings
- Simplifies telepresence conference setup where precise participant layout and video forcing settings are crucial



The MCU initially displays the conference templates list as a closed tab in the RMX Manager main screen. The tab indicates the number of saved conference templates.



Toolbar Buttons

The list of the **Conference Template** toolbar and the **Conferences List** toolbar buttons is given here.

The **Conference Template** toolbar includes the following buttons:

Conference Templates - Toolbar Buttons

Button	Description
New Conference Template	Creates a new Conference Template.
Delete Conference Template	Deletes one or more Conference Templates that are selected in the list.
Start Conference from Template	Starts an ongoing conference from the Conference Template that has an identical name, ID, parameters, and participants as the template.
Schedule Reservation from Template	Creates a conference Reservation from the Conference Template with the same name, ID, parameters, and participants as the Template. Opens the **Scheduler** dialog box enabling you to modify the fields required to create a single or recurring Reservation based on the template.

The **Conferences List** toolbar includes the following button:

Conferences List - Toolbar Button

Button	Description
 Save Conference to Template	Saves the selected ongoing conference as a Conference Template.

Accessibility Features

Poly products include a number of features to accommodate users with disabilities.

Accessibility Feature	Description
Screen reader capable	Users who have limited or low vision can access the RMX Manager software using a screen reader and a mouse.
Natively integrated software zoom	Users can zoom the software size to 150%.
Hardware status indicators (RMX 1800, 2000, and 4000 only)	LED indicators provide status and functionality information on the hardware interface.
Software status indicators	Graphic and text information provide status and functionality in the software interface.
Language settings	Users can change the software user interface to a natively integrated, supported language.

Network Configuration

Topics:

You configured most of the basic network settings for the RealPresence Collaboration Server during initial set up using the Fast Configuration Wizard.

Configure additional network settings or integrate with other systems (if supported by your deployment) before you use RealPresence Collaboration Server. For more information on network configuration or advanced network options, see the *Polycom RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Technical Reference*.

Supported Network Configurations

This section lists the Supported Network Configurations

The RealPresence Collaboration Server supports the following conferencing network configurations:

- IP conferencing network
- ISDN (audio/video) conferencing network
- Multipoint conferencing network

IP Conferencing Network

Typically, the RealPresence Collaboration Server 2000 and RealPresence Collaboration Server, Virtual Edition use a single LAN port for system management, signaling, and IP conferencing.

You can separate the management and signaling networks when deploying RealPresence Collaboration Server 2000 into Maximum Security Environments.

The RealPresence Collaboration Server 1800 and RealPresence Collaboration Server 4000 use separate LAN ports for system management and IP conferencing.

ISDN (Audio/Video) Conferencing Network

To enable ISDN-video and ISDN-voice participants to connect to the MCU, you must define an ISDN (audio/video) network service.

You can define only two ISDN (audio/video) network services of the same Span Type (E1 or T1). Each network service can attach spans from either or both cards.

The following systems support ISDN audio/video networks:

- RealPresence Collaboration Server 1800 with three DSP cards
- RealPresence Collaboration Server 2000
- RealPresence Collaboration Server 4000

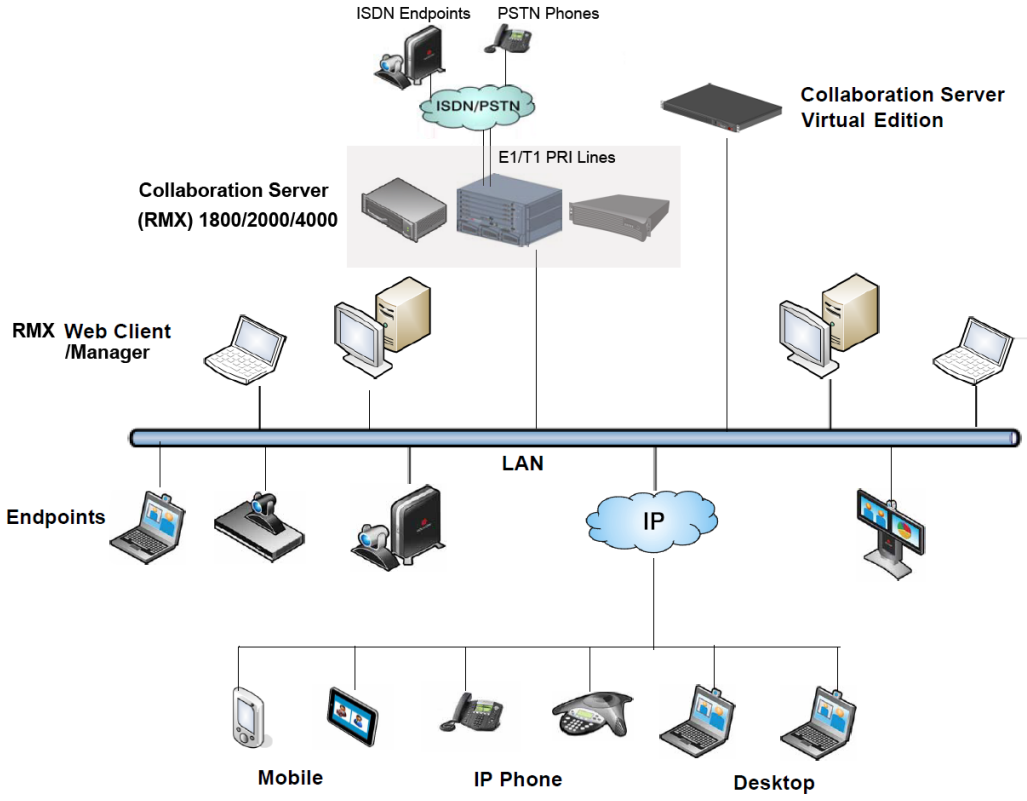
You configure most of the parameters of the first ISDN (audio/video) network service in the Fast Configuration Wizard, which runs automatically if the system detects an RTM ISDN card during first-time setup.

For more information, see the *Polycom RealPresence Collaboration Server (RMX) 1800/2000/4000/ Virtual Edition Getting Started Guide*.

Multipoint Conferencing Network

The following figure describes the multipoint conferencing network using the RealPresence Collaboration Server.

Figure 1: Multipoint Video Conferencing using a RealPresence Collaboration Server



Installing the RMX Manager Software

You can download and install the RMX Manager software from Poly Online Support Center or through the RealPresence Collaboration Server system web interface.

Download and Install the RMX Manager through Poly Online Support Center

You can download the RMX Manager software from Poly Online Support Center and install it on your local computer system.

Poly recommends using Microsoft Internet Explorer to download the RMX Manager software.

Procedure

1. Go to the Collaboration & Conferencing Platforms page at Poly Online Support Center.
2. Click the link for your RealPresence Collaboration Server (RMX) version's support page.
3. Select the appropriate software version of the **Local Web Client (RMX Manager)** in the **Current Releases** tab.
4. Accept the **End User License Agreement** and the **Export Restrictions Agreement**.
5. Click **Open** to launch the .zip file after it downloads.
6. Go to `RMX_x-x-x-xxx_LocalWebClient_RMXManager\RmxManagerInstallerMsi` and launch `setup.exe`.
7. Follow the directions in the install wizard to complete the software installation.

Download and Install RMX Manager from the System Web Interface

You can download and install the RMX Manager using the system web interface.

You must use Internet Explorer to download the software through the system web interface.

Procedure

1. Open Internet Explorer and go to `http://<Collaboration Server IP Address>/RMXManager.html`.

   The RMX Manager installation page displays.
2. Click **Install**.

   The installer verifies the application's requirements on the workstation.

   The application launches after your system completes the installation.

RealPresence Collaboration Server Network Port Usage

The following table summarizes the port numbers and their usage in the RealPresence Collaboration Server.

RealPresence Collaboration Server Network Port Usage

Connection Type	Port Number	Protocol	Description	Configurable
HTTP	80	TCP	Management between the RealPresence Collaboration Server and RMX Manager	No
HTTPS	443	TCP	Secured management between the RealPresence Collaboration Server and RMX Manager	No
DNS	53	HW - UDP VE - TCP	Domain name server	Disable in the IP network service
DHCP	68	HW - UDP VE - TCP	Dynamic Host Configuration Protocol	Disable in the IP network service
SSH	22	TCP	The RealPresence Collaboration Server terminal SSH is not supported when the Collaboration Server is in Ultra Secure Mode	No
NTP	123	UDP	Enables access to a time server on the network	No
H.323 GK RAS	1719	UDP	Gatekeeper RAS messages traffic	No
H.323 Q.931	1720 - incoming; 49152-59999 - outgoing	TCP	H.323 Q.931 call signaling Each outgoing call has a separate port that is allocated dynamically	Yes - for outgoing calls only Configure in the **Fixed Ports** section of the IP network service
H.323 H.245	49152 - 59999	TCP	H.245 control Each outgoing call has a separate port that is allocated dynamically It can be avoided by tunneling	Yes - for outgoing calls only Configure in the **Fixed Ports** section of the IP network service

Connection Type	Port Number	Protocol	Description	Configurable
SIP server	5060, 60000	UDP, TCP	Connection to the SIP Server Sometimes port 60000 is used when the system cannot reuse the TCP port This port can be set in the Central signaling (CS) configuration file	Yes - in the IP network service
SIP Outbound proxy	5060, 60000	UDP, TCP	Connection to the SIP outbound proxy Sometimes port 60000 is used when the system cannot reuse the TCP port This port can be set in the Central signaling (CS) configuration file	Yes - in the IP network service
SIP-TLS	60002	TCP	Required for Binary Floor Control Protocol (BFCP) functionality for SIP People+Content content sharing	No - port is not opened if SIP People+Content is disabled
RTP	49152 - 59999	UDP	RTP media packets The ports are dynamically allocated	Yes - Configure in the **Fixed Ports** section of the IP network service
RTCP	49152 - 59999	UDP	RTP control The ports are dynamically allocated	Yes - Configured in the **Fixed Ports** section of the IP network service
SIP -TLS	5061	TCP	SIP -TLS for SIP server and outbound proxy	No
Main MCU - API 1st Connection	4505,4506	TCP	Salt API Note: Applicable only to Modular MCU mode	Not configurable
Main MCU - API 2nd Connection	10020	TCP	Soft Blade API Note: Applicable only to Modular MCU mode	Not configurable
Soft Blade - API 1st Connection	32768 - 61000	TCP	Salt API Note: Applicable only to Modular MCU mode	Not configurable
Soft Blade - API 2nd Connection	32768 - 61000	TCP	Soft Blade API Note: Applicable only to Modular MCU mode	Not configurable

Integrate with the Poly Clariti Manager System

If your organization has the Poly Clariti solution, integrate your RealPresence Collaboration Server with the Poly Clariti Manager system and set it to use as the device (endpoint and server) application manager.

The Poly Clariti Manager system can also manage users and conference participants.

For more information, see the *Poly Clariti Manager Operations Guide*.

Before you integrate, add the MCUs to the Poly Clariti Manager system.

If your organization uses the Poly Clariti Manager system Global Address Book for conference and endpoint management, add a user account on the Clariti Manager that the RealPresence Collaboration Server can use as its machine integration account. Write down the user name and password for the machine integration account. You need this information for configuring the required system flags.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, click **New Flag**.
3. To enable machine integration with the Poly Clariti Manager system, add and configure the **EXTERNAL_CONTENT_DIRECTORY**, **EXTERNAL_CONTENT_IP**, **EXTERNAL_CONTENT_PASSWORD**, and **EXTERNAL_CONTENT_USER** system flags.
4. To allow endpoints included in a cascaded conference to display content (sometimes called content snatching), add the **ENABLE_CONTENT_SNATCH_OVER_CASCADE** system flag and set its value to `YES`.
5. For environments that include NAT Firewall deployments, add the **NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT** system flag and set its value to 3.
6. Click **OK** and when prompted, click **Yes**.

   After the RealPresence Collaboration Server resets, RealPresence Collaboration Server (RMX) users can access this GAB to add participants to conferences. However, the RealPresence Collaboration Server uses the Global Address Book in read-only mode, which means you must add or modify Address Book entries on the Poly Clariti Manager.

Related Links

System Flags on page 264
Configuring the Address Book on page 159

Integrate with the Poly Clariti Core or Poly Clariti Edge System

If your organization has the Poly Clariti solution, integrate your RealPresence Collaboration Server with the Poly Clariti Core or Poly Clariti Edge system and set it up as the call control for the conferencing network.

Configure the Poly Clariti Core or Poly Clariti Edge system as the H.323 gatekeeper and/or SIP server, endpoint registrar, and virtual meeting room manager.

Procedure

1. If not already done, add the RealPresence Collaboration Servers and the Poly Clariti Core or Poly Clariti Edge system as device instances to the Poly Clariti Manager system.
2. In RMX Manager, go to **RMX Management** > **Rarely Used** > **IP Network Services**.
3. From **IP Network Services**, double-click **Default IP Service** and select the required **IP Network Type**: **H.323** or **H.323 & SIP**.
4. Go to **Gatekeeper** tab and from the **Gatekeeper** drop-down list, select **Specify**.
5. Enter either the Poly Clariti Core system's **IP Address or Name** (as registered in the DNS).
6. As required, enter the **IP Address or Name** for an alternate backup gatekeeper.
7. Enter the **MCU Prefix in Gatekeeper** number, which is the number this network service uses to register with the Poly Clariti Core or Poly Clariti Edge gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU.
8. Complete the other fields as required and then click **OK**.

Integrate with HARMAN Media Suite

RealPresence Collaboration Server can dial out to a HARMAN Media Suite (previously Polycom RealPresence Media Suite) for conference recording if you first establish a dial-out Recording Link, which is a dial-out connection from the MCU to the HARMAN Media Suite.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Recording Links** ().
2. In the **Recording Links** list, click **New Recording Link** ().
3. Define the following recording link parameters:

Recording Link Parameters

Parameter	Description
Name	A unique descriptive name to identify to the virtual recording room (VRR) on the HARMAN Media Suite.
Type	Select the network environment: H.323 or SIP
IP Address	• If no H.323 gatekeeper is configured, enter the IP Address of the HARMAN Media Suite. • If an H.323 gatekeeper is configured, enter its IP address or alias. • If a SIP server is configured, enter its IP address.

Parameter	Description
Alias Name	If using the endpoint alias instead of the IP address, first select the alias type and then enter the endpoint alias. The name should be the same as HARMAN Media Suite registration information. If the recording link defines the VRR, enter the RealPresence Media Suite E.164 +VRR in the Alias Name. If the recording link doesn't define the VRR, enter the HARMAN Media Suite E. 164 that registers to the Poly Clariti Core or Poly Clariti Edge system as the Alias Name. The default VRR is used for recording. If you're associating this recording link to a VRR on the HARMAN Media Suite, define the alias as follows: • If using the HARMAN Media Suite IP address, enter the VRR number as the Alias Name. For example, if the VRR number is 5555, enter `5555`. • If the Alias Type is set to **H.323 ID**, enter the HARMAN Media Suite IP address and the VRR number in the format: `<Media Suite IP Address>##<VRR number>` For example: If the Media Suite IP is 173.26.120.2 and the VRR number is 5555, enter `173.26.120.2##5555` • If the Alias Type is set to **E.164**, enter the HARMAN Media Suite E.164 followed by VRR number:<Media Suite E.164><VRR number> For example: If the HARMAN Media Suite E.164 is 123456 and the VRR number is 5555, enter `1234565555`.
Alias Type	Depending on the format used to enter the information in the IP address and Alias fields, select **H.323 ID** or **E.164** (for multiple Recording links). **E-mail ID** and **Participant Number** are also available.

4. Click **OK**.

IP Network Services

IP network services enable RealPresence Collaboration Server to function within IP network environments.

IP network services encompass the network parameters required for the MCU to connect with other IP devices on the same network or outside the network through a firewall. These services require definition on system onset.

Warning: Set Up IP Network Services on Virtual Edition MCUs Only Using the Text User Interface

Create or modify IP Network Services on Polycom RealPresence Collaboration Server, Virtual Edition **only** using the text user interface. Only view these settings when using RMX Manager. If you attempt to modify these settings using RMX Manager, you may experience extreme consequences to the point of blocking access to or usage of the RealPresence Collaboration Server.

IP Network Services Overview

Two IP Network Services are defined for the RealPresence Collaboration Server.

The two IP Network Services are:

- Management Network Service
- Default IP Service (Conferencing Service)

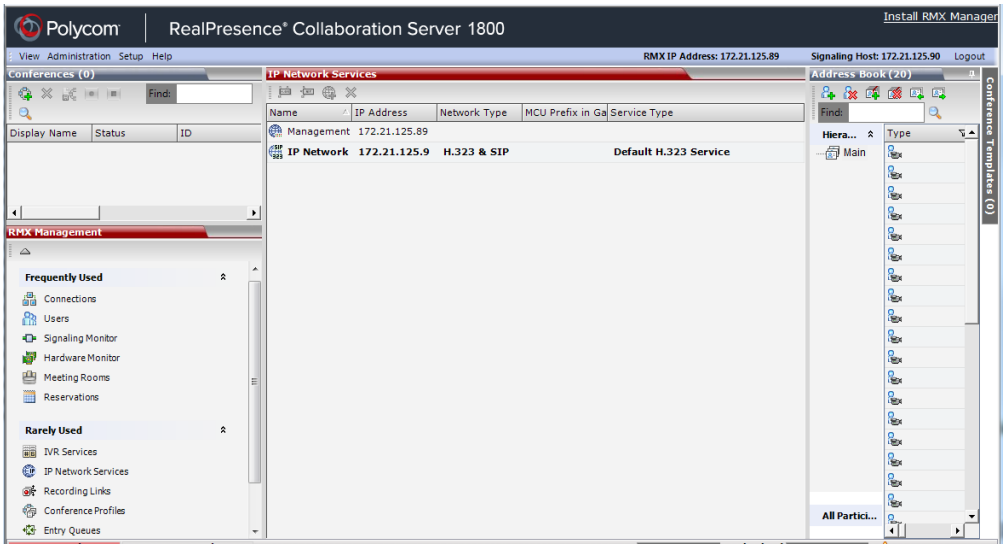
Connection between the RealPresence Collaboration Server management applications (RMX Manager) and participant connections to conferences (dial-in/dial-out) are supported within IPv4, IPv6, and IPv6 & IPv4 IP addressing environments.

When IPv4 is selected, IPv6 fields are hidden, and conversely when IPv6 is selected, IPv4 fields are hidden. When IPv6 & IPv4 is selected both IPv6 and IPv4 fields are displayed.

Note: For the purposes of comprehensive documentation, all screen captures in this chapter pertaining to RealPresence Collaboration Servers display dialog boxes with IPv6 & IPv4 selected.

When the RealPresence Collaboration Server is configured for IPv4 and IPv6 addressing, the addition of the sdp-anat option tag in the SIP Require and SIP Supported headers allows a mixture of IPv4 and IPv6 addressing to be specified by the Session Description Protocol (SDP).

The IP Network Services are configured by selecting IP Network Services (under the Rarely Used menu) in the RMX Management section of the RMX Manager application.



Management Network Service (Primary)

The Management Network is used to connect between the Collaboration Server and the management applications (RMX Manager application) and enable these applications to control the MCU.

The Management Network contains the network parameters, such as the IP address of the MCU's control unit, responsible for connecting the Collaboration Server with the management applications, such as RMX Manager. This IP address can be utilized by the administrator to connect to the control unit should the MCU become corrupted or inaccessible.

In Collaboration Servers 2000/4000/1800, during First Time Power-up, the Management Network parameters can be set either via a USB key or by using a cable to create a private network. For more

information, see First Entry Power-up and Configuration in Polycom RealPresence Collaboration Server Getting Started Guide, and Appendix - Direct Connections to the Collaboration Server.

In Virtual Edition Collaboration Server:

- With DHCP available - The Management Network parameters are automatically set during First Time Power-up and whenever the Collaboration Server is restarted.
- With no DHCP available - The Management Network properties must be set manually via the text user interface described in Modifying Network Settings Using TUI.

Default IP Service (Conferencing Service - Media and Signaling)

The Default IP Service (media and signaling) is used to configure and manage communications between the RealPresence Collaboration Server and conferencing devices such as endpoints, gatekeepers, SIP servers, etc.

The Default IP Service contains parameters for:

- Signaling Host IP Address
- External conferencing devices

Calls from all external IP entities are made to the Signaling Host, which initiates call set-up, and in RealPresence Collaboration Servers 2000/4000, assigns the call to the appropriate media card.

Conferencing related definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the Default IP Service is configured by the Fast Configuration Wizard, which runs automatically upon:

- First time power-up.
- Deletion of the Default IP Service, followed by a system reset.

For more information, see First Entry Power-up and Configuration in the *Polycom RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Getting Started Guide*.

Using IPv6 Networking Addresses for RealPresence Collaboration Server Internal and External Entities

IPv6 addresses can be assigned to both RealPresence Collaboration Server (Internal) and External Entity addresses.

RealPresence Collaboration Server Internal Addresses (Default Management Network Service):

- Control Unit
- Signaling Host
- Shelf Management
- MPM1 and MPM2 (media cards in RealPresence Collaboration Servers 2000/4000) - Separately

External Entities:

- Gatekeepers (Primary & Secondary)
- SIP Proxies on RMX Manager
- DNS Servers
- Default Router
- Defined participants

IPv6 Addressing Guidelines

Use the following guidelines with IPv6 addressing.

- Minimum Internet Explorer 7 is required for the RMX Manager to connect to the RealPresence Collaboration Server using IPv6.
- The default IP address version is IPv4.
- The IP address field in the Address Book entry for a defined participant can be either IPv4 or IPv6. A participant with an IPv4 address cannot be added to an ongoing conference while the Collaboration Server is in IPv6 mode nor can a participant with an IPv6 address be added while the Collaboration Server is in IPv4 mode.

  An error message, indicating Bad IP address version, is displayed and the New Participant dialog box remains open so that the participant's address can be entered in the correct format.
- Participants that do not use the same IP address version as the Collaboration Server in ongoing conferences launched from Meeting Rooms, Reservations and Conference Templates, are disconnected. An error message, indicating Bad IP address version, is displayed.
- IP Security Protocols (IPSec) are not supported.

Management Network

Warning: Use the description below ONLY for viewing the RealPresence Collaboration Server, Virtual Edition, IP Network Services. To modify it, lookup Modifying Network Settings Using TUI.

The Management Network parameters must be modified if you want to:

- Directly connect to the RealPresence Collaboration Server from a workstation
- Modify routes
- Modify DNS information
- In RealPresence Collaboration Server, Virtual Edition - modify DHCP availability

---

Note: Changes made to any of these parameters only take effect when the RealPresence Collaboration Server is reset. An Active Alarm is created when changes made to the system have not yet been implemented and the MCU must be reset.

Figure 2: Management Network Properties - Collaboration Servers 2000/4000

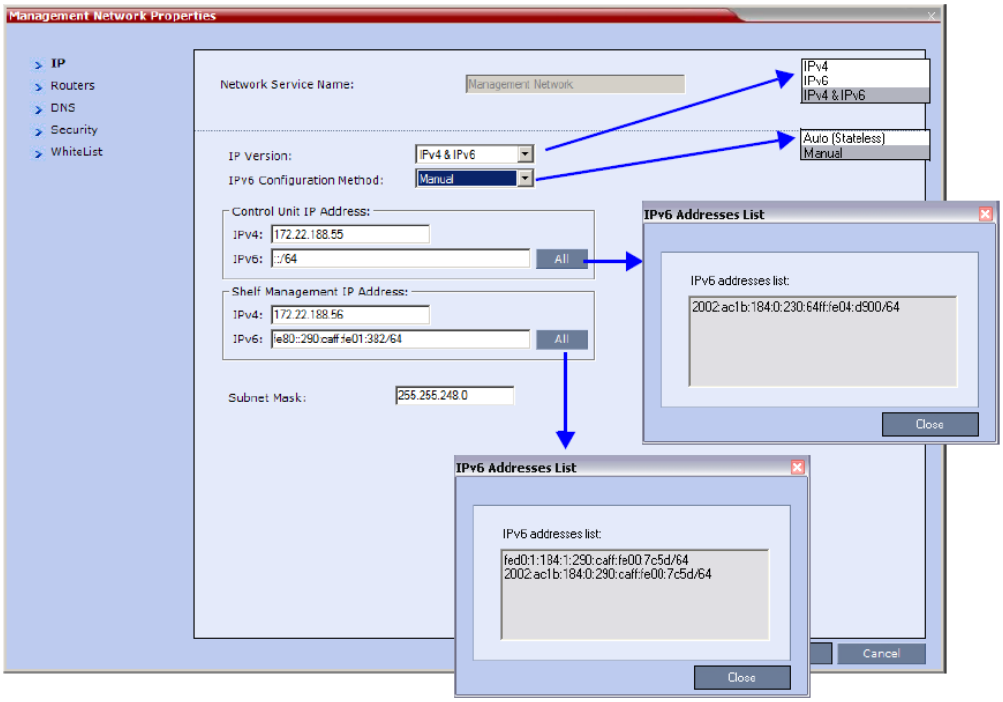


Figure 3: Management Network Properties - Collaboration Server 1800

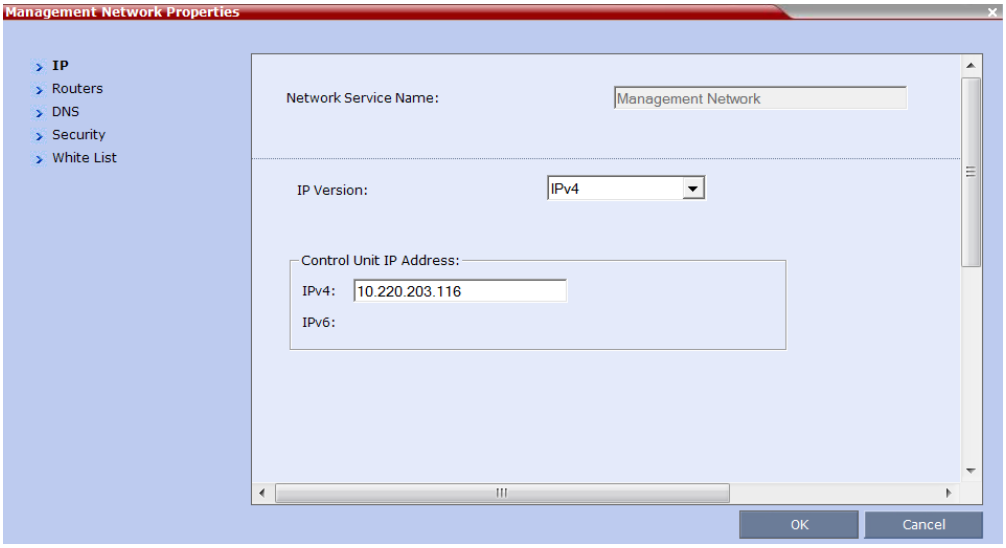
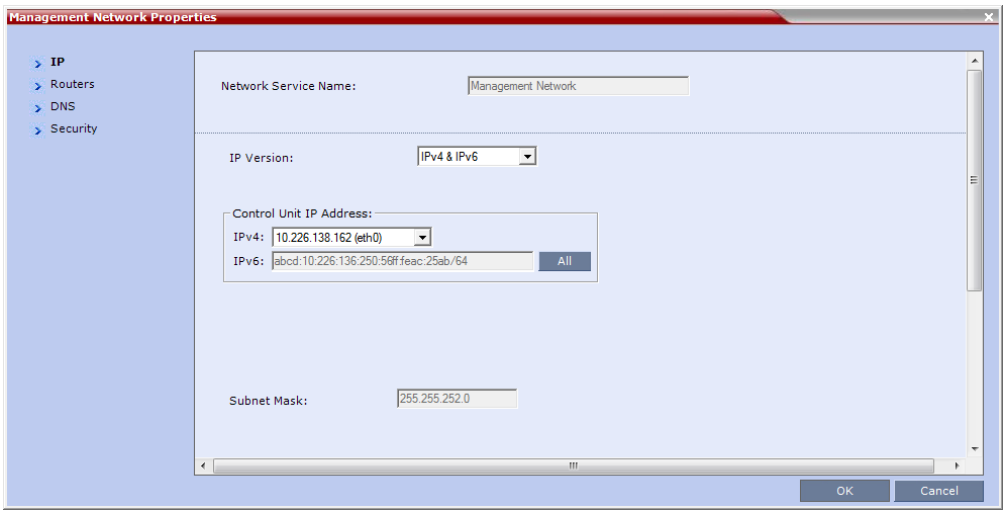


Figure 4: Management Network Properties - Collaboration Server Virtual Edition



The following fields can be viewed or modified (in RealPresence Collaboration Server Virtual Edition - viewed only):

Default Management Network Service – IP Tab

Field	Description	
Network Service Name	Displays the name of the Management Network. This name cannot be modified. **Note:** This field is displayed in all Management Network Properties tabs.	
IP Version	IPv4	Select this option for IPv4 addressing only. **Note:** This is the only addressing mode supported in Collaboration Server 1800.
	IPv6	Select this option for IPv6 addressing only.
	IPv4 & IPv6	Select this option for both IPv4 and IPv6 addressing. **Note:** If the gatekeeper cannot operate in **IPv6** addressing mode, the **H323_RAS_IPV6** System Flag should be set to **NO**. For more information see The CS System Flags.

Field	Description	
IPv6 Configuration Method **(Collaboration Servers 2000/4000 only)**	Auto (Stateless)	Select this option to allow automatic generation of the following addresses: • Link-Local (For internal use only) • Site-Local • Global
	Manual (recommended with IPv6)	Select this option to enable manual entry of the following addresses: • Site-Local • Global Manual configuration of the following address types is not permitted: • Link-Local • Multicast • Anycast
Control Unit IP Address	IPv4	The IPv4 address of the Collaboration Server. This IP address is used by the RMX Manager to connect to the Collaboration Server.
	IPv6 (Not in Collaboration Server 1800)	The IPv6 address of the MCU. This IP address is used by the RMX Manager to connect to the Collaboration Server. **Note:** Internet Explorer 7 is required for the RMX Manager to connect to the MCU using IPv6.
	All	Click **All** to display the IPv6 addresses as follows: • **Auto** - If selected, Site-Local and Global site addresses are displayed. • **Manual** - If selected, only the Manual site address is displayed.

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3">Shelf Management IP Address

(Collaboration Servers 2000/4000 only)</td><td>IPv4</td><td colspan="2">The IPv4 address of the RMX Shelf Management Server. This IP address is used by the RMX Manager for Hardware Monitoring purposes.</td></tr>
<tr><td rowspan="2">IPv6</td><td colspan="2">The IPv6 address of the RMX Shelf Management Server. This IP address is used by the RMX Manager for Hardware Monitoring purposes.

Note: Internet Explorer 7 is required for the RMX to connect to the MCU using IPv6.</td></tr>
<tr><td>All</td><td>Click All to display the IPv6 addresses as follows:
• Auto - If selected, Site-Local and Global site addresses are displayed.
• Manual - If selected, only the Manual site address is displayed.</td></tr>
<tr><td>Subnet Mask</td><td colspan="3">Enter the subnet mask of the Control Unit.

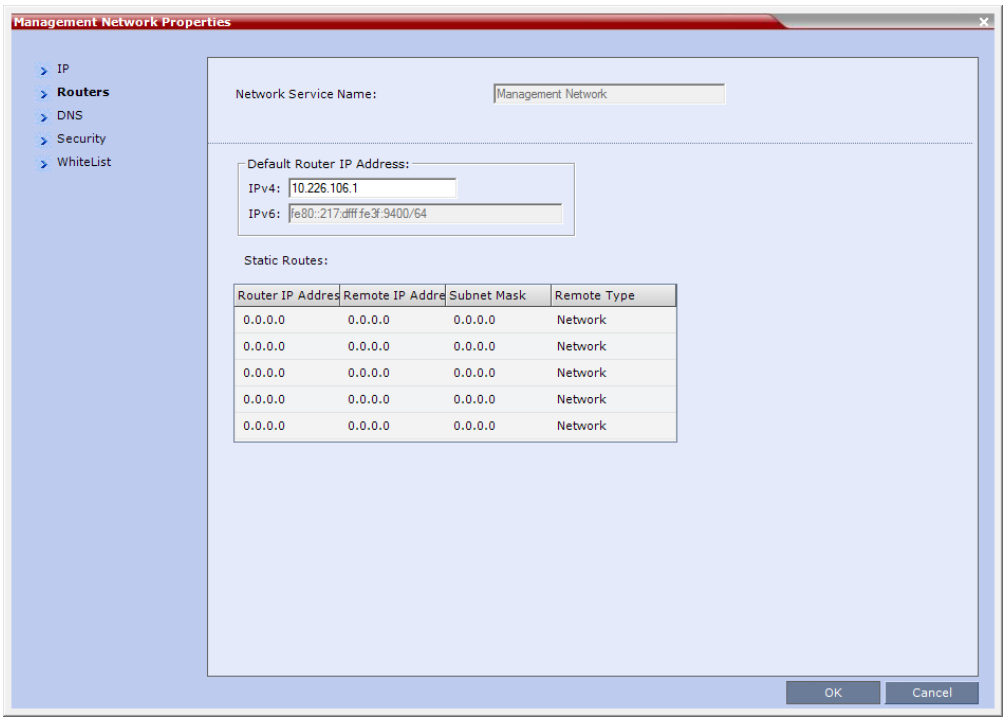
Note: This field is specific to IPv4 and is hidden in IPv6 only mode.</td></tr>
</table>

Note: On RealPresence Collaboration Server 2000 an additional tab called **LAN Ports** appears.

If an attempt is made to modify these settings, the message below will be displayed:

```
Failed to update the Management Network Service:
STATUS_SHM_IP_ADDRESS_CANT_BE_CHANGED_IN_SMCU
```

Figure 5: Routers



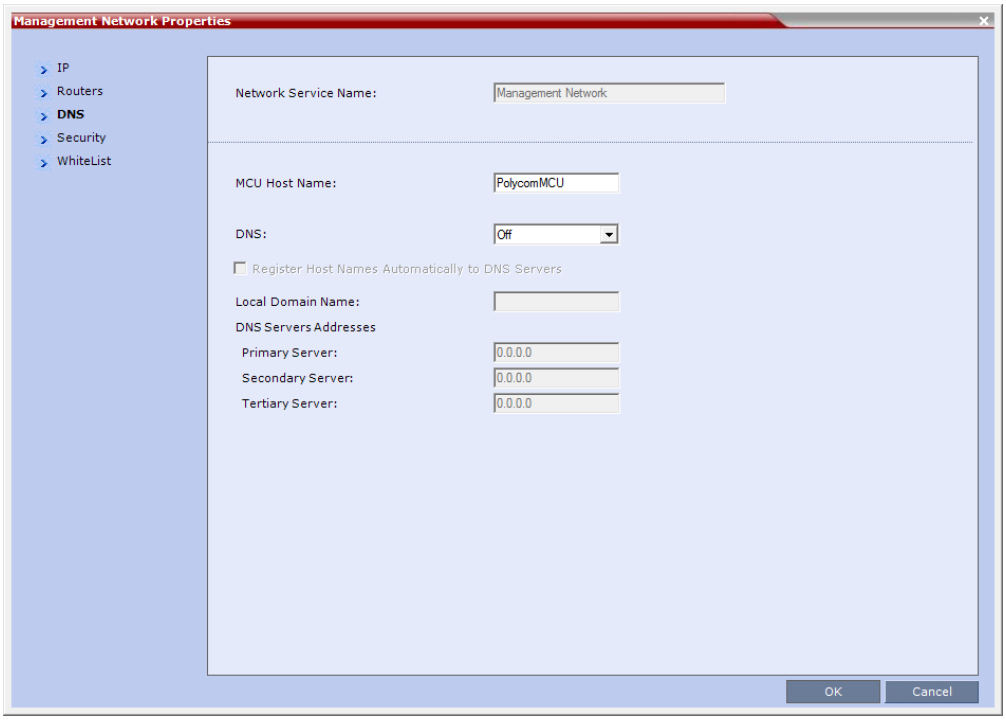
In RealPresence Collaboration Server, Virtual Edition all fields are disabled, and can be viewed only.

Default Management Network Service – Routers

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	IPv6 (Not in Collaboration Server 1800)	

Field	Description	
Static Routes (IPv4 Only Table)		The system uses **Static Routes** to search other networks for endpoint addresses outside the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first), click the appropriate column, and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	Enter the IP address of the entity to be reached outside the local network. The **Remote Type** determines whether this entity is a specific component (Host) or a network. • If **Remote Type** is Host, enter the endpoint IP address. • If **Remote Type** is Network, enter the other network segment.
	Remote Subnet Mask	Enter the remote network subnet mask.
	Remote Type	Select the router connection type: • **Network** – For a connection to a router segment in another network. • **Host** – For a direct connection to an endpoint on another network.

Figure 6: DNS



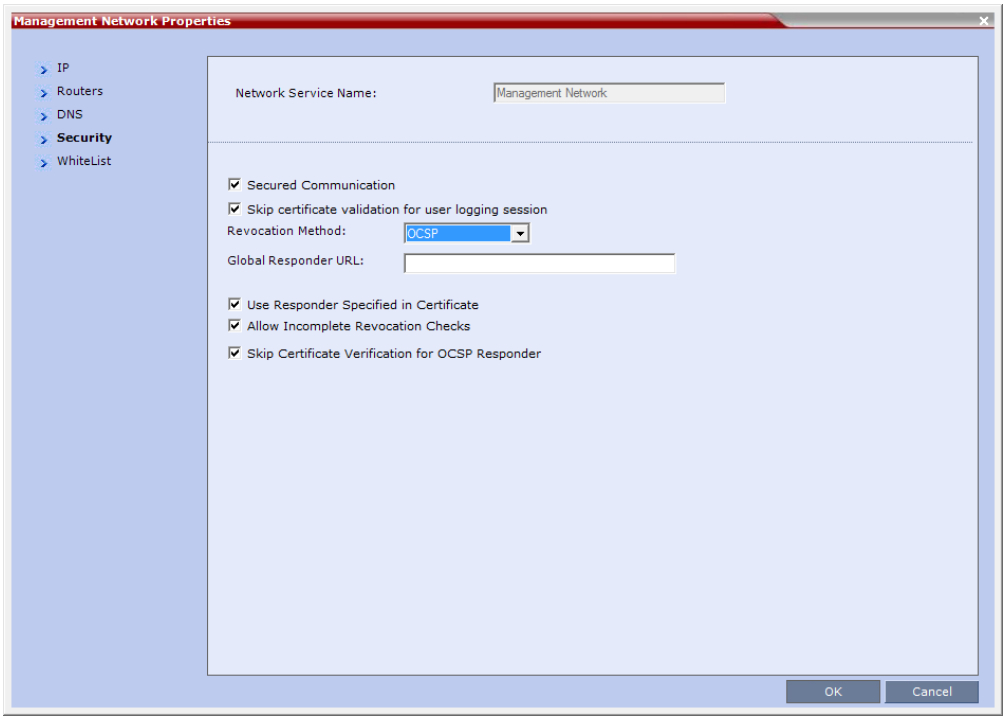
The following fields can be viewed or modified (in RealPresence Collaboration Server Virtual Edition - viewed only; modified values are not applied):

Default Management Network Service – DNS

Field	Description
MCU Host Name	The name of the MCU on the network.
DNS	Select: • Off – If DNS servers are not used in the network. • Specify – To enter the IP addresses of the DNS servers. **Note:** The IP address fields are enabled only if **Specify** is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management (for RealPresence Collaboration Servers 2000/4000/1800) with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses	

Field	Description
Primary Server	The static IP addresses of the DNS servers. A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

Figure 7: Security



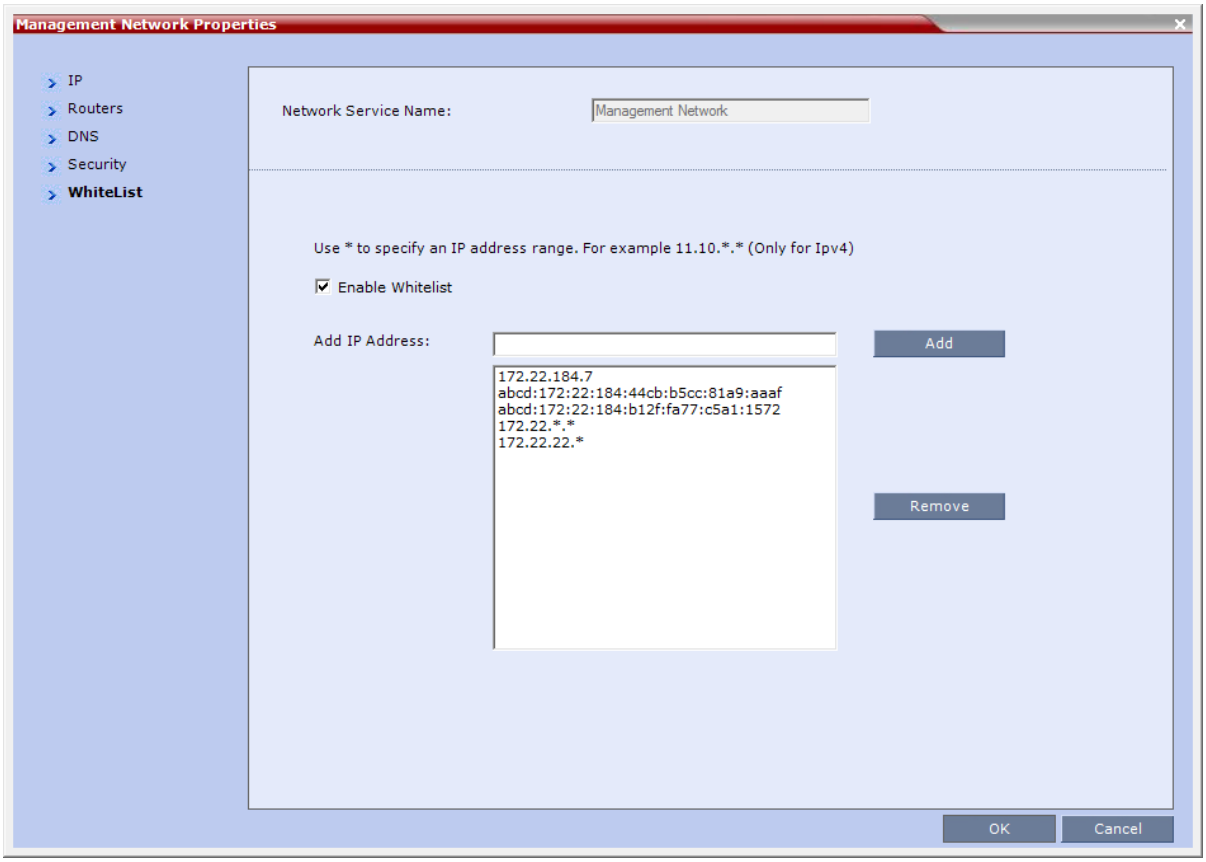
The following fields can be viewed or modified (in RealPresence Collaboration Server Virtual Edition - viewed only):

Management Network Properties – Security Parameters

Field	Description
Secured Communication	Select to enable Secured Communication. The RealPresence Collaboration Server supports TLS 1.0 and SSL 3.0 (Secure Socket Layer). A SSL/TLS Certificate must installed on the RealPresence Collaboration Server for this feature to be enabled. This box is checked by default when the MCU is in Ultra Secure Mode. For more information see Secure Communication Mode.

Field	Description
Skip certificate validation for user logging session	Select this check box to prevent peer certificate requests being issued. For more information see Public Key Infrastructure (PKI). This check box must be cleared when enabling Secured Mode. If it is not cleared an Active Alarm is created and a message is displayed stating that Secured Communications Mode must be enabled.
Revocation Method	Possible values: • NONE • CRL • OSCP - Not in RealPresence Collaboration Server, Virtual Edition
Global Responder URL	For a detailed description of these fields see Certificate Management and Certificate Revocation.
Use Responder Specified in Certificate	
Allow Incomplete Revocation Checks	
Skip Certificate Validation for OSCP Responder	For a detailed description see Certificate Management and Certificate Revocation.

Figure 8: A White List



Contains the addresses of IP Networking Entities permitted to connect to the RealPresence Collaboration Server Management Network; Networking Entities such as Network Hosts, Control Workstations, Gatekeepers SIP/ DNS Servers, etc.

Default IP Network Service

The Default IP Network Service is defined initially during the First Time Power-up or if the Default IP Service has been deleted, followed by an Collaboration Server restart.

Note: In RealPresence Collaboration Server, both the Management and the Media & Signaling networks use identical IP settings. Thus, no separate configuration is required.

Therefore, this section is relevant only for Collaboration Servers 2000/4000/1800.

Once the Default IP Network Service is defined, you can modify its properties through the IP Network Properties dialog boxes. The Default IP Service parameters need to be modified if you want to change the:

- Network type that the Collaboration Server connects to
- IP address of the Collaboration Server Signaling Host
- IP addresses of the Collaboration Server Media boards
- Subnet mask of the Collaboration Server's IP cards
- Gatekeeper parameters or add gatekeepers to the Alternate Gatekeepers list

- SIP server parameters

Figure 9: Default IP Service - Collaboration Servers (RMX) 2000/4000

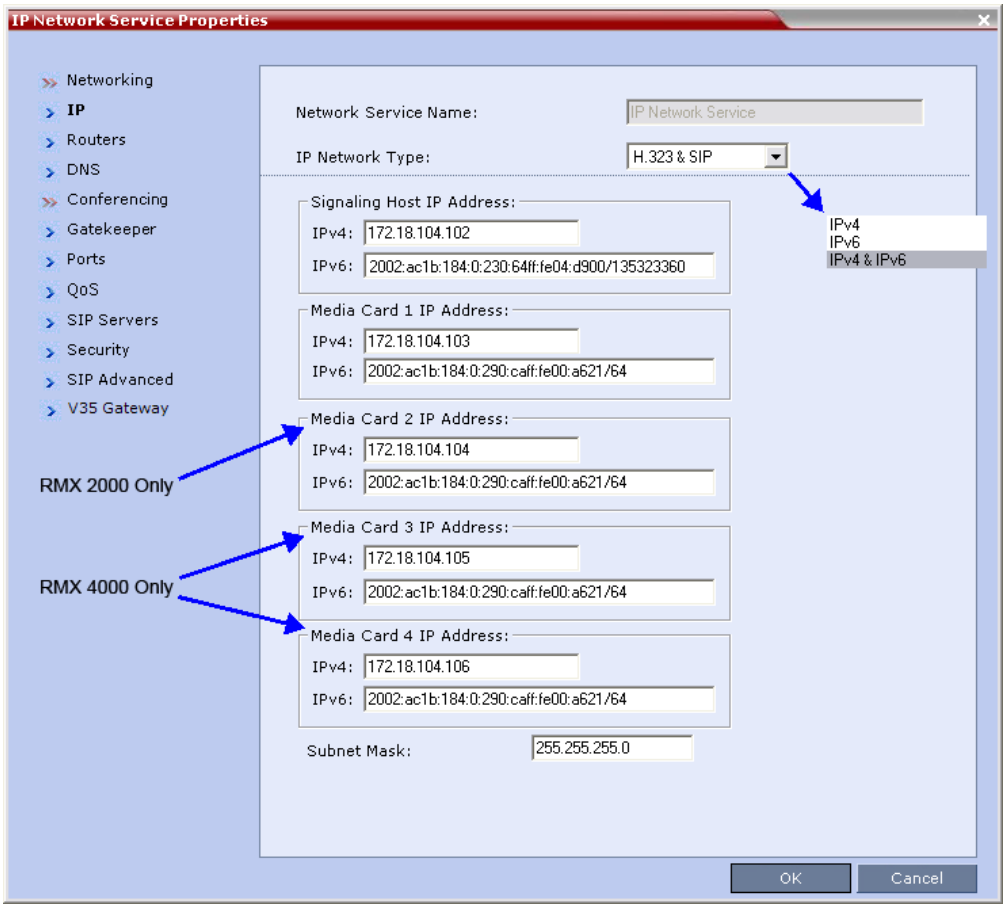
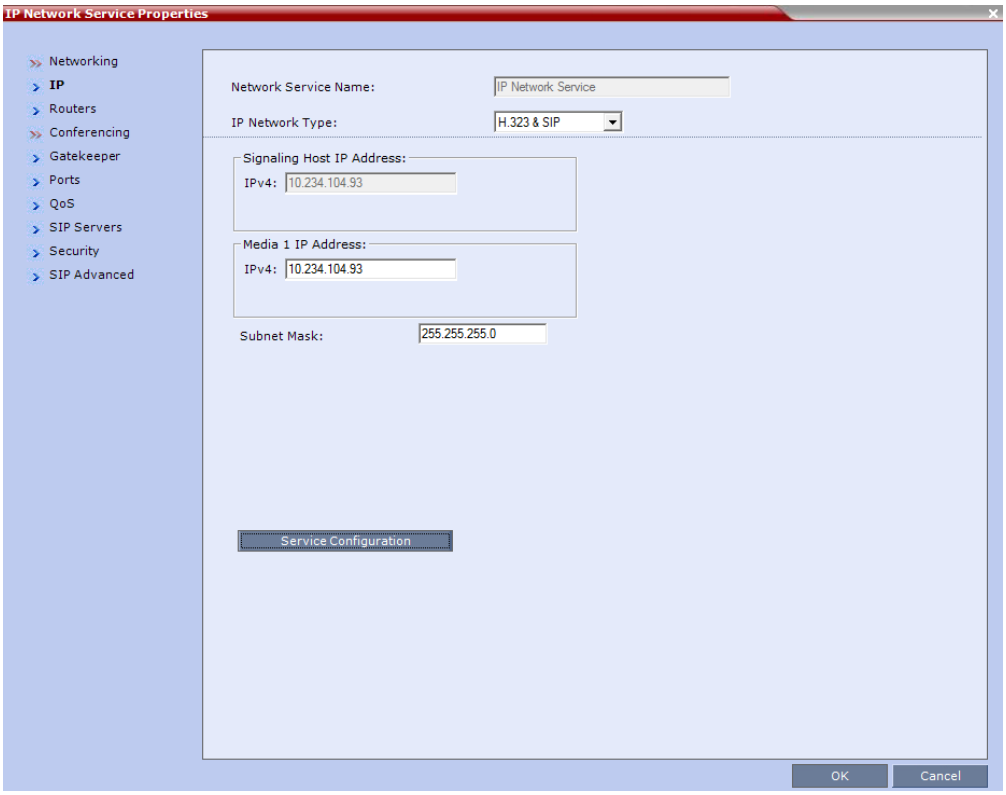


Figure 10: Default IP Service - Collaboration Server (RMX) 1800



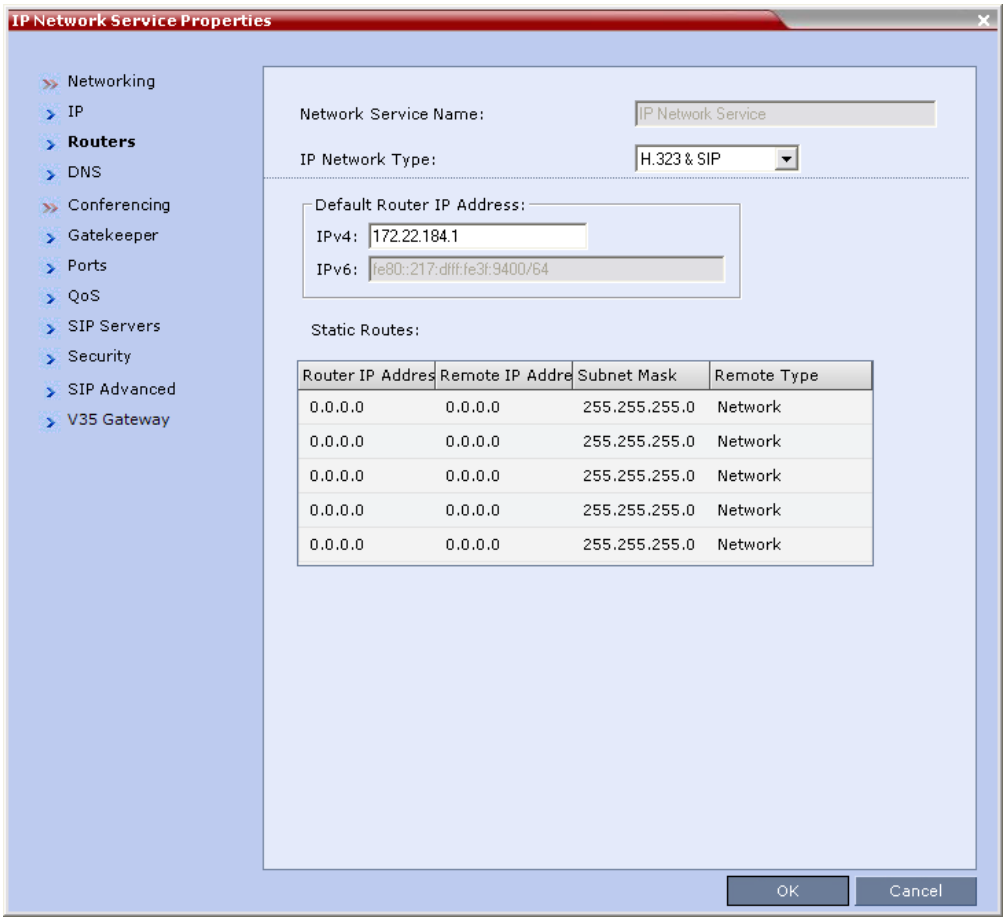
Default IP Network Service – IP

Field	Description
Network Service Name	The name **Default IP Service** is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. **Note:** This field is displayed in all IP Signaling dialogs and can contain character sets that use Unicode encoding.

Field	Description
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: • **H.323** - For an H.323-only Network Service. • **SIP** - For a SIP-only Network Service. • **H.323 & SIP** - For an integrated IP Service. Both H. 323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	On Collaboration Server 1800 this field is disabled as only one IP address is used for signaling and media transmission. Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the Collaboration Server are initiated from this address. This address is used to register the Collaboration Server with a Gatekeeper or a SIP Proxy server.
Media Card 1 IP Address	• For Collaboration Server 1800 - Enter the IP address of the media card to be used by IP endpoints when dialing in to the MCU. • For Collaboration Server 2000/4000 - Enter the IP address of the first media card as provided by the network administrator.first media card Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.
Media Card 2 IP Address (Collaboration Server 2000/4000)	Enter the IP address of the second media card if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these address.
Media Card 3 IP Address (Collaboration Server 4000)	Enter the IP address of the third media cards if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.

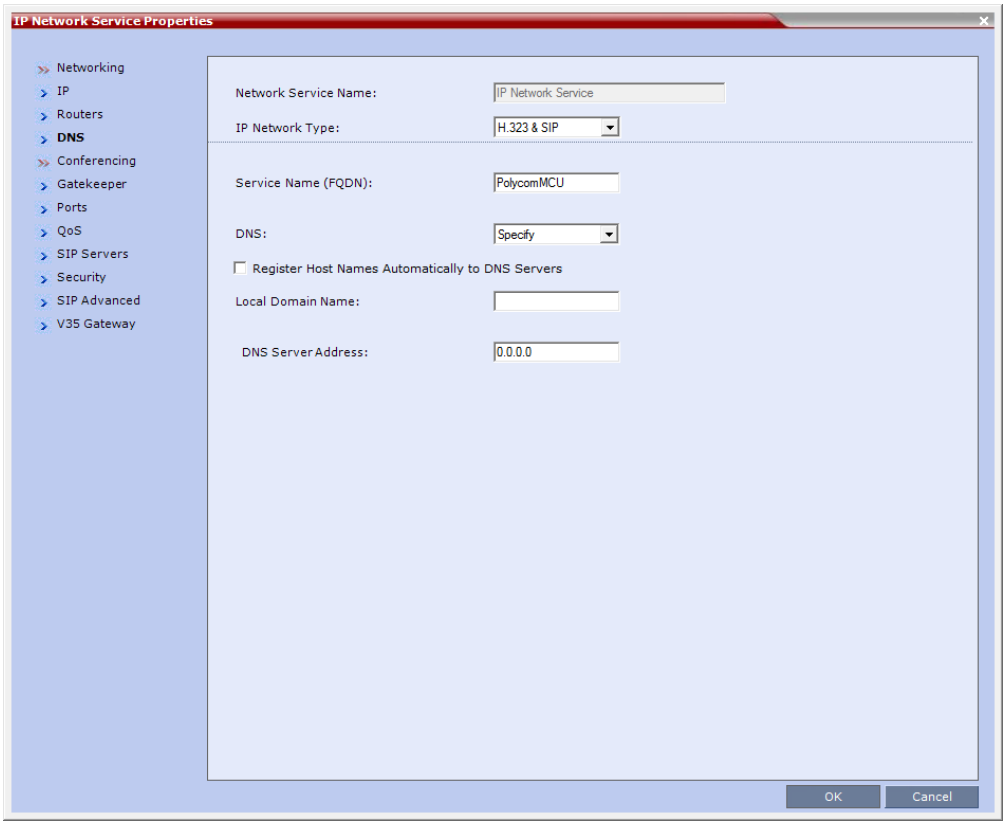
Field	Description
Media Card 4 IP Address (Collaboration Server 4000)	Enter the IP address of the fourth media cards if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.
Subnet Mask	Enter the subnet mask of the MCU. Default value: 255.255.255.0.

Figure 11: Routers Tab



With the exception of **IP Network Type**, the field definitions of the **Routers** dialog box are the same as for the Default Management Network. For more information see Default Management Network Service – Routers.

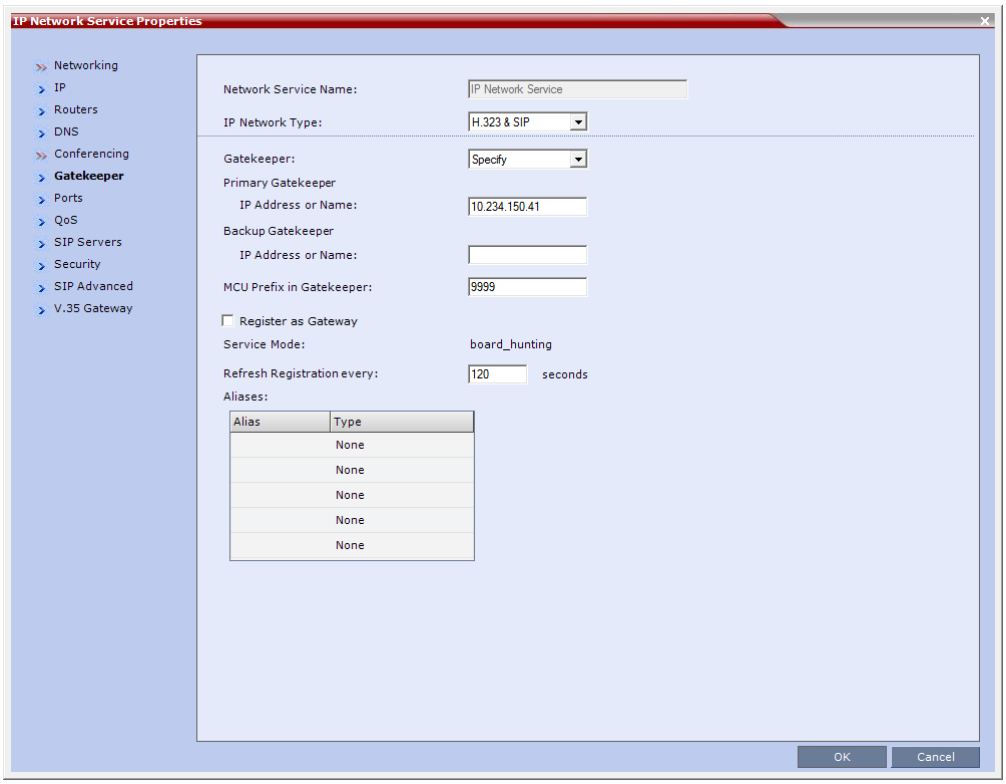
Figure 12: DNS Tab



In the **DNS Server Address** field, enter the IP address of the DNS Server for the IP Network Service.

- If the DNS field in the IP Network Service is set to Specify and the DNS is not configured or disabled, the DNS configured for the Management Network will be used.
- When upgrading from a version that does not support a DNS per IP Network Service, the DNS configured for the Management Network will be used.
- In both Standard Security and Ultra Secure Modes:
  - A separate DNS can be configured for the Management Network Service and the IP Network Service.
  - If a Multiple Services License is installed, a separate DNS can be configured for each additional IP Network Service that is defined. For more information see Multiple Network Services.

Figure 13: Gatekeeper Tab

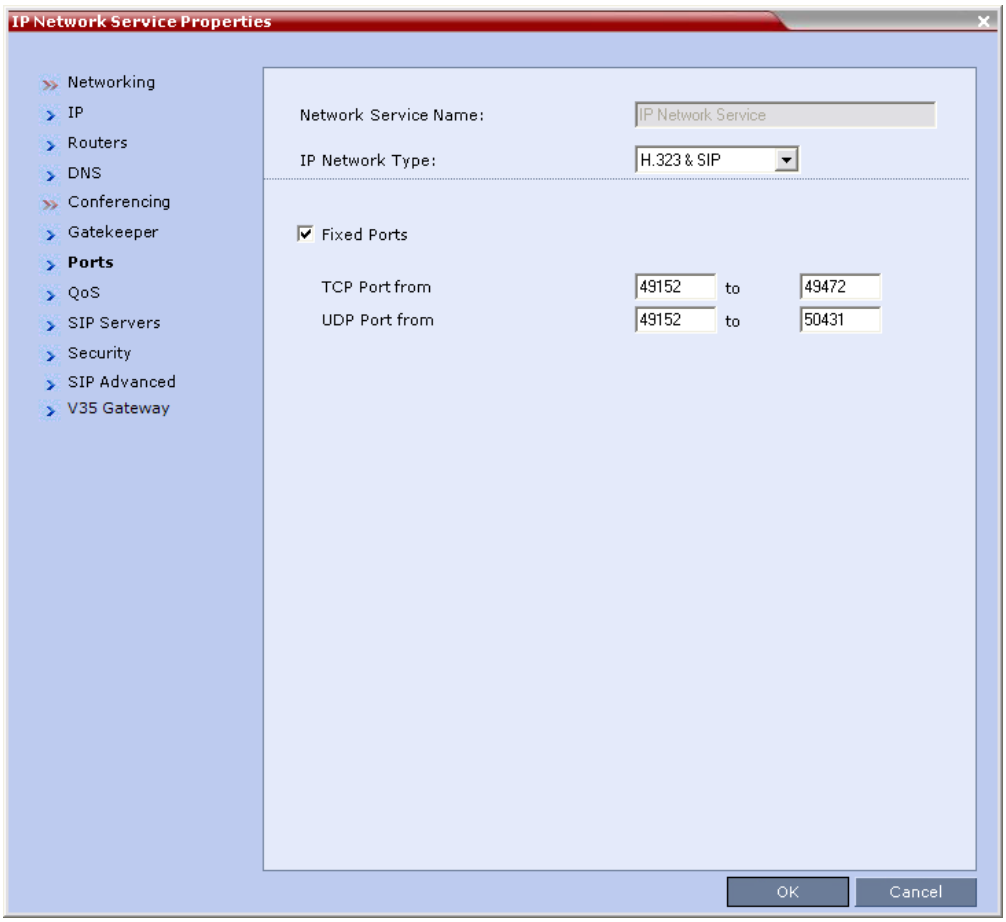


Default IP Service – Conferencing – Gatekeeper Parameters

Field	Description	
Gatekeeper	Select Specify to enable configuration of the gatekeeper IP address. When **Off** is selected, all gatekeeper options are disabled.	
Primary Gatekeeper IP Address or Name	Enter either the gatekeeper's host name as registered in the DNS or IP address.	**Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.
Alternate Gatekeeper IP Address or Name	Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.	
MCU Prefix in Gatekeeper	Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU. When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.	

Field	Description
Register as Gateway	Select this check box if the Collaboration Server is to be seen as a gateway, for example, when using a Cisco gatekeeper. **Note:** Do not select this check box when using Polycom ReadiManager or a Radvision gatekeeper.
Refresh Registration every __ seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. **Note:** • It is recommended to use default settings. • This is a re-registration and not a 'keep alive' operation – an alternate gatekeeper address may be returned.
Aliases	
Alias	The alias that identifies the Collaboration Server's Signaling Host within the network. Up to five aliases can be defined for each Collaboration Server. **Note:** When a gatekeeper is specified, at least one alias must be entered in the table. Additional aliases or prefixes may also be entered.
Type	The type defines the format in which the card's alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Note:** Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.

Figure 14: Ports Tab



Settings in the **Ports** tab allow specific ports in the firewall to be allocated to multimedia conference calls.

The port range recommended by IANA (Internet Assigned Numbers Authority) is 49152 to 65535. The Collaboration Server uses this recommendation along with the number of licensed ports to calculate the port range.

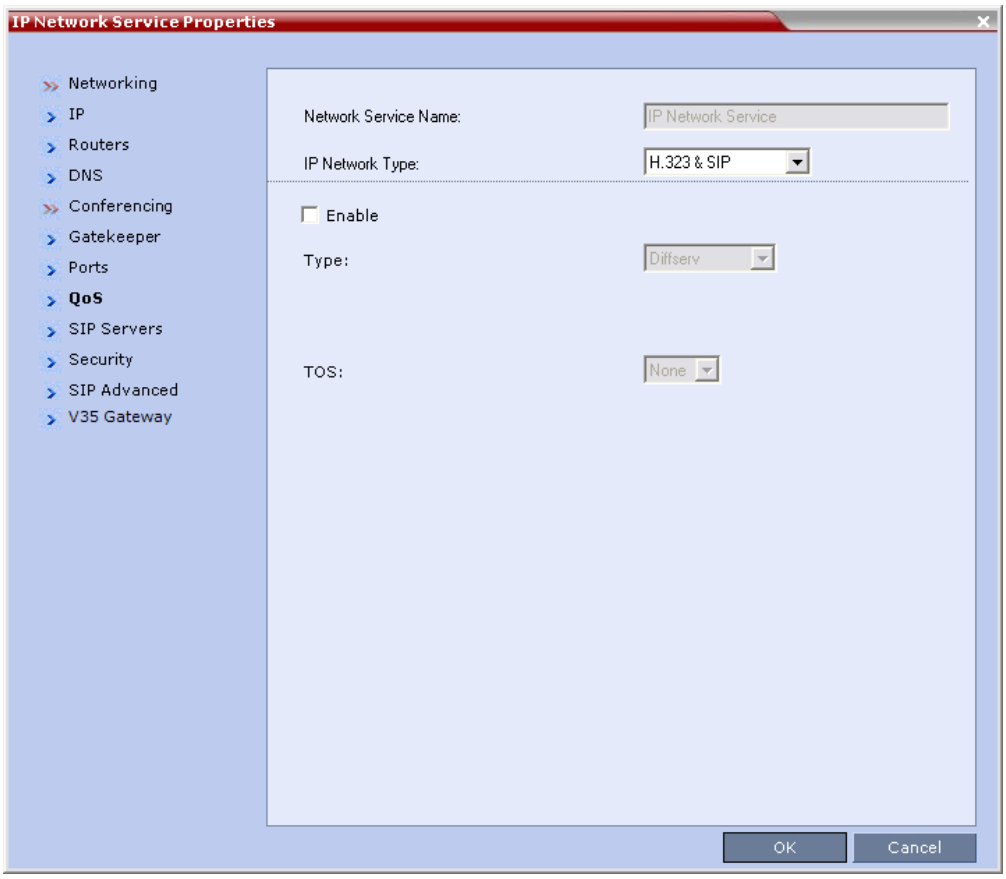
Default IP Service – Conferencing – Ports Parameters

Field	Description
Fixed Ports	Leave this check box cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC). Click this check box to manually define the port ranges or to limit the number of ports to be left open. **Note:** When ICE Environment is enabled, 8 additional ports are allocated to each call.

Field	Description
TCP Port from - to	Displays the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control). **Note:** Each H.323 dial out call consumes an additional port, thus the number of ports need to be configured as: Number of H.323 Dial out simultaneous calls x 3 ports.
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports: • Enter the first and last port numbers in the range, and the range must be 3000 ports per media card. • When ICE environment is enabled, the range must be 6000 ports per media card.

Note: If you do not specify an adequate port range, the system accepts the settings though it issues a warning. Calls are rejected when the Collaboration Server's ports are exceeded.

Figure 15: QoS Tab



Quality of Service (QoS) is important when transmitting high bandwidth audio and video information. QoS can be measured and guaranteed in terms of:

- Average delay between packets
- Variation in delay (jitter)
- Transmission error rate

DiffServ and Precedence are the two QoS methods supported by the Collaboration Server. These methods differ in the way the packet's priority is encoded in the packet header.

The Collaboration Server's implementation of QoS is defined per Network Service, not per endpoint.

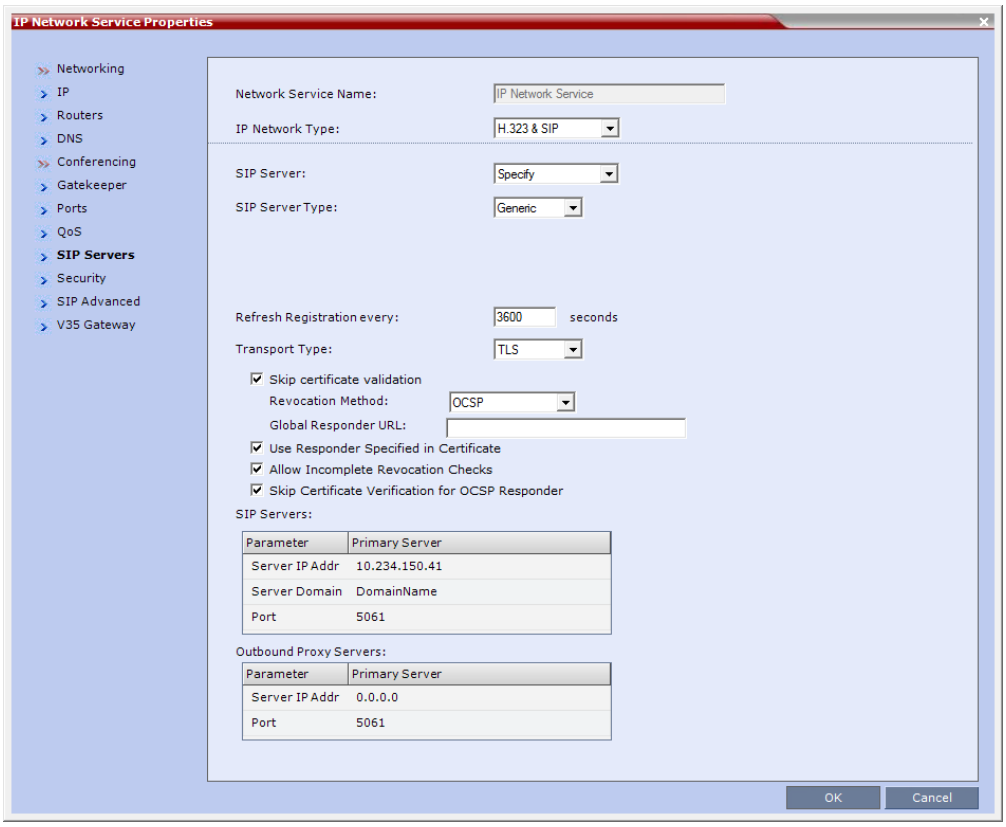
Note: The routers must support QoS in order for IP packets to get higher priority.

Default IP Service – Conferencing – QoS Parameters

Field	Description
Enable	Select to enable the configuration and use of the QoS settings. When un-checked, the values of the DSCP (Differentiated Services Code Point) bits in the IP packet headers are zero.
Type	DiffServ and Precedence are two methods for encoding packet priority. The priority set here for audio video and IP Signaling packets should match the priority set in the router. • **DiffServ**: Select when the network router uses DiffServ for priority encoding. The default priorities for both audio and video packets is 0x31. These values are determined by the **QOS_IP_VIDEO** and **QOS_IP_AUDIO** flags in the system.cfg file. The default priority for Signaling IP traffic is 0x00 and is determined by the **QOS_IP_SIGNALING** flag in the system.cfg file. • **Precedence**: Select when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence should be combined with None in the TOS field. The default priority is 5 for audio and 4 for video packets. **Note:** Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.
Audio / Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.

Field	Description
TOS	Select the type of Service (TOS) that defines optimization tagging for routing the conferences audio and video packets. • **Delay**: The recommended default for video conferencing; prioritized audio and video packets tagged with this definition are delivered with minimal delay (the throughput of IP packets minimizes the queue sequence and the delay between packets). • **None**: No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select None if you do not know which standard your router supports.

Figure 16: SIP Servers Tab



Default IP Network Service – SIP Servers

Field	Description
SIP Server	Select: • **Specify** – To manually configure SIP servers. • **Off** – If SIP servers are not present in the network. **Note:** When set to **Specify**, the **Security** tab is displayed.
SIP Server Type	Select: • **Generic** - For non Microsoft environments. • **Microsoft** - For Microsoft SIP environments.
Refresh Registration	This defines the time in seconds, in which the Collaboration Server refreshes it's registration on the SIP server. For example, if "3600" is entered the Collaboration Server will refresh it's registration on the SIP server every 3600 seconds.
Transport Type	Select the protocol that is used for signaling between the Collaboration Server and the SIP Server or the endpoints according to the protocol supported by the SIP Server: **UDP** – Select this option to use UDP for signaling. **TCP** – Select this option to use TCP for signaling. **TLS** – The Signaling Host listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected. The following protocols are supported: TLS 1.0, SSL 2.0 and SSL 3.0. **Note:** If TLS is selected, the Skip Certificate Validation and the other certificate related fields are displayed.
Skip Certificate Validation	When checked, no Certificate Validation is performed.

Field	Description
Revocation Method	For a detailed description of these fields see Certificate Management and Certificate Revocation.
Global Responder URL	
Use Responder Specified in Certificate	
Allow Incomplete Revocation Checks	
Skip Certificate Validation for OSCP Responder	
SIP Servers: Primary Server	
Server IP Address	Enter the IP address of the preferred SIP server. If a DNS is used, you can enter the SIP server name. **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use **Names** instead of **IP Addresses**.
Server Domain Name	Enter the name of the domain that you are using for conferences. The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when a call to EQ1@polycom.com reaches its outbound proxy, this proxy looks for the SIP server in the polycom.com domain, to which it will forward the call. When this call arrives at the SIP server in polycom.com, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. Default port is 5060.
Outbound Proxy Servers: Primary Server	

Field	Description
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required). **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.

SIP TCP Keep-Alive

Keep Alive behavior is defined for each IP Network Service and can be modified by adding the following system flags and modifying their values according to System Flags: SIP_TCP_KEEP_ALIVE_TYPE / BEHAVIOR.

System Flags - SIP_TCP_KEEP_ALIVE_TYPE / BEHAVIOR

Flag	Possible Flag Values
SIP_TCP_KEEP_ALIVE_TYPE	NONE No Keep Alive messages are sent.
	MS (Default when Microsoft SIP Server Type is selected for the Network Service). • Keep Alive messages are sent only after successful registration. • A Ping response is not expected.

Flag	Possible Flag Values
	RFC5626 • In the SIP Header, the Flow-Timer Header Field is mandatory. • Keep Alive messages are sent only after successful registration. A Ping response is expected and if none is received, the value of the `SIP_TCP_KEEP_ALIVE_BEHAVIOR` system flag is checked. If its value is `DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE`: • For a Register Dialog, a Reregister Message is sent. There is no disconnection. • For a Call Dialog, no further messages are sent. There is no disconnection. If its value is `RE_REGISTRATION_WHEN_NO_PONG_RESPONSE`: • Both Register and Call Dialogs are disconnected.
	RFC6223 Behavior is the same as for RFC5626 with the following differences: • In the SIP Header, the Via Header “keep” is mandatory. • In the SIP Header, the Flow-Timer Header Field is optional.
	PLCM (Default when Generic SIP Server Type is selected for the Network Service). For Call and successful Register Dialogs: • Two CR LF character sequences are sent • No Ping response is expected
SIP_TCP_KEEP_ALIVE_BEHAVIOR	If the value of the System Flag, SIP_TCP_KEEP_ALIVE_TYPE= RFC5626 or RFC6223 and no Ping is received, the value of this System Flag is checked. Possible Values: • `RE_REGISTRATION_WHEN_NO_PONG_RESPONSE` • `DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE` (Default) For a full description see the description for the `SIP_TCP_KEEP_ALIVE_TYPE` flag (above).

Keep Alive Frequency

The Keep Alive frequency is set by the SIP Server using the Via Header keep and Flow Timer fields of the SIP Header.

If the Collaboration Server is functioning as the server, the Keep Alive frequency is set according to the hard coded values listed in the following table.

Keep Alive - Frequency

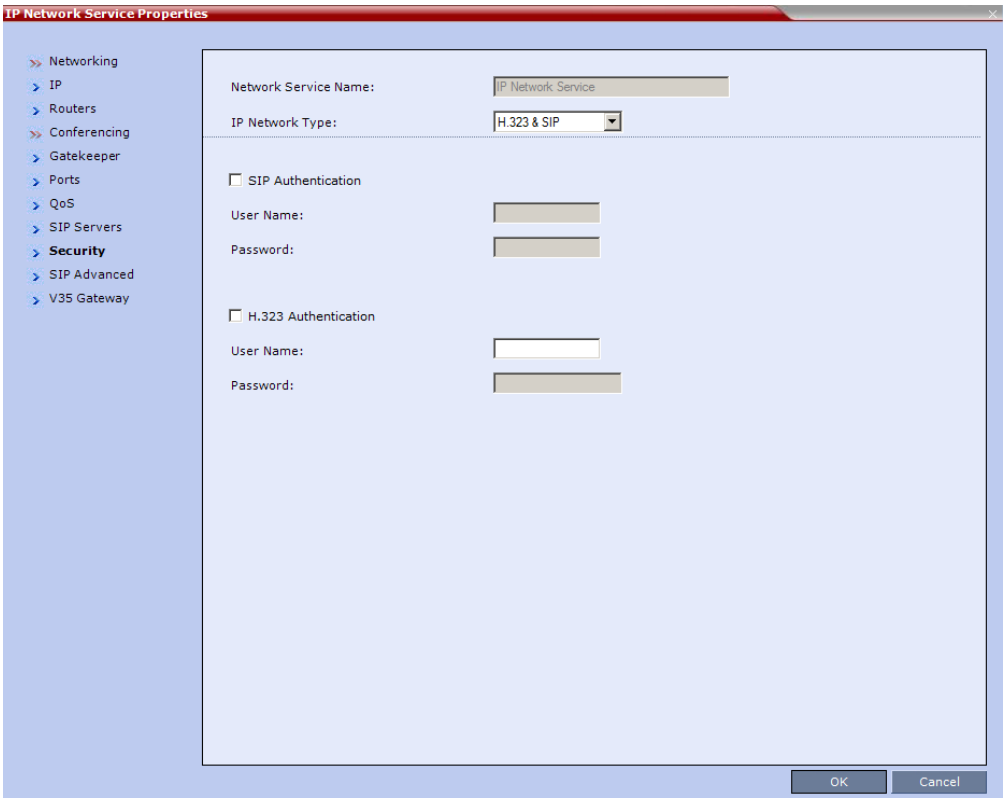
Field	Seconds
SIP_TCP_KEEP_ALIVE_DISABLE	None
SIP_TCP_KEEP_ALIVE_MS	300
SIP_TCP_KEEP_ALIVE_5626	60
SIP_TCP_KEEP_ALIVE_6223	
SIP_TCP_KEEP_ALIVE_PLCM	

In compliance with UC APL requirements, the NAT Keep Alive method has been enhanced according to IETF RFC 5626. For a full description of Keep Alive see IETF RFC 5626 and IETF RFC 6223.

For more information see Ultra Secure Mode in the System Security chapter.

Note: When updating the parameters of the SIP Server in the **IP Network Service - SIP Servers** dialog box, the Collaboration Server must be reset to implement the change.

Figure 17: Security Tab



Note: Security tab is only displayed if the SIP Server field in the SIP Servers tab is set to Specify.

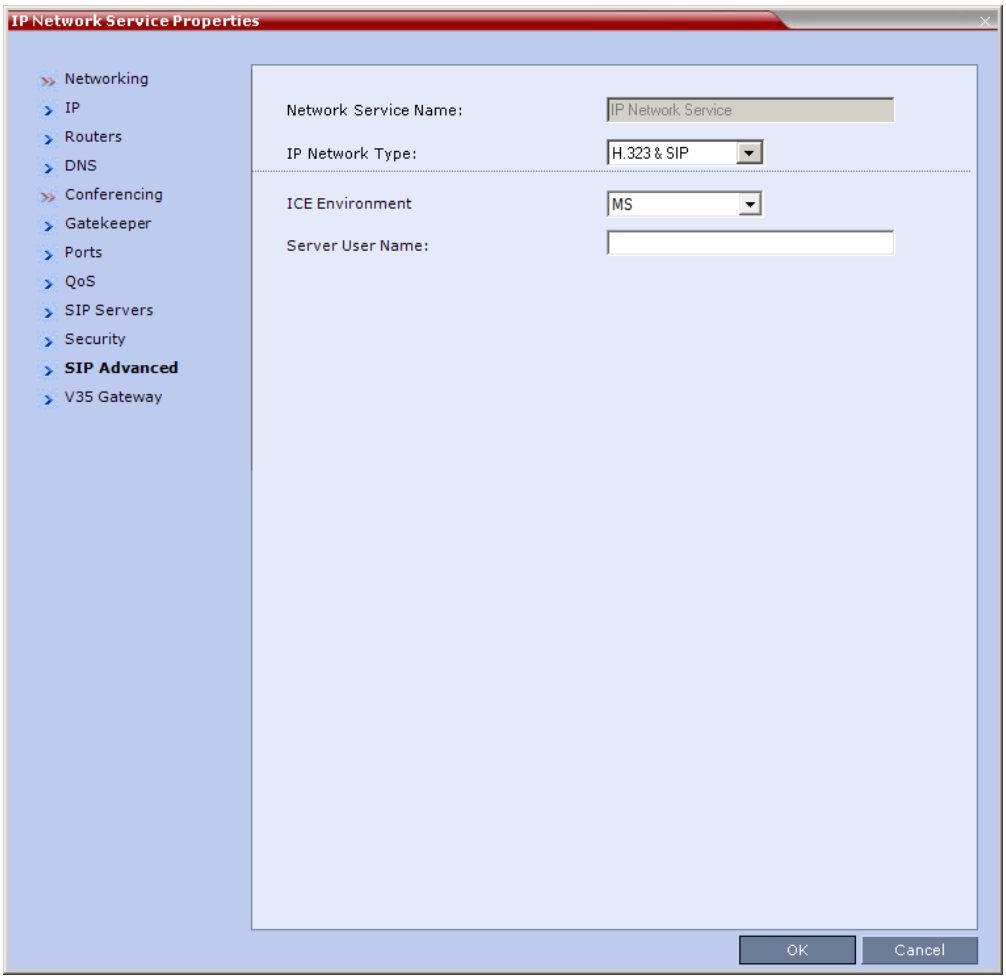
Default IP Network Service – Security (SIP Digest)

Field		Description	
SIP Authentication		Click this check box to enable SIP proxy authentication. Select this check box only if the authentication is enabled on the SIP proxy, to enable the Collaboration Server to register with the SIP proxy. If the authentication is enabled on the SIP proxy and disabled on the RMX, calls fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the SIP proxy.	
	User Name	Enter the user name for the Collaboration Server to use to authenticate itself with the SIP proxy. This name must be defined in the SIP Proxy.	These fields can contain up to 20 ASCII characters.
	Password	Enter the password for the Collaboration Server to use to authenticate itself with the SIP proxy. This password must be defined in the SIP proxy.	

Field		Description	
H.323 Authentication		Click this check box to enable H.323 server authentication. Select this check box only if the authentication is enabled on the gatekeeper, to enable the Collaboration Server to register with the gatekeeper. If the authentication is enabled on the gatekeeper and disabled on the RMX, calls fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the gatekeeper.	
	User Name	Enter the user name for the Collaboration Server to use to authenticate itself with the gatekeeper. This name must be defined in the gatekeeper.	These fields can contain up to 64 ASCII characters.
	Password	Enter the password for the Collaboration Server to use to authenticate itself with the gatekeeper. This password must be defined in the gatekeeper.	

If the **Authentication User Name** and **Authentication Password** fields are left empty, the SIP Digest authentication request is rejected. For registration without authentication, the Collaboration Server must be registered as a trusted entity on the SIP server.

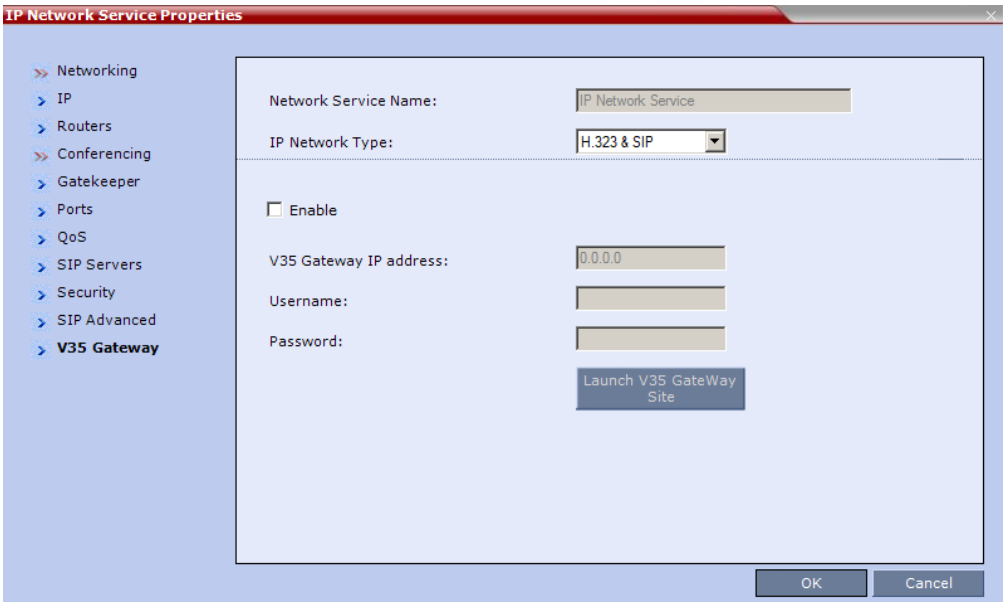
Figure 18: SIP Advanced



Default IP Network Service – SIP Advanced

Field	Description
ICE Environment	Select MS (for Microsoft ICE implementation) to enable the ICE integration.
Server User Name	Enter the Collaboration Server User name as defined in the **Active Directory**. For example, enter **rmx1234**. This field is disabled if the **ICE Environment** field is set to **None**.

Figure 19: V35 Gateway



Network Service - V35 Tab

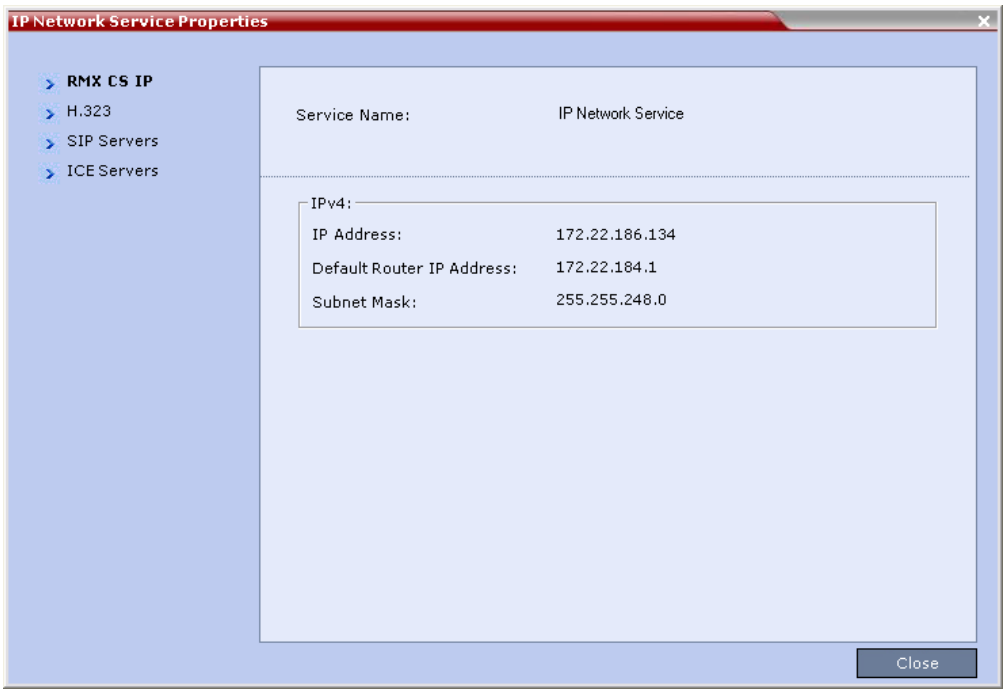
Field	Description
V35 Gateway IP Address	Enter the **Management IP** address of the management interface of the **Serial Gateway**. For more information see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide* for Maximum Security Environments, Serial Gateway S4GW - Maximum Security Mode.
Username	Enter the **User Name** that the Collaboration Server uses to log in to the management interface of the Serial Gateway.
Password	Enter the **Password** that the Collaboration Server uses to log in to management interface of the **Serial Gateway**.

Note: When updating the parameters of the SIP Server in the IP Network Service - SIP Servers dialog box, the Collaboration Server must be reset to implement the change.

IP Network Monitoring

The **Signaling Monitor** is the Collaboration Server entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy and Outbound proxy and their interaction with the MCU.

Figure 20: IP Network Services Properties - RMX CS IP Tab

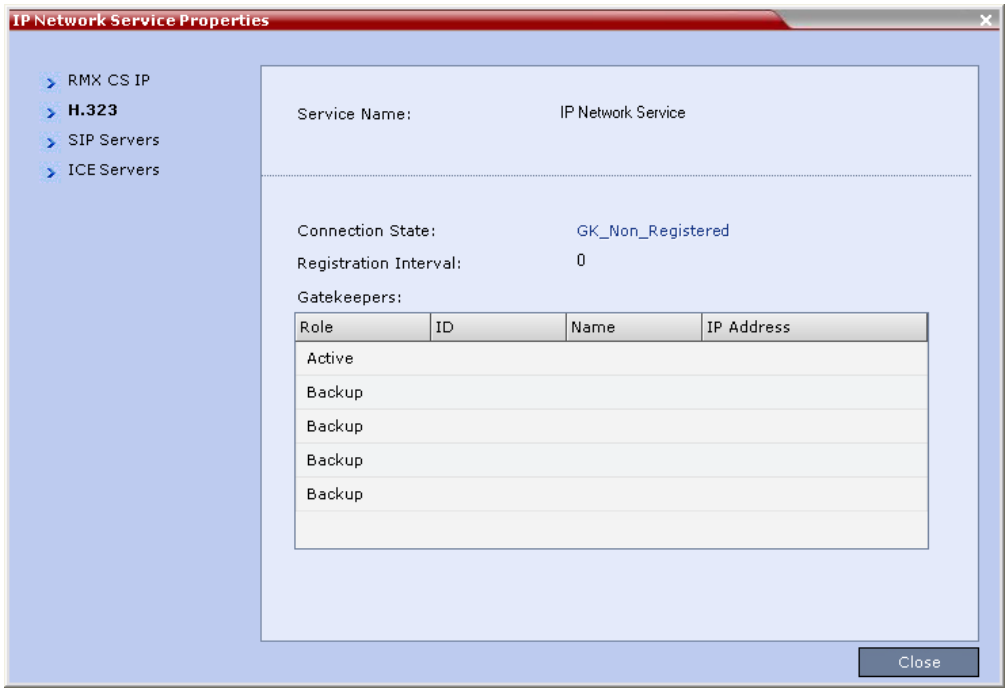


IP Network Services Properties – RMX CS IP Parameters

Field	Description	
Service Name	The name assigned to the **IP Network Service** by the **Fast Configuration Wizard**. In Collaboration Server Virtual Edition, this name is Default IP Service. **Note:** This field is displayed in all tabs.	
IPv4	IP Address	
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	Subnet Mask	The subnet mask of the MCU. Default value: 255.255.255.0.

Field	Description		
IPv6	IP Address		
	Scope	Global	The Global Unicast IP address of the Collaboration Server.
		Site-Local	The IP address of the Collaboration Server within the local site or organization.
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.	

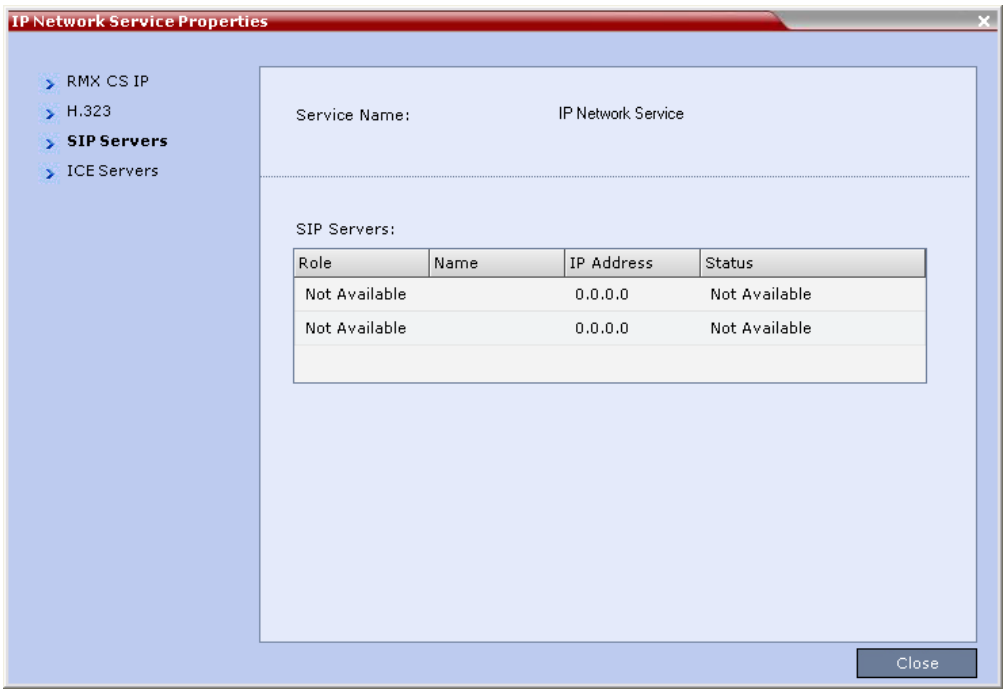
Figure 21: H.323 Tab



IP Network Services Properties – H.323 Parameters

Field	Description	
Connection State	The state of the connection between the Signaling Host and the gatekeeper: **Discovery** - The Signaling Host is attempting to locate the gatekeeper. **Registration** - The Signaling Host is in the process of registering with the gatekeeper. **Registered** - The Signaling Host is registered with the gatekeeper. **Not Registered** - The registration of the Signaling Host with the gatekeeper failed.	
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.	
	Role	**Active** - The active gatekeeper. **Backup** - The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.
	Name	The gatekeeper's host's name.
	IP Address	The gatekeeper's host's name.

Figure 22: SIP Servers



IP Network Services Properties – SIP Servers Tab

Field	Description
Role	**Active** -The default SIP Server is used for SIP traffic. **Backup** -The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP Server.
IP Address	The SIP Server's IP address.
Status	The connection state between the SIP Server and the Signaling Host. **Not Available** - No SIP server is available. **Auto** - Gets information from DHCP, if used.

Figure 23: ICE Servers

IP Network Services Properties – ICE Servers Tab

Field	Description
Role	The ICE Server's role is displayed: • STUN password server • STUN Server UDP • STUN Server TCP • Relay Server UDP • Relay Server TCP
IP Address	The ICE Server's IP Address.

Field	Description
Status 1/2/3/4	A status is displayed for each media card installed in the Collaboration Server: • Connection O.K. • MS – register fail • MS – subscribe fail • MS – service fail • Connection failed • User/password failed • Channel didn't receive any packets for 5 seconds • Channel exceeded allotted bandwidth • Unknown failure In systems with multiple media cards, Status 1 refers to the uppermost media card.
FW Detection	The Firewall Detection status is displayed: • Unknown • UDP enabled • TCP enabled • Proxy -TCP is possible only through proxy • Block – both UDP & TCP blocked • None

Modifying Network Settings Using TUI

This section described how to modify Collaboration Server, Virtual Edition network setting via TUI (Text User Interface).

Through this interface you can:

- Control the Collaboration Server’s Management Network settings.
- Configure the DNS server connection.
- Configure the SSH setup.
- Modify the default polycom-polycom username-password combination.

This is the only safe way to modify any of the Collaboration Server Virtual Edition settings, without risking likely hazardous consequences to Collaboration Server operation and accessibility.

Management Network

To modify the Collaboration Server's Management Network parameters, it is necessary to establish a direct connection between a workstation and the Collaboration Server.

Note: In RealPresence Collaboration Server, both the Management and the Media & Signaling networks use identical IP settings. Thus, no separate configuration is required.

Determine Network Setup Mode

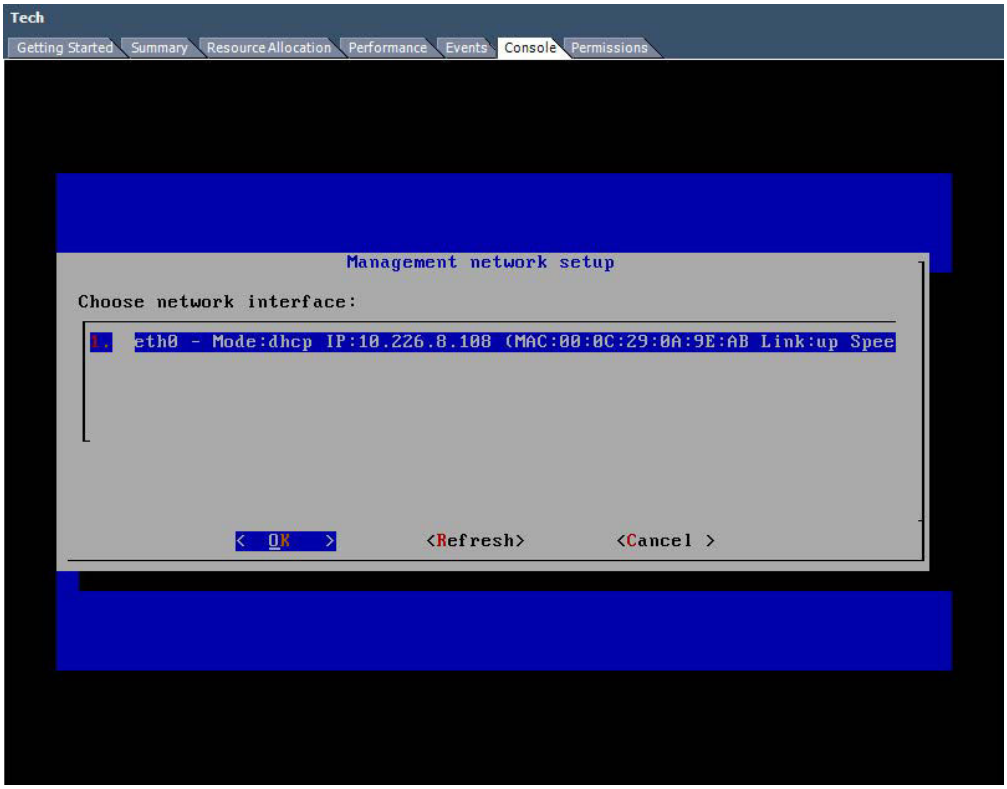
The network configuration mode is determined during installation, but may be modified via the network setup mode menu.

The Collaboration Server, Virtual Edition, can operate in two network configuration modes:

- Manual - The user manually configures the network connections using the TUI tool.
- DHCP (default mode) - The network is automatically configured with no user intervention.

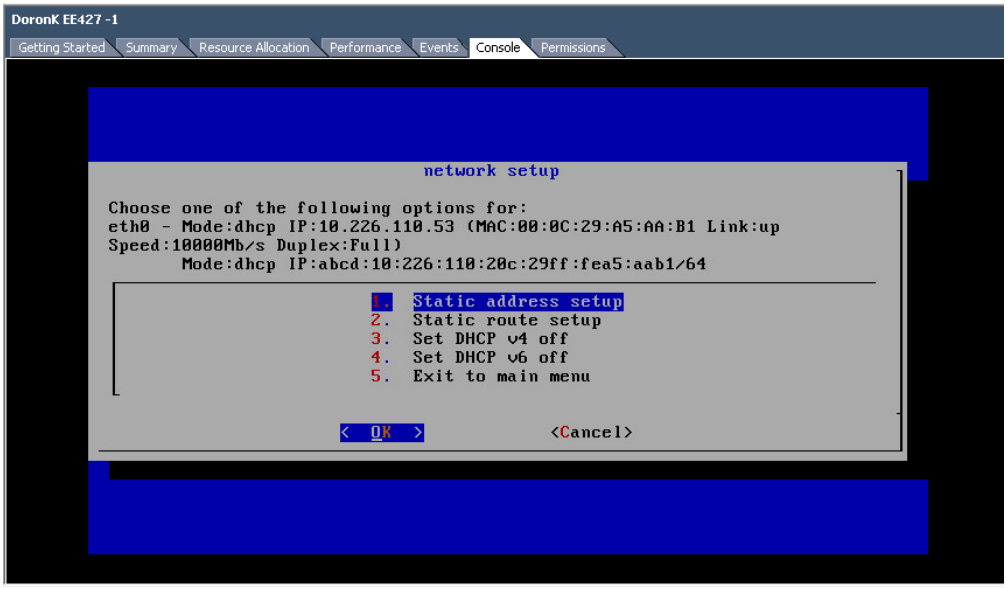
Procedure

1. Navigate to the Welcome to network setup menu, as described above (see the procedure on navigating to the network setup menu right under Management Network).
2. Use the arrow keys to select Management network setup and press ENTER to view the current configuration for Management and Media & Signaling network setup.



3. To modify this setup press **ENTER**.

   The network setup mode menu is displayed.

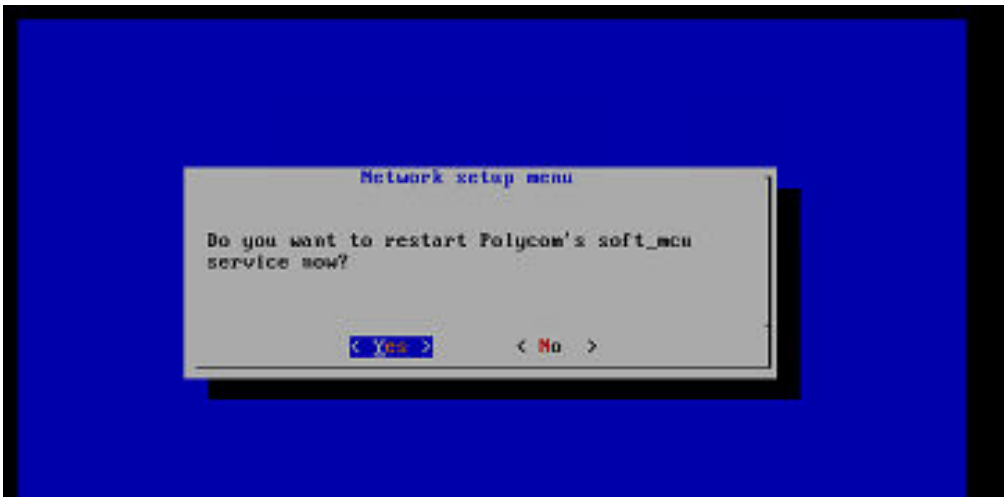


Note that the menu options for DHCP mode do not reflect the current DHCP status, but the commands you may request. Thus, as an example, when you select Set DHCP v4 on, it does not signify that the IPv4 networking setup current mode is DHCP, but that it becomes DHCP only following your selection.

Should both DHCP options be currently off (meaning, in the menu these commands allow you to set them both to on), network setup configuration is currently Static, and you may configure it using the Static setup options. However, even if IPv6 DHCP is currently off, IPv6 neighbor solicitation is enabled.

4. To save the changes you make and exit the menu, select **Exit** to main menu.

   You are prompted to perform system reset.



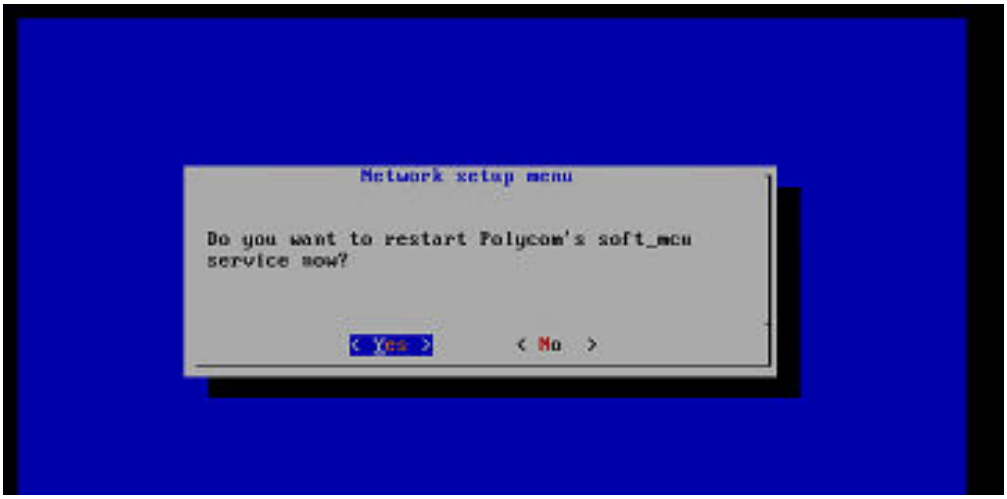
It is recommended that you select Yes for the changes you made to take effect.

Configure the Connection to the DNS Server

The Welcome to network setup menu allows you to reliably determine the soft MCU connections to the DNS server.

Procedure

1. Navigate to the Welcome to network setup menu, as described above (see the procedure on navigating to the network setup menu right under Management Network).
2. Select DNS setup, to display the DNS setup menu.



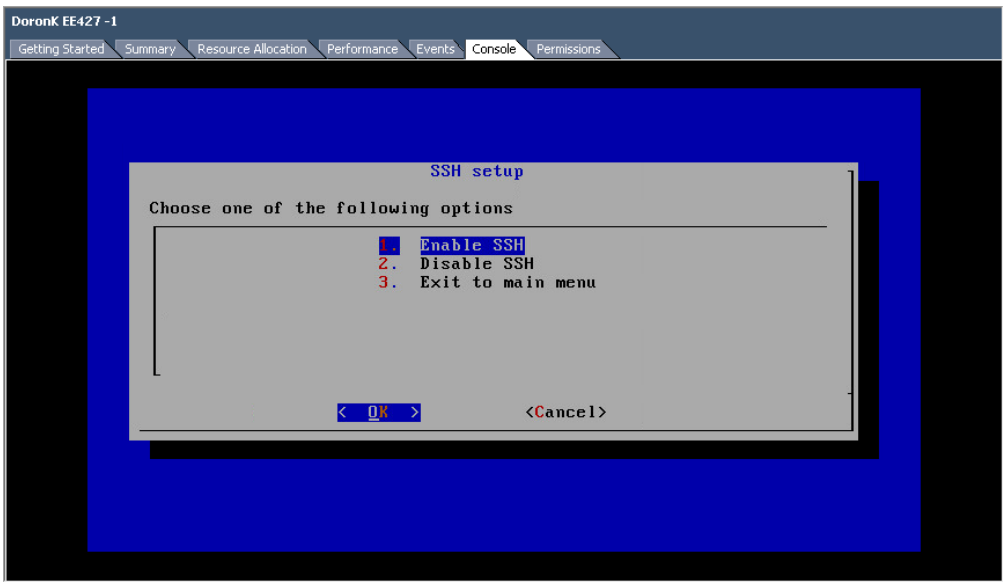
3. Modify the DNS settings according to requirements.
4. When done, use TAB to select OK to save settings and exit.

Toggle Remote Connection Using SSH

RealPresence Collaboration Server, allows you to connect the MCU remotely via a secured connection using SSH. However, this option may be disabled (or enabled) to allow access only via a vSphare client, thus ensuring no remote connection is possible.

Procedure

1. Navigate to the Welcome to network setup menu, as described above (see the procedure on navigating to the network setup menu right under Management Network).
2. Use the arrow keys to select SSH setup, and press **ENTER**, to display the SSH setup menu.



3. Use the arrow keys to determine whether to allow secured remote connection using SSH, and press **ENTER**.
4. Use the **Exit** to main menu option to return to the main menu.

Note: System reset is not mandatory following SSH status change.

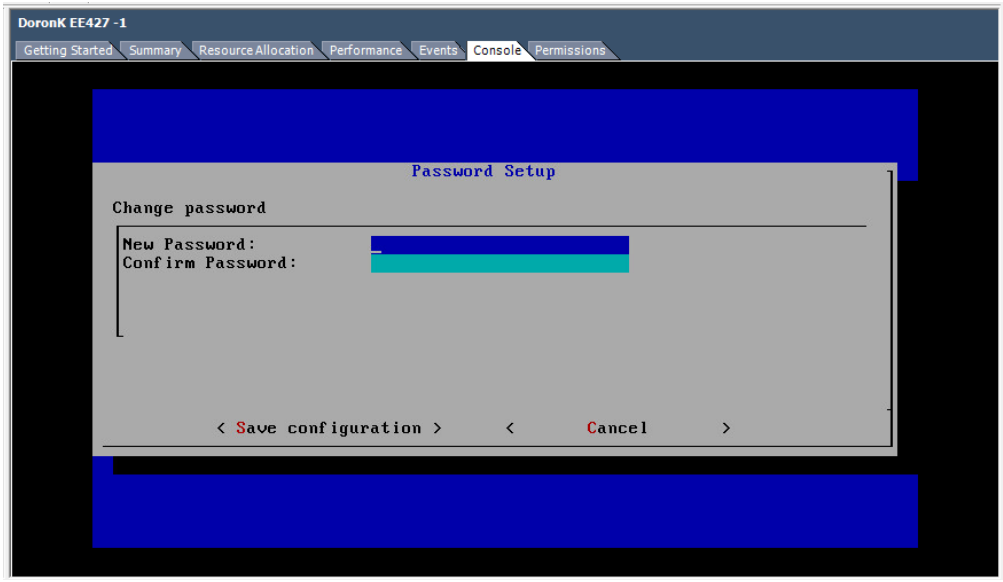
Modify the Default Password

RealPresence Collaboration Server, is deployed with a built-in polycom-polycom default username-password combination for network setup purposes.

It is highly recommended to modify the password so as to decrease the risk of system abuse by unauthorized entities.

Procedure

1. Navigate to the Welcome to network setup menu, as described above (see the procedure on navigating to the network setup menu right under Management Network).
2. Use the arrow keys to select Change password, and press ENTER, to display the Password Setup screen.



3. At the appropriate fields, enter the new password twice, and Save configuration.

   The console polycom user's password is now defined as the password you entered.

Note: System reset is not mandatory following password change.

LAN Redundancy

LAN Redundancy enables the redundant LAN port connection to automatically replace the failed LAN port by using another physical connection and NIC (Network Interface Card).

When a LAN port fails, IP network traffic failure is averted and network or endpoints disconnections do not occur. When LAN cables are connected to both LAN 1 and LAN 2 ports, the Collaboration Server automatically selects which port is active and which is redundant.

Media Redundancy - Collaboration Server 2000/4000

On the Collaboration Servers 2000/4000, LAN 1 and LAN 2 ports on the RTM LAN card can be used as redundant media ports.

Figure 24: Collaboration Server 2000/4000 RTM LAN Card on Rear Panel

Media Redundancy on the Collaboration Server 2000/4000 is dependent on the settings of the `LAN_REDUNDANCY` and `MULTIPLE_SERVICES` System Flags as summarized in the following table:

Collaboration Servers 2000/4000 - Media Redundancy - System Flags

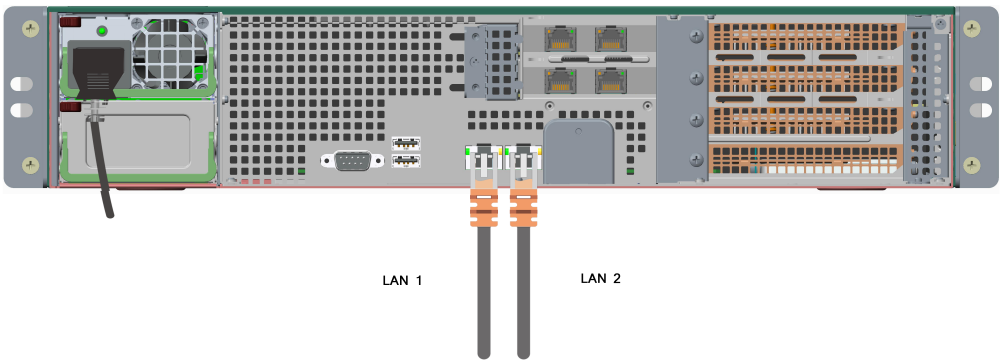
System Flag / Value	Collaboration Server 2000	Collaboration Server 4000
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	No Redundancy	
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES		
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Media Redundancy Only	Full Redundancy
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	Full Media Redundancy (If only one **IP Network Service** is defined per media card.)	

Media and Signaling Redundancy - Collaboration Server 1800

On Collaboration Server 1800 LAN 1 and LAN 2 are the redundant media and signaling ports.

- LAN 1 port is used for standard communications
- LAN 2 port can be used to define a second Network Service or for LAN Redundancy

The following cables are connected to the LAN ports on the rear panel of Collaboration Server 1800:



LAN Connections to the IP Ports

IP Port	Description
LAN 1	For management network connections: When LAN redundancy is enabled, LAN 1 is used for management, media, and signaling network connections.
LAN 2	For media, and signaling network connections: When LAN redundancy is enabled, LAN 2 is the backup for the LAN 1 port.

Media Redundancy on Collaboration Server 1800 is dependent on the settings of the LAN_REDUNDANCY and MULTIPLE_SERVICES System Flags as summarized in the following table:

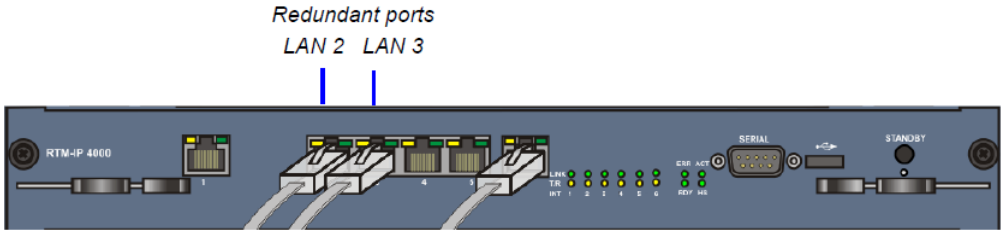
RMX 1800 - Media Redundancy - System Flags

System Flag / Value	Collaboration Server 1800
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	No Redundancy. If a second LAN cable is connected to Port 2, Network separation is enabled (the Management Network Service is separated from the Default IP Network Service)
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	No Redundancy.
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Full Redundancy.
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	These flags cannot be set to YES simultaneously.

Signaling and Management Redundancy - Collaboration Server 4000

On Collaboration Server 4000, for Signaling and Management Redundancy when LAN_REDUNDANCY = YES and MULTIPLE_SERVICES = NO, the LAN 3 port on the RTM-IP 4000 card is redundant to the LAN 2 port. LAN ports 4 and 5 are never used.

Figure 25: RealPresence Collaboration Server (RMX) 4000 - RTM IP 4000 on Rear Panel2



On Collaboration Server 4000 Signaling and Management Redundancy is implemented using the LAN ports on the RTM-IP card and is dependent on the settings of the LAN_REDUNDANCY and MULTIPLE_SERVICES System Flags as summarized in the following table.

RMX 4000 - Signaling and Management Redundancy - System Flags

Flag / Value	Port Usage	
	LAN 2	LAN 3
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	Management	Signaling

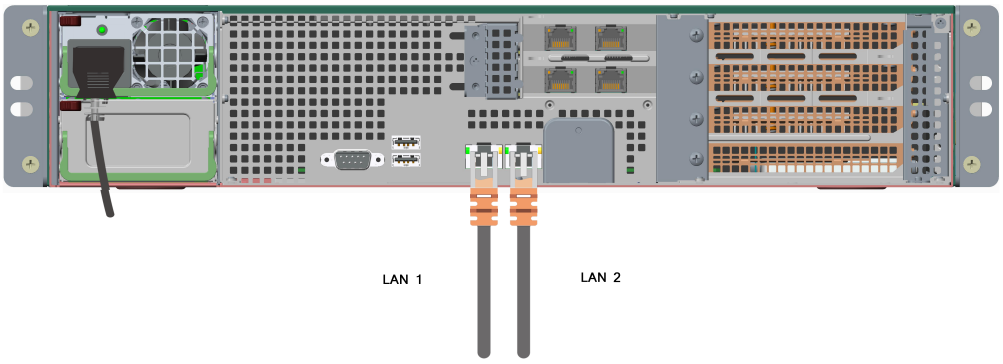
Flag / Value	Port Usage	
	LAN 2	LAN 3
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	Management	Not Used
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Management & Signaling (LAN 3 is redundant to LAN 2)	
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	Management	Management

Management Redundancy - Collaboration Server 1800

On Collaboration Server 1800, for Management Redundancy, the `LAN 2` port is redundant to the `LAN 1` port and must have a LAN cable connected.

LAN Redundancy is not supported by Collaboration Server 1800 with no DSP cards.

Figure 26: Collaboration Server 1800 - LAN 2 Connection on Rear Panel



On Collaboration Server 1800, Management Redundancy is implemented using the `LAN 1` and `LAN 2` ports and is dependent on the settings of the `LAN_REDUNDANCY` and `MULTIPLE_SERVICES` System Flags as summarized in the following table.

RMX 1800 - Management Redundancy - System Flags

Flag / Value	Port Usage	
	LAN 2	LAN 3
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	Management	Media and Signaling
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	Management	Media and Signaling

Flag / Value	Port Usage	
	LAN 2	**LAN 3**
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Management, Media and Signaling.	LAN 2 is redundant to LAN 1
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	These flags cannot be set to **YES** simultaneously.	

Configuration Requirements

LAN Redundancy is disabled by default, and can be disabled by setting the LAN_REDUNDANCY System Flag to NO, in which case the LAN 2 port must be connected to the IP network.

LAN Redundancy can be modified by changing the LAN_REDUNDANCY system flag to YES and connecting the appropriate LAN cables to the LAN ports on the Collaboration Server as described below.

Modify LAN Redundancy in Collaboration Server 1800

You can modify LAN Redundancy in Collaboration Server 1800.

Procedure

» Connect the additional LAN cable to **LAN 2** port on the rear panel of Collaboration Server 1800.

Modify LAN Redundancy in Collaboration Server 2000/4000

You can modify LAN Redundancy in Collaboration Server 2000/4000.

Note: On Collaboration Server 2000, one RTM LAN card is required.

For more information see *RealPresence Collaboration Server 2000 Hardware Guide, Installing or Replacing the RTM LAN*.

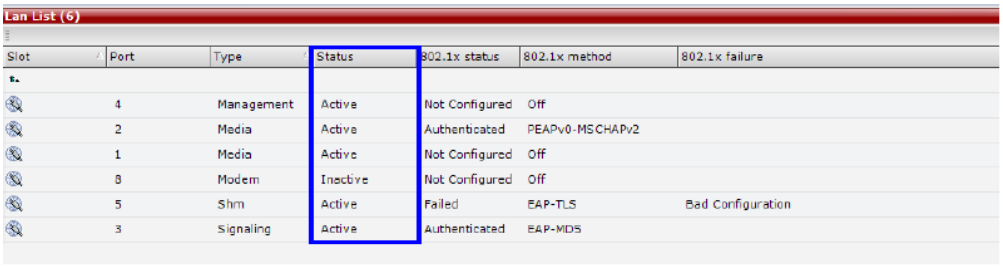
Procedure

1. Connect the additional LAN cable to LAN 1 port on the RTM LAN.
2. For Collaboration Server 2000, select **Setup** > **System Configuration** > **System Flags**, and there add the flag RMX2000_RTM_LAN and set it to YES to activate the installed RTM LAN card.
3. LAN Redundancy can be enabled simultaneously with Multiple Networks. To enable the Multiple Networks option, set the MULTIPLE_SERVICES flag to YES.
4. If required, reset the Collaboration Server (specifically when adding the RMX2000_RTM_LAN flag).

Hardware Monitor Indications

When LAN Redundancy is enabled on the Collaboration Server, LAN 2 port is **Active**. With LAN redundancy, when LAN LEDs are lit they indicate that a physical connection of the cables is present but does not indicate their activity status.

In the **Hardware Monitor** pane the **Lan List** displays the Collaboration Server LAN ports together with their **Status** indication.



The **Hardware Monitor Status** indications are summarized in the following table:

RTM LAN Indications

Status	Description
Active	The LAN port cable is connected.
Inactive	The LAN port cable is not connected.
Standby	The LAN Redundancy option is enabled and this LAN port is the redundant and in standby mode. In case of failure, this port becomes active.

NAT Traversal

NAT (Network Address Translation) **Traversal** is a set of techniques enabling participants behind firewalls to remotely connect to conferences, hosted on the Collaboration Server, via the Internet.

Note: NAT Traversal is applicable only to Collaboration Server Virtual Edition.

Session Border Controller (SBC)

All signaling and media for both SIP and H.323 are routed through an **SBC**.

The following **SBC** environments are supported:

- **SAM - Polycom SBC**
- **Acme Packet** - A 3rd party **SBC**
- **VBP - Polycom Video Border Proxy**

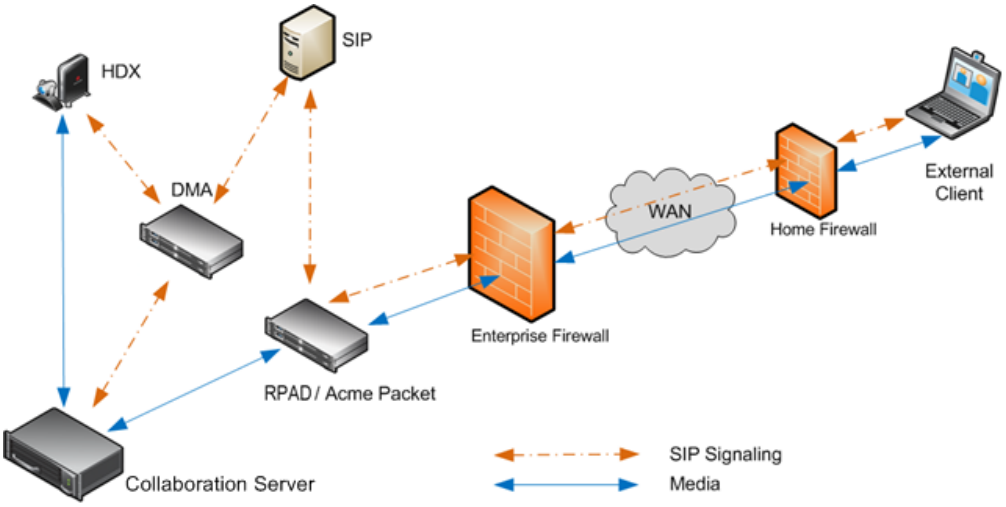
Deployment Architectures

The following **NAT Traversal** topologies are given as examples. Actual deployments depend on user requirements and available infrastructure.

Remote Connection Using the Internet

Remote connection call flow scenarios.

Note: On the Collaboration Server 2000/4000, full media redundancy is supported if only one IP Network Service is defined per media card.



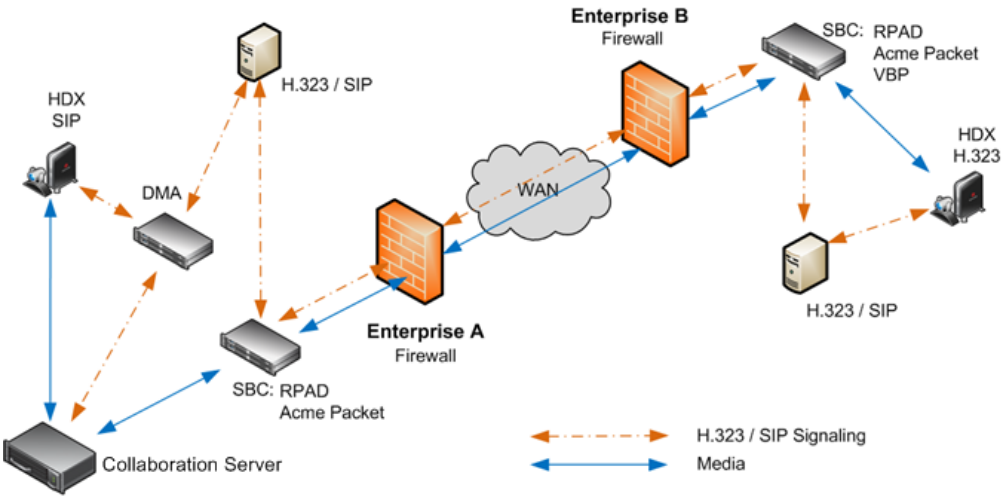
The following **Remote Connection** call flow options are supported:

Remote Connections

Enterprise Client		
Environment	**Registered**	**SBC**
SIP / H.323	Yes	SAM / Acme Packet
SIP / H.323	No	SAM / Acme Packet
SIP / H.323	No	SAM Only

Business to Business Connections

Business to Business connection call flow scenario.



The following **Business to Business** connection call flow options are supported:

Business to Business Connections

Enterprise A Client				Enterprise B Client		
Environment	**Registered**	**SBC**		**SBC**	**Registered**	**Environment**
H.323	Yes	Access Director		Access Director	Yes	H.323
H.323	Yes	Access Director		Access Director	Yes	H.323
SIP	Yes	Access Director		Access Director	Yes	H.323
SIP	Yes	Acme Packet		Acme Packet	Yes	H.323

Enable and Modify FW NAT Keep Alive

The Collaboration Server can be configured to send a **FW NAT keep alive** message at specific **Intervals** for the **RTP**, **UDP** and **BFCP** channels.

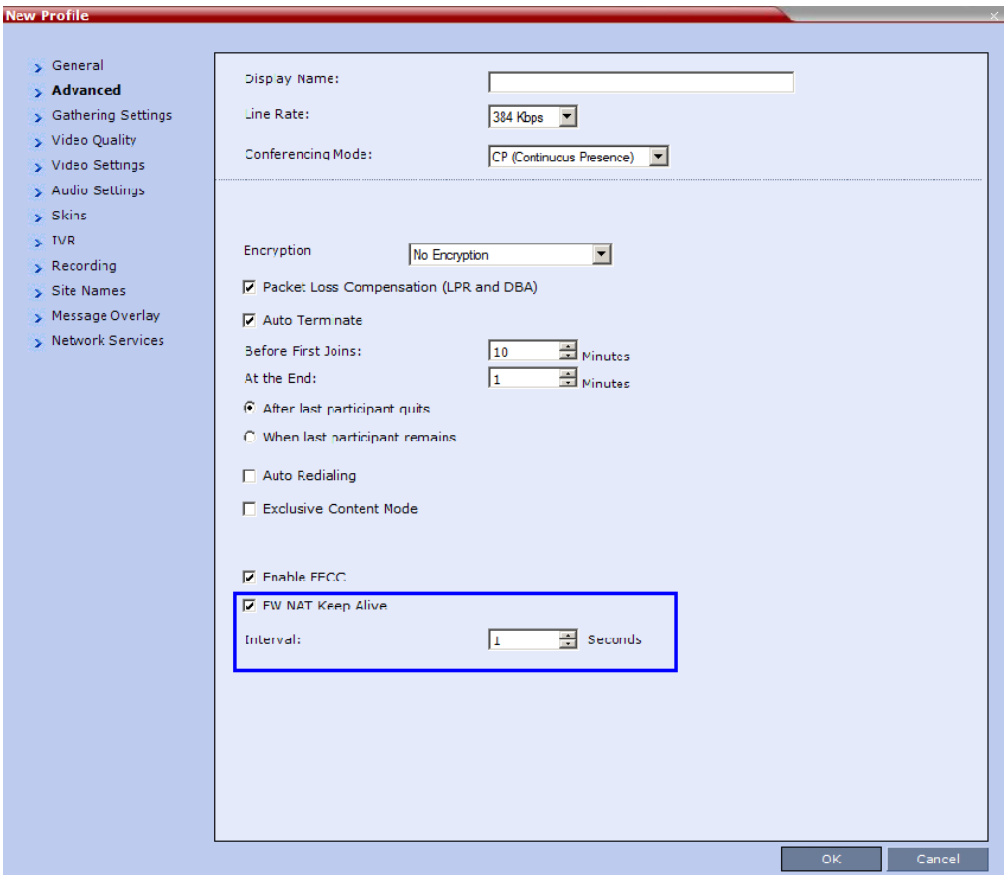
This is necessary because port mappings in the firewall are kept open only if there is network traffic in both directions. The firewall will only allow **UDP** packets into the network through ports that have been used to send packets out.

By default the Collaboration Server sends a **FW NAT Keep Alive** message every **30** seconds. As there is no traffic on the **Content** and **FECC** channels as a call begins, the firewall will not allow any incoming packets from the **Content** and **FECC** channels in until the Collaboration Server sends out the first of the **FW NAT Keep Alive** messages 30 seconds after the call starts.

If **Content** or **FECC** are required within the first 30 seconds of a call the **FW NAT Keep Alive Interval** should be modified to a lower value.

Procedure

1. Click **New Profile**, and select the **Advanced** tab.



2. Select the **FW NAT Keep Alive** check box, and if required, modify the **Interval** field within the range of **5 - 86400** seconds.

System Configuration in SBC environments

In an environment that includes **SAM** (a **Polycom SBC**), to ensure that a **RealPresence Mobile** endpoint can send content to a conference the value of the system flag `NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT` must be set to at least 3.

For more details on modifying the values of system flags, see Manually Adding a System Flag.

Network Traffic Control

The Network Traffic Control mechanism controls the level of UDP packets generated by the system. It regulates a set of queuing systems and mechanisms by which UDP packets are received and transmitted to the network router.

During a conference blast-out UDP packets can cause overloads on the network. MCU bandwidth usage can increase to above the designated conference participant line rate settings, causing network bandwidth issues such as latency and packet loss.

Three Network Traffic Control Flags are used to control the Network Traffic mechanism:

- `ENABLE_TC_PACKAGE` –

  When the flag is set to NO (default), Network Traffic Control is disabled on the Collaboration Server. Set the flag to YES to enable Network Traffic Control.

- `TC_BURST_SIZE -`

  This flag regulates the Traffic Control buffer or max burst size as a percentage of the participant line rate. In general, higher traffic rates require a larger buffer. For example, if the flag is set to 10 and the participants line rate is 2MB, then the burst size is 200Kbps.

  Default = 10

  Flag range: 1-30.

- `TC_LATENCY_SIZE -`

  This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue.

  Default = 500

  Flag range: 1-1000 (in milliseconds).

SIP Proxy Failover With Poly Clariti Core or Poly Clariti Edge

Collaboration Server systems that are part of Poly Clariti Core or Poly Clariti Edge system environment can benefit from the Poly Clariti Core or Poly Clariti Edge system's SIP Proxy Failover functionality.

SIP Proxy Failover is supported in the Poly Clariti Core or Poly Clariti Edge system's Local Clustering mode, with redundancy achieved by configuring two Poly Clariti Core or Poly Clariti Edge servers to share a single virtual IP address.

The virtual IP address is used by the Collaboration Server as the IP address of its SIP Proxy.

No additional configuration is needed on the Collaboration Server.

Should a SIP Proxy failure occur in one of the Poly Clariti Core or Poly Clariti Edge system servers:

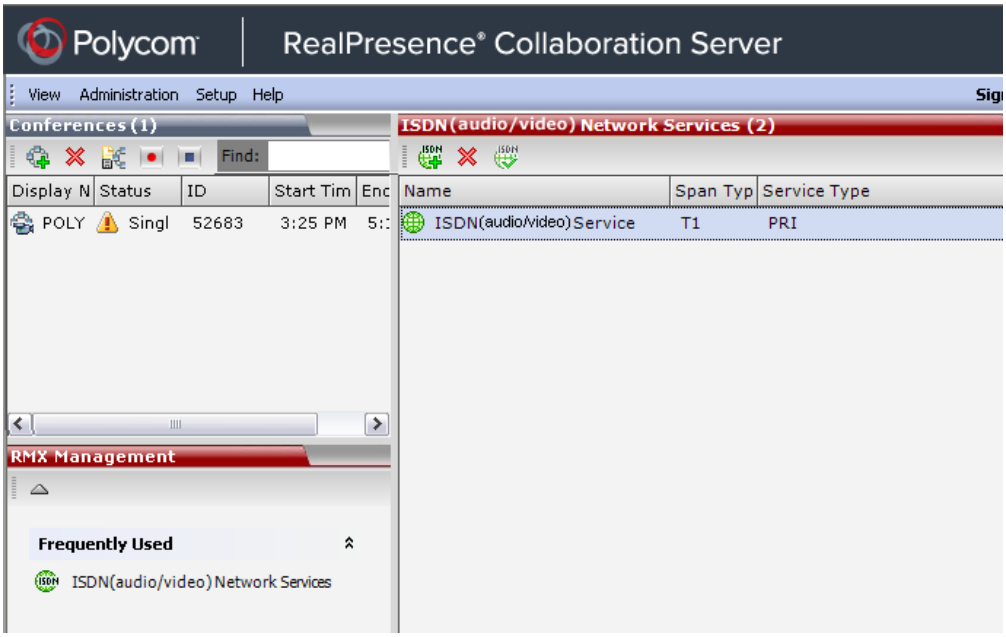
- The other Poly Clariti Core or Poly Clariti Edge system server takes over as SIP Proxy.
- Ongoing calls may be disconnected.
- Previously ongoing calls will have to be re-connected using the original IP address, registration and connection parameters.
- New calls will connect using the original IP address, registration and connection parameters.

ISDN (Audio/Video) Network Services

To enable the RealPresence Collaboration Server to function within ISDN (audio/video) network environments, network parameters must be defined for the ISDN (audio/video) Network Service.

Note: ISDN (audio/video) IP Network Services as well as ISDN (audio/video) endpoints are supported only in Polycom RealPresence Collaboration Servers 2000/4000/1800.

The configuration dialog boxes for both these network services are accessed from the **RMX Management** pane of the RMX Manager.



Note: RealPresence Collaboration Server 1800 supports ISDN (audio/video) only with 3 DSP cards installed, and with built-in ISDN (audio/video) hardware.

ISDN (Audio/Video) Network Services Overview

To enable ISDN-video and ISDN-voice participants to connect to the MCU, an ISDN (audio/video) Network Service must be defined.

You can define a maximum of two ISDN (audio/video) Network Services, of the same Span Type (E1 or T1) for RealPresence Collaboration Server. Each Network Service can attach spans from either or both cards.

Most of the parameters of the first ISDN (audio/video) Network Service are configured in the Fast Configuration Wizard, which runs automatically if an RTM ISDN card is detected in the RealPresence Collaboration Server during first time power-up. For more information, see Procedure 1: First-time Power-up in the *Polycom RealPresence Collaboration Server (RMX) 1800/2000/4000/Virtual Edition Getting Started Guide*.

Supported Capabilities and Conferencing Features:

- ISDN-video is supported only in **Continuous Presence** (CP) conferences.
- ISDN-video is supported only in Continuous Presence (CP) conferences.
- Simple audio negotiation.
- Supported video resolutions are the same as for IP.
- Supported video Protocols are the same as for IP: H.261, H.263, H.264.
- H.239 for content sharing.
- Lecture Mode.
- DTMF codes.
- Securing of conferences.

- Basic cascading between two MCUs using an ISDN-video link is available and forwarding of DTMF codes can be suppressed.

Non Supported Capabilities and Conferencing Features:

- NFAS (Non-Facility Associated Signaling)
- Leased line usage
- Restricted Channel mode
- Aggregation of channels
- E1 and T1 spans cannot operate simultaneously
- E1 and T1 spans cannot operate simultaneously
- Primary and secondary clock source configuration (they are automatically selected by the system)
- Auto detection of **Audio Only** setting at endpoint
- Auto re-negotiation of bit rate
- Additional network services (two currently supported)
- Change of video mode (capabilities) from remote side during call
- Audio algorithms G.729 and G.723.1
- FECC
- H.243 Chair Control
- T.120 data sharing protocol
- H.261 Annex D
- MIH Cascading using an ISDN-video connection as cascade link

The system administrator can use the RMX Management – ISDN (audio/video) Network Services section of the RealPresence Collaboration Server Manager to add a second ISDN (audio/video) Network Service or modify the first ISDN (audio/video) Network Service.

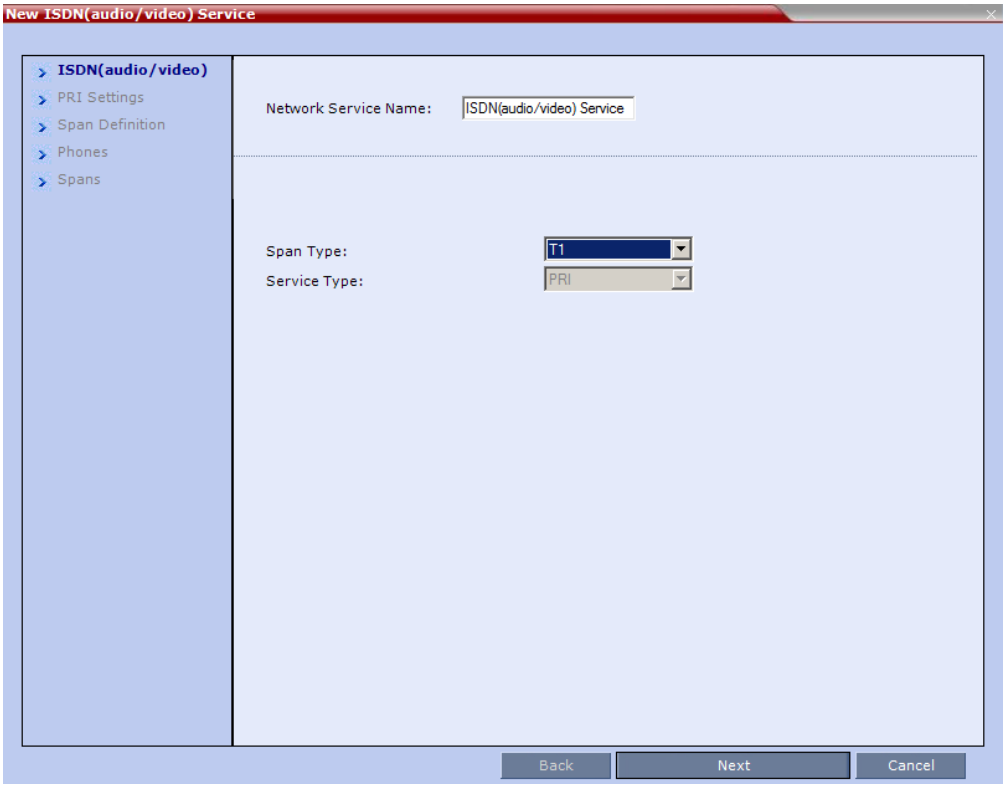
Note: A new ISDN (audio/video) Network Service can be defined even if no RTM ISDN card is installed in the system.

Obtaining ISDN (Audio/Video) Required Information

Before configuring the ISDN (audio/video) Network Service, obtain the following information from your ISDN (audio/video) Service Provider.

- Switch Type
- Line Coding and Framing
- Numbering Plan
- Numbering Type
- Numbering Type

Note: If the Collaboration Server is connected to the public ISDN-video Network, an external CSU or similar equipment is needed.

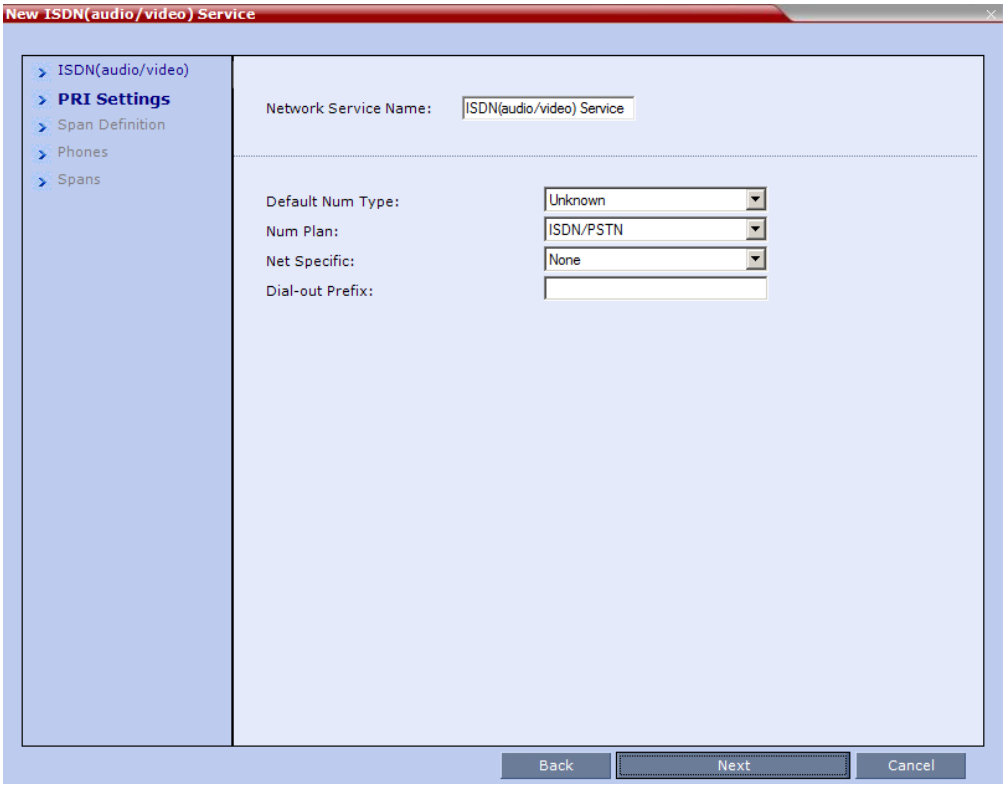


ISDN (Audio/Video) Service Settings

Field	Description
Network Service Name	Specify the service provider's (carrier) name or any other name you choose, using up to 20 characters. The Network Service Name identifies the ISDN (audio/video) Service to the system. Default name: ISDN (audio/video) Service **Note:** This field is displayed in all ISDN (audio/video) Network Properties tabs and can contain character sets that use Unicode encoding.

Field	Description
Span Type	Select the type of spans (ISDN (audio/video)) lines, supplied by the service provider, that are connected to the Collaboration Server. Each span can be defined as a separate Network Service, or all the spans from the same carrier can be defined as part of the same Network Service. Select either: • **T1** (U.S. – 23 B channels + 1 D channel) • **E1** (Europe – 30 B channels + 1 D channel) Default: T1 **Note:** E1 and T1 spans cannot operate simultaneously.
Service Type	PRI is the only supported service type. It is automatically selected.

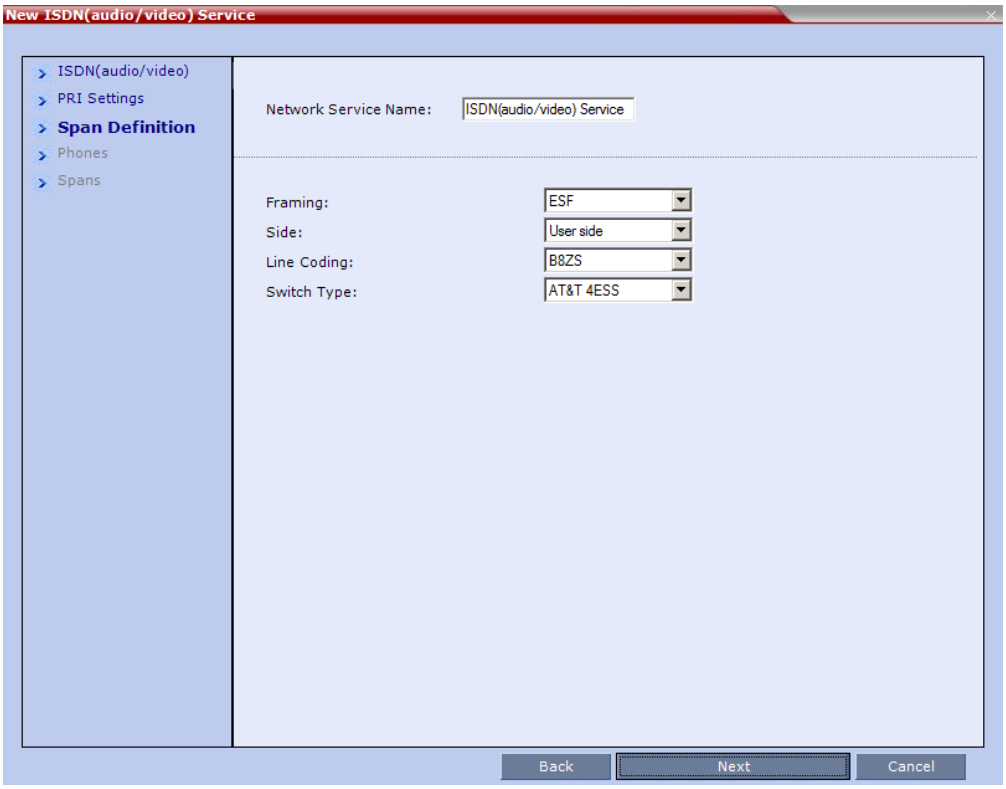
Figure 27: PRI Settings



ISDN (Audio/Video) Service Settings

Field	Description
Default Num Type	Select the Default Num Type from the list. The Num Type defines how the system handles the dialing digits. For example, if you type eight dialing digits, the Num Type defines whether this number is national or international. If the PRI lines are connected to the Collaboration Server via a network switch, the selection of the Num Type is used to route the call to a specific PRI line. If you want the network to interpret the dialing digits for routing the call, select **Unknown**. Default: **Unknown** **Note:** For E1 spans, this parameter is set by the system.
Num Plan	Select the type of signaling (Number Plan) from the list according to information given by the service provider. Default: **ISDN-video** **Note:** For E1 spans, this parameter is set by the system.
Net Specific	Select the appropriate service program if one is used by your service provider (carrier). Some service providers may have several service programs that can be used. Default: **None**
Dial-out Prefix	Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required. The field can contain be empty (blank) or a numeric value between 0 and 9999. Default: Blank

Figure 28: Span Definition

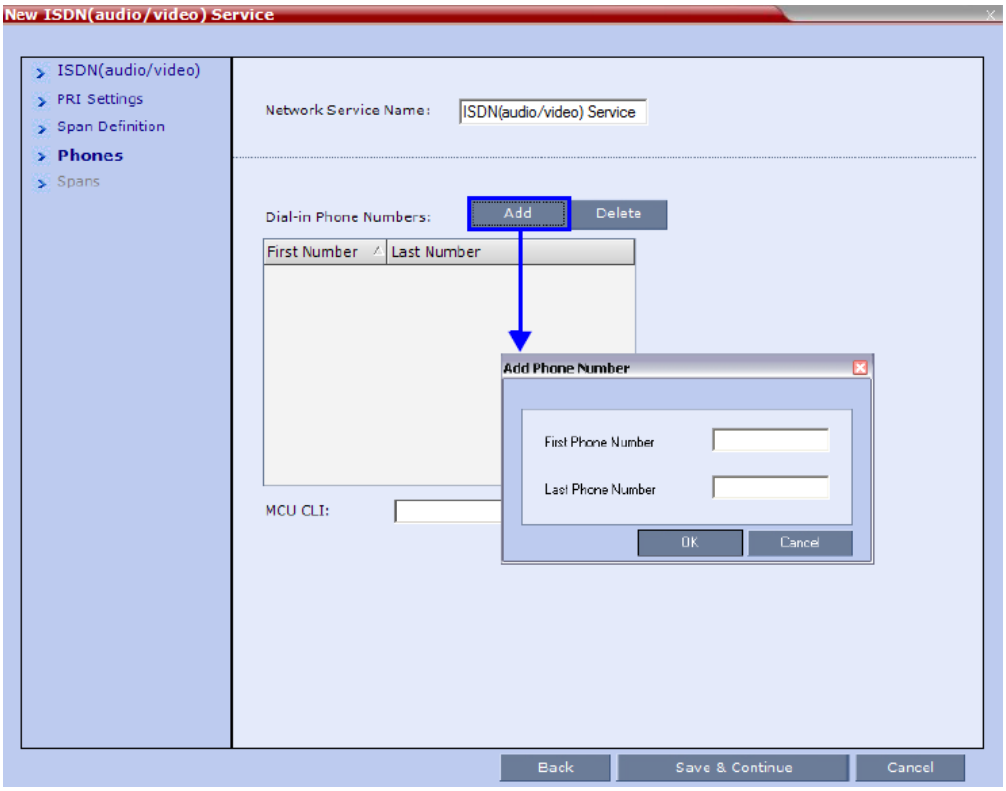


Span Definition

Field	Description
Framing	Select the Framing format used by the carrier for the network interface from the list. • For T1 spans, default is **SFSF**. • For E1 spans, default is **FEBE**.
Side	Select one of the following options: • User side (default) • Network side • Symmetric side **Note:** If the PBX is configured on the network side, then the Collaboration Server unit must be configured as the user side, and vice versa, or both must be configured symmetrically.
Line Coding	Select the PRI line coding method from the list. • For T1 spans, default is **B8ZS**. • For E1 spans, default is **HDB3**.

Field	Description
Switch Type	Select the brand and revision level of switch equipment installed in the service provider's central office. • For T1 spans, default is **AT&T 4ESS**. • For E1 spans, default is **EURO ISDN**. **Note:** For T1 configurations in Taiwan, Framing must be set to **ESF** and Line Coding to **B8ZS**.

Figure 29: Add Phone Number Dialog Opens

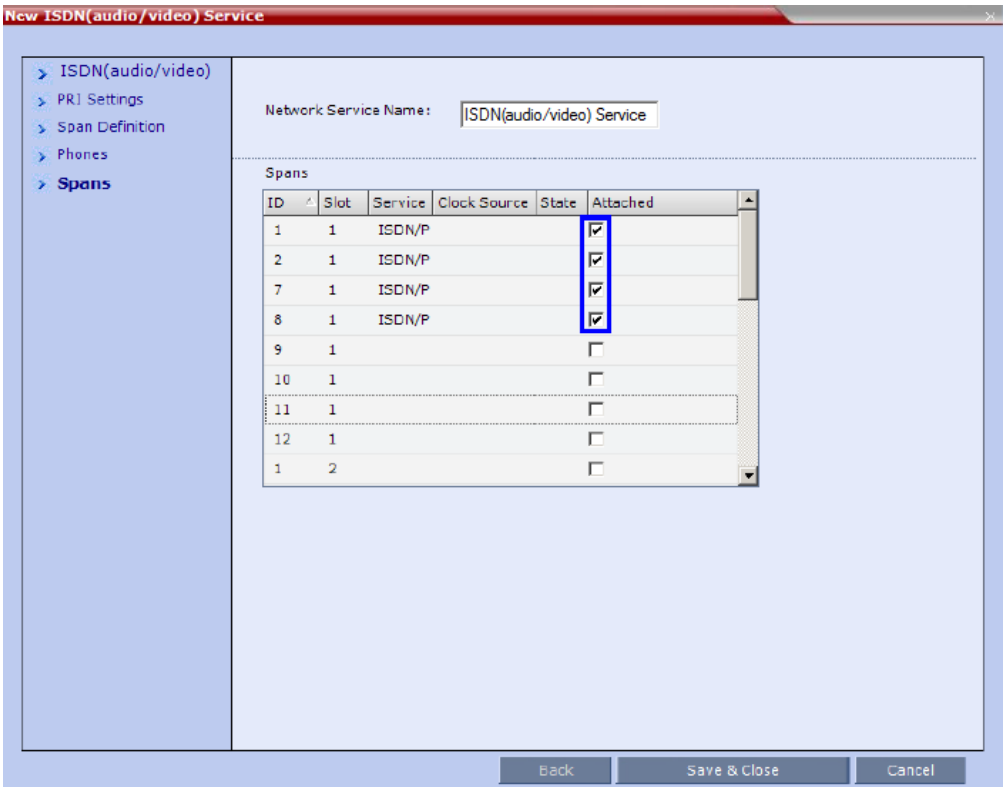


Phones Settings

Field	Description
First Number	The first number in the phone number range.
Last Number	The last number in the phone number range.

Note:
- A range must include at least two dial-in numbers.
- A range cannot exceed 1000 numbers.

Figure 30: Spans



- **ID** – The connector on the ISDN (audio/video) card (PRI1 - PRI12).
- **Slot** – The media card that the ISDN (audio/video) card is connected to (1 or 2)
- **Service** – The Network Service to which the span is assigned, or blank if the span is not assigned to a Network Service
- **Clock Source** – Indicates whether the span acts as a clock source, and if it does, whether it acts as a Primary or Backup clock source. The first span to synchronize becomes the primary clock source.
- **State** – The type of alarm: No alarm, primary-secondary or red alarm.

Polycom Open Collaboration Network

Use the Polycom Open Collaboration Network (POCN) to natively interoperate with Cisco systems that use the Cisco Telepresence Interoperability Protocol (TIP).

Note:
- You can use POCN and TIP only in AVC conferencing mode.
- You can't move participants between TIP enabled meetings and non-TIP enabled meetings during ongoing conferences.

Interoperability with Cisco TIP

RealPresence Collaboration Server can natively interoperate with Cisco Telepresence Systems (CTS) using TIP, ensuring optimum quality multiscreen, multipoint calls between the following endpoints:

- Polycom ITP Version 3.1.1
  - RPX 200
  - RPX 400
  - OTX 300

    RealPresence Collaboration Server requires a telepresence license.
- Polycom video conferencing endpoints
  - Standalone HDX
  - RealPresence Group Series 300/500
- Microsoft
  - MS Lync (using MS-ICE)
  - RTV 720p
- CTS Version 1.10
  - CTS 1300
  - CTS 3010

Conferences hosted on the RealPresence Collaboration Server can include a mix of existing endpoints that don’t support TIP and CTS endpoints.

Note: Note the following supported system requirements and limitations:

- Although Cisco legacy endpoints are interoperable with RealPresence Collaboration Server (RMX) 1800 with no DSP cards, the MCU isn’t supported for integration into third-party and partner environments.
- RealPresence Collaboration Server (RMX) 1800 Entry Level isn’t supported in POCN.
- TIP-enabled endpoints must support TIP Version 7 or higher.

Deployment Architectures

The following deployment architectures provide examples for multipoint topologies. Actual deployments depend on user requirements and available infrastructure:

- Single company with Polycom and Cisco Infrastructure
  - CTS and Polycom Telepresence Rooms in a corporate environment.
- Company to company via service provider
  - Model 1: Mixed Polycom and Cisco infrastructure at one of the companies, Cisco only infrastructure at the other.
  - Model 2: Polycom only infrastructure at one of the companies, Cisco only infrastructure at the other.

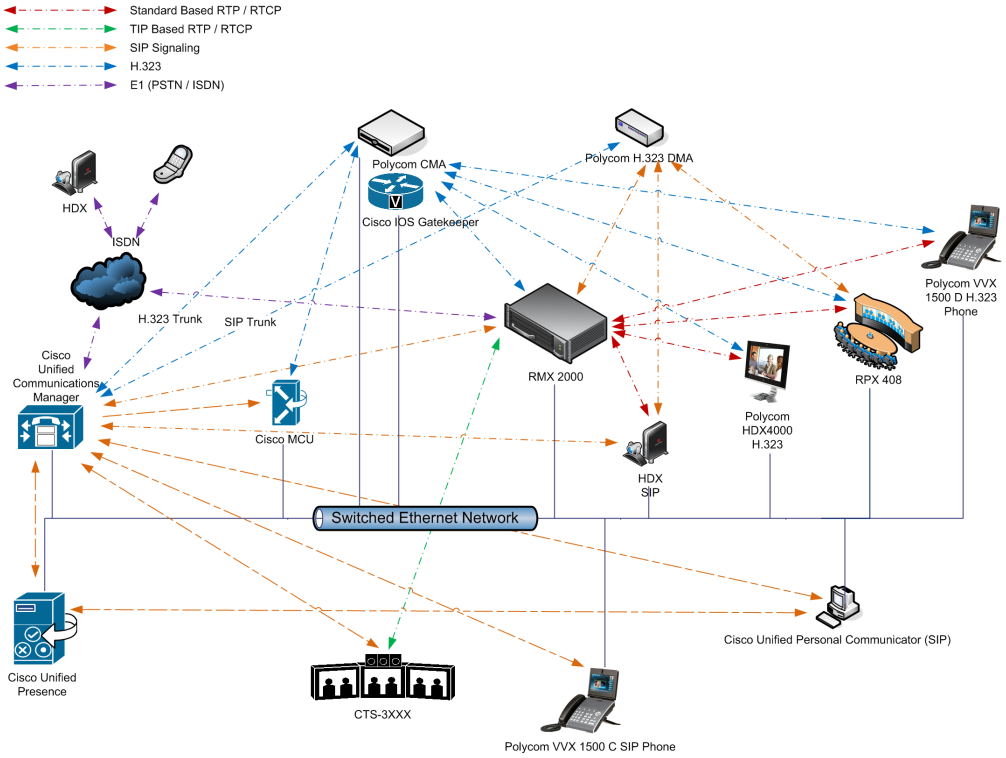
Single Company Model - Poly and Cisco Infrastructure

The deployment architecture in single company with Poly and Cisco Infrastructure - Poly endpoints using SIP shows a company that has a mixture of Poly and Cisco endpoints, room systems, and telephony

equipment that needs to enable multipoint calls between all its video and audio endpoints using the RealPresence Collaboration Server as the conference bridge.

As shown in Single company with Poly and Cisco Infrastructure - Poly endpoints using SIP, Cisco Telepresence endpoints can connect to conferences using the TIP protocol, with Poly endpoints connected to the same conferences using SIP protocol.

Figure 31: Single Company with Poly and Cisco Infrastructure - Poly Endpoints Using SIP



Poly endpoints can also connect to Entry Queues, Meeting Rooms and conferences using all protocols, including TIP and SIP.

The following table lists components and versions of the RealPresence Collaboration Server and Cisco Telepresence Systems (CTS) Integration Solution Architecture.

Cisco Solution Architecture Components

Component	Version	Description
CUCM	8.5.1, 8.6.2	Cisco Unified Communication Manager: Configure CUCM to: • Route calls to Poly Clariti Core (if present). • Route all H.323 calls to the IOS gatekeeper, which can be either Poly Clariti Core or IOS.

Component	Version	Description
IOS	15.1T	Cisco Internetwork Operating System - Gatekeeper
Endpoints (CTS)	1.7.2 (ATT), 1.8.1	Telephony, desktop, and room systems. • CTS endpoints must register to CUCM.
Cisco Unified Video Conferencing 5230	7.2	MCU
Cisco Unified Presence	8.5, 8.6	Network-based Presence and Instant Messaging.
Cisco Unified Contact Center Express	8.0, 8.5	Call distributor (ACD), interactive voice response (IVR), and computer telephony integration (CTI).
Cisco IP Polycom Communicator	7.0,8.6	Windows PC-based softphone application.
Cisco Unified Personal Polycom Communicator	8.5(2),8.5(5)	Web client for Presence and Instant Messaging.
Cisco Unified Video Advantage	2.2(2)	Video telephony functionality for Cisco Unified IP phones.
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5.1 / CUCM 8.6.1 compatible	IP Phones.
Cisco Unified IP Phones 9971	CUCM 8.5 / CUCM 8.6(2) compatible	IP Phones.
CTMS	1.7.3, 1.8.2	Cisco Telepresence Multipoint Switch.
Cisco Unified Border Element	15.1T	SBC - Voice and video connectivity from enterprise IP network to Service Provider SIP trunks.
Telepresence Server	2.2(1.54)	Telepresence Server.
VCS	X7.1	Video Communication Server / Session Manager.

Component	Version	Description
Poly Clariti Core	4.0	• Enabling of Poly Clariti Core is essential if Content sharing is active. • All SIP endpoints register to Poly Clariti Core as a SIP Proxy. • Configure Poly Clariti Core to route SIP calls (with CTS destination) to CUCM. If Poly Clariti Core isn't present in the solution architecture, SIP endpoints must register to CUCM as gatekeeper. • Configure Poly Clariti Core with a VMR (virtual meeting room) to route the incoming calls to the RealPresence Collaboration Server.
RealPresence Collaboration Server	7.6 and higher	MCU: • Functions as the network bridge for multipoint calls between H. 323, SIP, and TIP endpoints. • Interface the RealPresence Collaboration Server to CUCM using a SIP trunk, enabling CTS to join multipoint calls on RealPresence Collaboration Server. Signaling goes through the CUCM while the media in TIP format goes directly between the CTS and RealPresence Collaboration Server. • Configure the RealPresence Collaboration Server to route outbound SIP calls to the Poly Clariti Core system. • The H.323 Network Service of the RealPresence Collaboration Server should register its dial prefix with the Poly Clariti Core gatekeeper. • Predefine an Ad hoc Entry Queue, designated as Transit Entry Queue on the RealPresence Collaboration Server when the Poly Clariti Core system isn't in use.

Component	Version	Description
MLA	3.0.3	Multipoint Layout Application Required for managing multiscreen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX, or OTX systems.
Poly Clariti Manager	5.5	Poly Converged Management Application - Gatekeeper • The gatekeeper must route calls to RealPresence Collaboration Server, Virtual Edition based on the RealPresence Collaboration Server prefix registration.
Endpoints		Telephony, desktop, and room systems. • H.323 endpoints must register to the IOS gatekeeper. • Poly SIP endpoints must register to Poly Clariti Core as SIP Proxy when Poly Clariti Core is in use. • H.323 endpoints must register to the IOS gatekeeper.

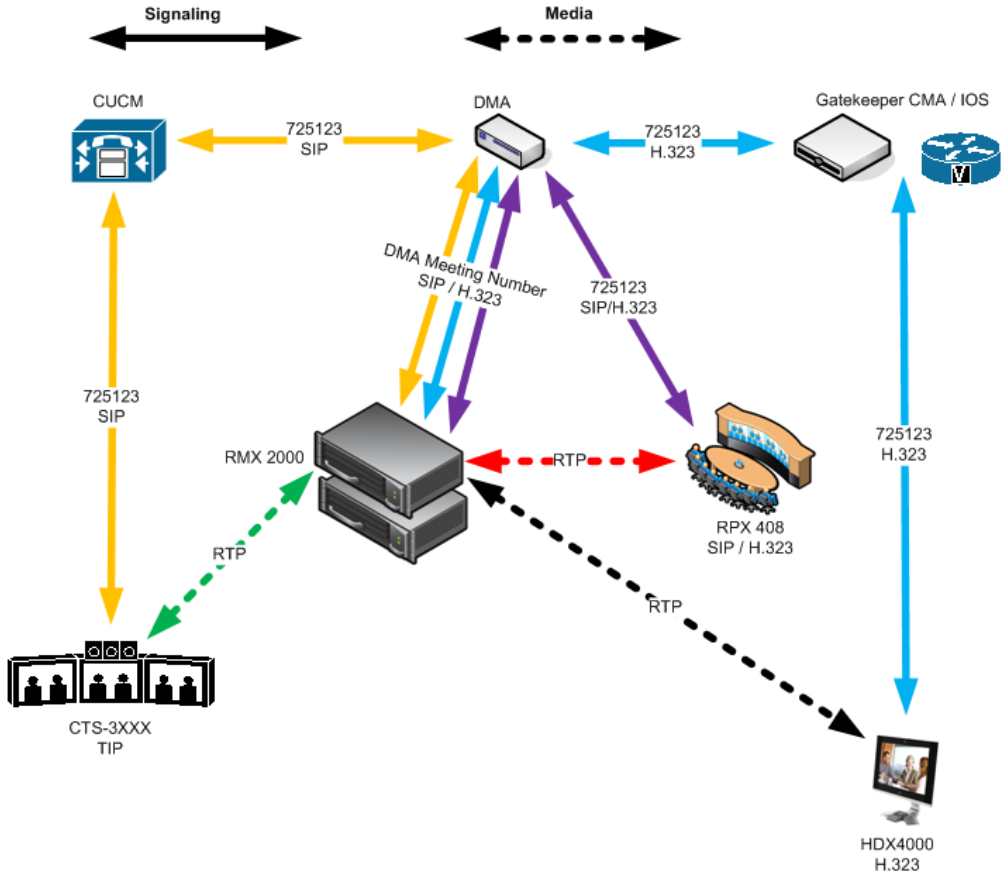
Call Flow - Multipoint Call with Poly Clariti Core

This section describes a multipoint call with Poly Clariti Core.

In this example:

- RealPresence Collaboration Server prefix in the gatekeeper: 72
- Virtual meeting room in Poly Clariti Core: 725123
- Poly Clariti Core Meeting Number: Generated by Poly Clariti Core

Figure 32: Multipoint Call with Poly Clariti Core



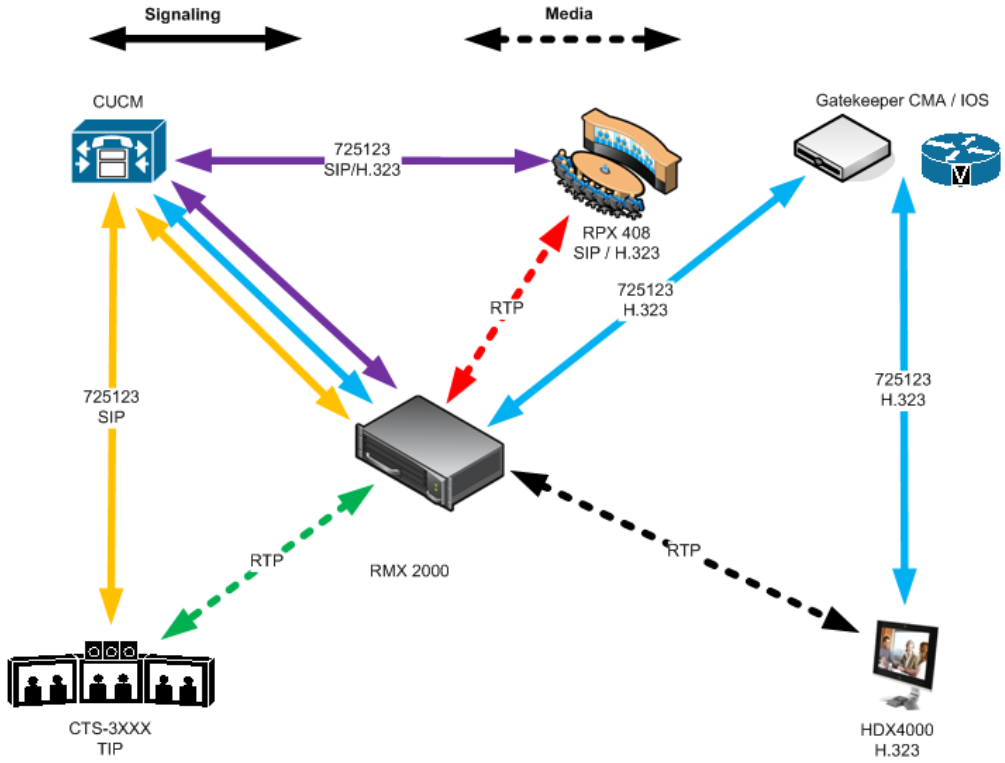
Call Flow - Multipoint Call without Poly Clariti Core

This section describes a multipoint call without Poly Clariti Core.

In this example:

- RealPresence Collaboration Server prefix in the gatekeeper: 72
- CUCM: According to its dial plan forwards calls with prefix 72 to the RealPresence Collaboration Server

Figure 33: Multipoint Call without Poly Clariti Core



Company to Company Models Using a Service Provider

Using this topology, both companies connect to a Service Provider via a Cisco Session Border Controller (SBC).

The Service Provider functions as a B2B Telepresence Exchange. This enables multipoint calls between the two companies and their respective video and audio endpoints using the RealPresence Collaboration Server as the conference bridge.

The SBC functions as a firewall that the Service Provider can configure according to Trust Relationships between two or several companies. By using this method, companies don't have to open their corporate firewalls and administer connectivity with the many companies they may need to communicate with.

The following section discusses two topology models:

- Model 1:
  - Company A has a Polycom only environment.
  - Company B has a Cisco only Environment.
- Model 2:
  - Company A has a mixed Polycom and Cisco environment.
  - Company B has a Cisco only Environment.

Model 1

The deployment architecture in Call Flows - Multipoint Call via Service Provider shows two companies: Company A and Company B.

Company A - has deployed a Poly solution including:

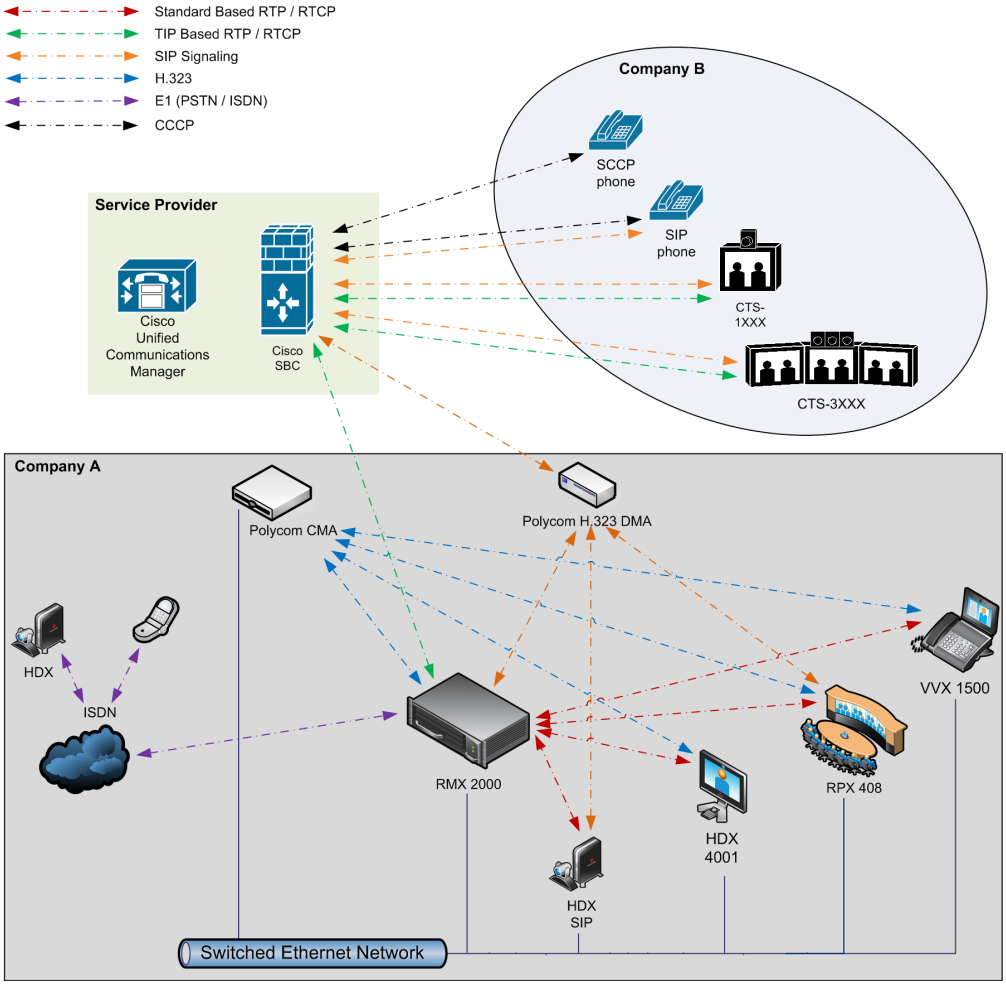
- Poly Clariti Core and/or Poly Clariti Edge
- RealPresence Collaboration Server
- MLA
- Poly Clariti Manager gatekeeper (for RealPresence Collaboration Server, Virtual Edition)
- Poly telephony and desktop endpoints.

The Poly Equipment section of the Solution Architecture Components table describes the roles of the Poly components.

Company B - has deployed a Cisco solution including:

- CTS 1000
- CTS 3000
- Cisco telephony and desktop endpoints

Figure 34: Company to Company via Service Provider - Model 1



Model 1 Call Flows - Multipoint Call via a Service Provider

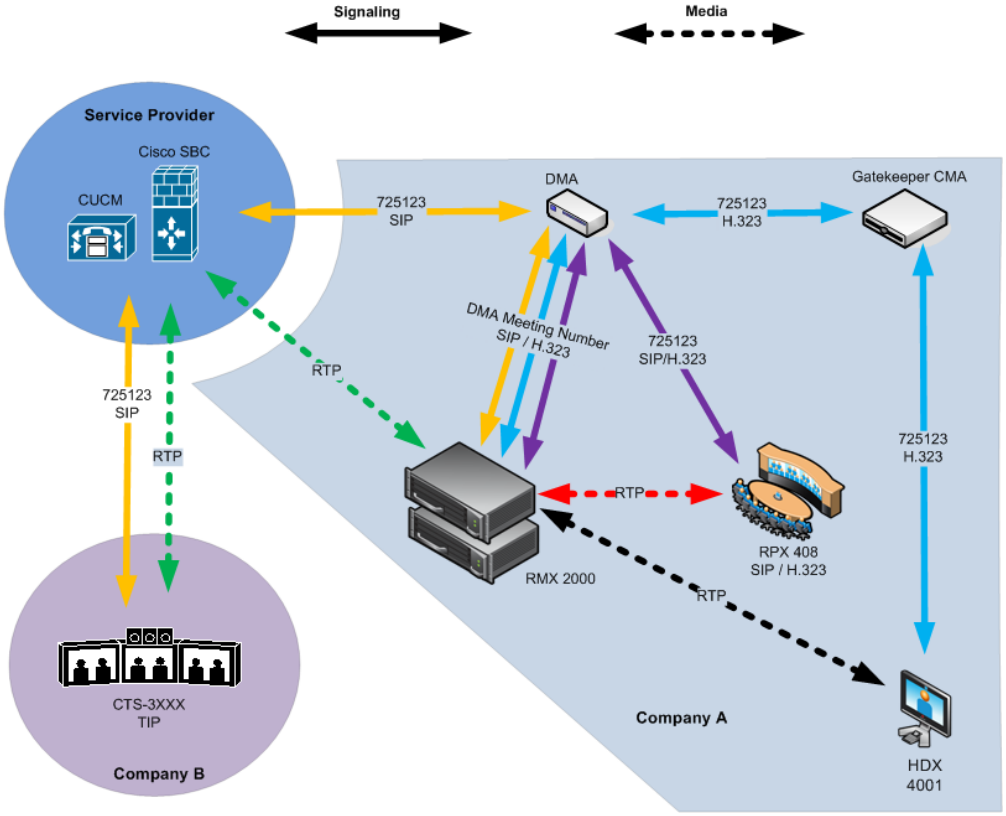
This section describes the Model 1 for a multipoint call via a service provider.

In this example:

- RealPresence Collaboration Server prefix in the gatekeeper: 72

- Virtual meeting room in Poly Clariti Core: 725123
- Poly Clariti Core Meeting Number: Generated by Poly Clariti Core

Figure 35: Multipoint Call via a Service Provider - Model 1



Model 2

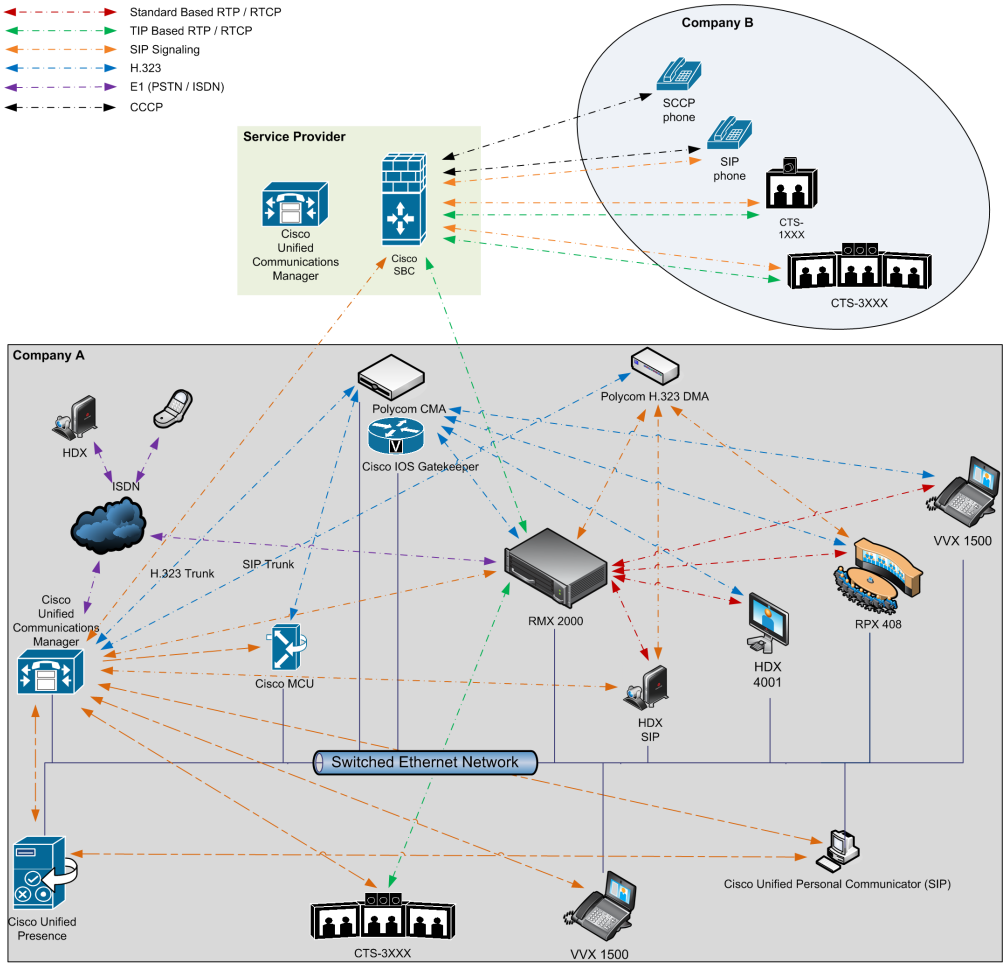
The deployment architecture in Deployment Architecture Composition shows two companies: Company A and Company B.

Company A - has the same deployment architecture as shown in Single Company Model - Polycom and Cisco Infrastructure.

Company B - has deployed a Cisco solution including:

- CTS 1000
- CTS 3000
- Cisco telephony endpoints

Figure 36: Company to Company via Service Provider - Model 2



Deployment Architecture Composition

This section describes the Deployment Architecture Composition for Company A and Company B.

The following section lists the differing or additional configuration requirements for each element of this deployment model:

Company A Solution Architecture Components

Component	Version	Description
CUCM	8.5	Cisco Unified Communication Manager: Configure CUCM with a SIP trunk to the Service Provider's SBC.

Component	Version	Description
RealPresence Collaboration Server	7.6.x and up	MCU: Configure RealPresence Collaboration Server to send and receive RTP streams to and from the Service Provider's SBC.

Company B Solution Architecture Components

Component	Version	Description
Cisco Endpoints		Endpoints should register with the Service Provider’s CUCM (or the local CUCM, if present).

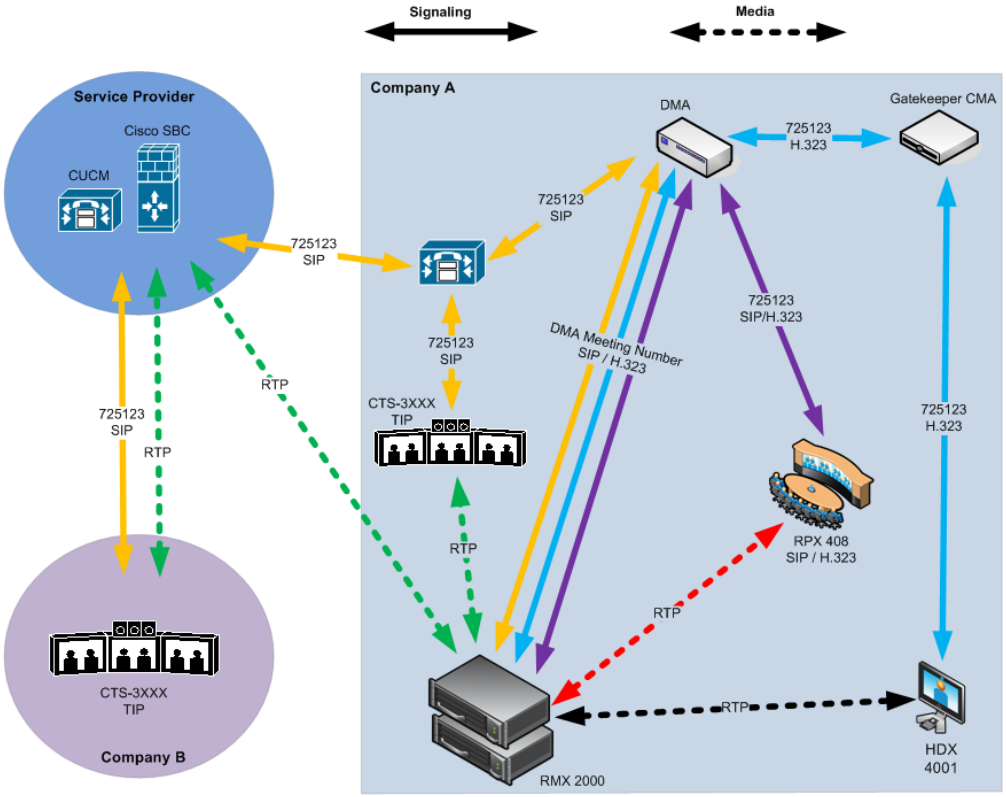
Model 2 Call Flow - Multipoint Call via Service Provider

This section describes the call flow of Multipoint Call via Service Provider for Model 2.

In this example:

- RealPresence Collaboration Server prefix in the gatekeeper: 72
- Virtual meeting room in Poly Clariti Core: 725123
- CUCM: According to its dial plan forwards calls with prefix 72 to the RealPresence Collaboration Server

Figure 37: Multipoint Call via a Service Provider - Model 2



Administration

The various deployment combinations and settings within the various deployment architectures affects the administration of the system.

Note: The Poly Clariti Core or Poly Clariti Edge acts for RealPresence Collaboration Servers 2000, 4000, and 1800 as the Poly Clariti Manager for RealPresence Collaboration Server, Virtual Edition.

Gatekeepers

This section describes the different ways to use a Poly Clariti Manager or Poly Clariti Core or Poly Clariti Edge system as a gatekeeper.

Gatekeeper Options

Option	Description
Standalone Poly Clariti Manager or Poly Clariti Core or Poly Clariti Edge system as a gatekeeper	You can use the Poly Clariti Manager or Poly Clariti Core or Poly Clariti Edge system as the only gatekeeper for the network. Bandwidth and call admission control of endpoints registered with the Poly Clariti Core or Poly Clariti Edge/Poly Clariti Manager system are split between the Poly Clariti Core or Poly Clariti Edge/Poly Clariti Manager system and the CUCM.
Standalone Cisco IOS gatekeeper	You can use the Cisco IOS Gatekeeper as the only gatekeeper for the network if the management capabilities of the Poly Clariti Manager or Poly Clariti Core or Poly Clariti Edge system aren’t required.
Neighbored Cisco IOS and Poly Clariti Manager or Poly Clariti Core or Poly Clariti Edge gatekeepers	Consider neighbored gatekeepers to make it easier to create a common dial plan and to integrate an existing Cisco telephony environment with an existing Poly network. Neighbored gatekeepers allow number translation while maintaining the existing environments.

Poly Clariti Core

You can configure the Poly Clariti Core system as a SIP proxy and registrar for the environment.

Using the Poly Clariti Core system as a SIP peer, it can host video calls between Cisco endpoints registered with the CUCM and Poly SIP endpoints registered with the Poly Clariti Core system.

CUCM

Registering Polycom SIP endpoints (voice and video) directly with CUCM, you can take advantage of supported telephone functions.

CUCM may not support the full range of codecs and features available on the Polycom equipment. CUCM supported codecs and features are used in such cases.

Configuring Cisco and Poly Equipment

The Multipoint Layout Application (MLA) is required for managing CTS 3XXX layouts whether Polycom TPX, RPX, or OTX systems are deployed or not.

MLA is a Windows application that allows conference administrators to configure and control video layouts for multipoint calls involving Polycom Immersive Telepresence (ITP) systems.

Call Detail Records (CDR) are generated on both the Poly Clariti Core or Poly Clariti Edge/Poly Clariti Manager Gatekeeper and the CUCM for reporting and billing purposes.

Guidelines

Refer to the following guidelines when configuring your deployment:

- IVR default audio files are enabled for all TIP Compatibility Modes.
- In order for the MCU to detect DTMF digits from TIP-enabled endpoints, set the system flag `SIP_REDUCE_AUDIO_CODECS_DECLARATION` to `YES`.
- If the flag is set to `NO`, the MCU can't detect DTMF digits from TIP endpoints.
- In a mixed TIP environment, there's no support for content in cascaded conferences.

Entry Queue and Virtual Entry Queue Access

TIP endpoints can dial in to conferences directly using the IVR, Entry Queue/Virtual Entry Queue, and IVR Only Service Provider.

Configuring the Conference and Entry Queue IVR Services

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The configuration process is the same for TIP and non-TIP enabled Conferences and Entry Queues.

Sharing Content

Poly and Cisco endpoints can share content within a Cisco Telepresence environment.

The content sharing experience depends on whether the endpoints are registered with the Poly Clariti Core or CUCM.

Endpoint Registration Options - Content Sharing Experience

Multipoint Calls on RealPresence Collaboration Server	Content Sharing	People+Content
Endpoints Registered to Poly Clariti Core		
HDX/ITP to HDX/ITP	Yes	Yes
HDX/ITP to Cisco CTS	Yes	Yes
Cisco CTS to HDX/ITP	Yes	No
Endpoints Registered to CUCM		
HDX/ITP to HDX/ITP	Yes	No
HDX/ITP to Cisco CTS	Yes	No
Cisco CTS to HDX/ITP	No	No

- H.239
    - Supports a variety of resolutions and frame rates.

  - Can be used with SIP and H.323 endpoints, desktop (CMAD), room systems (HDX), and ITP (OTX, RPX).
  - Not supported by Lync clients, IBM clients, and Cisco CTS endpoints.
  - Cannot be used when HDX endpoints are registered to CUCM.
- TIP
  - The resolution is fixed at XGA at 5fps, 512 Kbps.
  - Supported on HDX, Polycom ITP, and Cisco CTS systems.
- The following content compatibility options are available:
  - None (TIP not enabled) – TIP endpoints can't join the conference.
  - Prefer TIP - Both TIP and non-TIP endpoints can share content via H.264, base profile, using resolution and rate as described above.

Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag

The `MIN_TIP_COMPATIBILITY_LINE_RATE` System Flag determines the minimum line rate at which an Entry Queue or Meeting Room can be TIP enabled.

RealPresence Collaboration Server 2000, 4000, and 1800 requires CTS version 1.9.1, and if CUCM is present in the environment, set a minimum line rate of 1280 kbps in the conference profile. It rejects calls at lower line rates, therefore set the System Flag value to 1280 or higher.

RealPresence Collaboration Server, Virtual Edition requires CTS version 7. If CUCM is present in the environment, set a minimum line rate of 1024 kbps in the conference profile. It rejects calls at lower line rates, therefore set the System Flag value to 1024 or higher.

HD Video Resolutions for TIP calls are determined according to the following table:

TIP HD Video Resolution by Line Rate

Line Rate	Video Resolution
Line Rate >=3Mbps	HD1080p30
3Mbps > Line Rate >= 936kbps	HD720p30
Line Rate < 936kbps	Call is dropped.

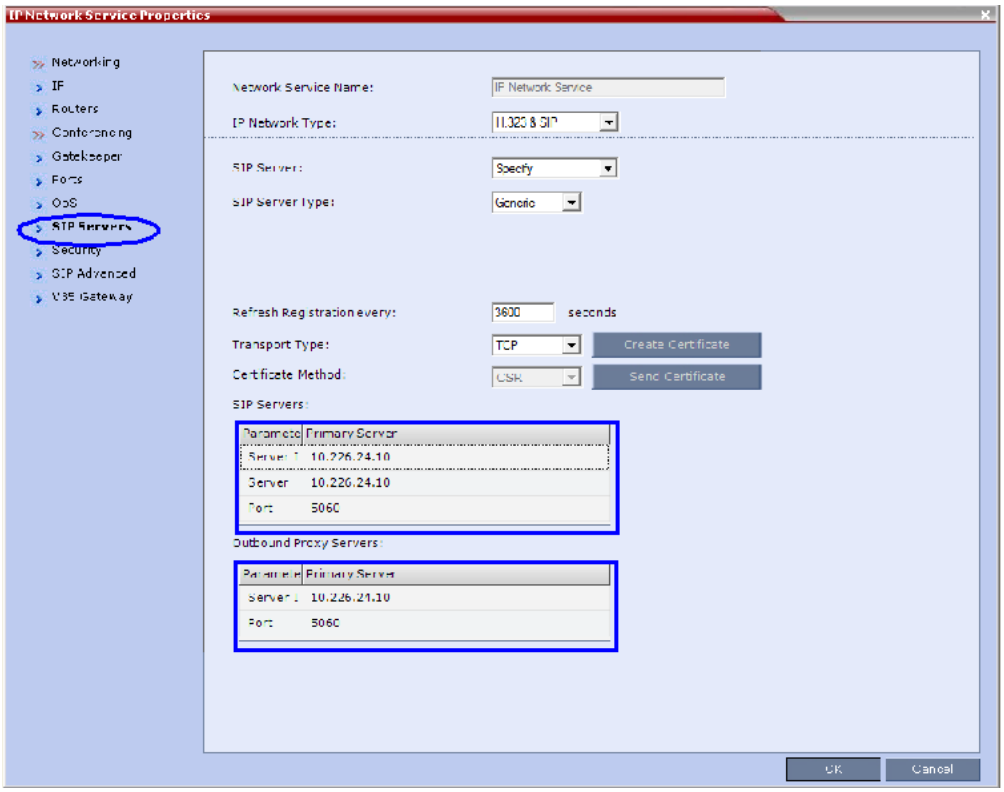
Configure RealPresence Collaboration Server to Statically Route Outbound SIP Calls to Poly Clariti Core or CUCM

Configuring the RealPresence Collaboration Server to statically route SIP calls to Poly Clariti Core or CUCM, it's important to also configure the RealPresence Collaboration Server's H.323 Network Service to register with Poly Clariti Core or Poly Clariti Manager (in RealPresence Collaboration Server, Virtual Edition) gatekeeper.

Procedure

1. In the **IP Network Services Properties** dialog, open the **SIP Servers** tab.
2. In the **SIP Server** field, select **Specify**.
3. In the **SIP Server Type** field, select **Generic**.
4. Set Refresh Registration to every **3600** seconds.
5. If not selected by default, change the **Transport Type** to **TCP**.

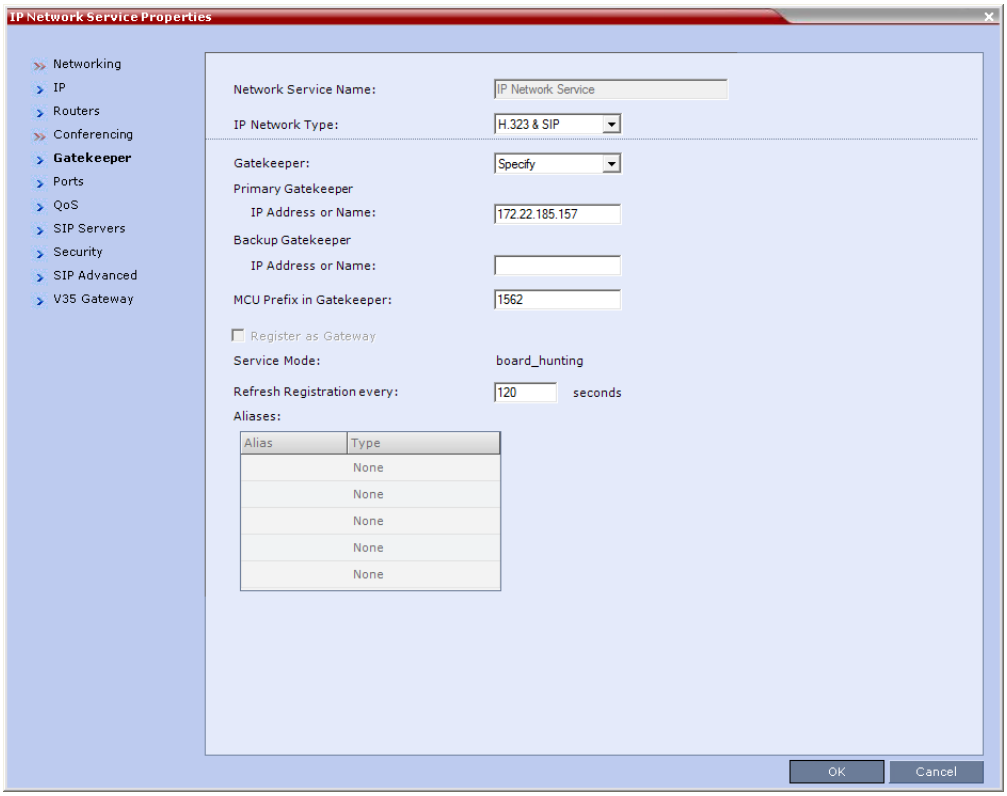
6. In the SIP Servers table:
   a. Enter the IP address of the Poly Clariti Core or CUCM in the **Server IP Address or Name** and **Server Domain Name** fields.
   b. Set the **Port** field to its default value: **5060**. Poly Clariti Core and CUCM use this port number by default.
7. In the **Outbound Proxy Servers** table:
   a. Enter the IP address in the **Server IP Address or Name** field (the same value in Step 6a).
   b. Set the **Port** field to its default value: **5060**. (By default, the Outbound Proxy Server is the same as the SIP Server.)



Configure RealPresence Collaboration Server H.323 Network Service to Register with Poly Clariti Core/ Poly Clariti Manager Gatekeeper

Procedure

1. In the **IP Network Services Properties** dialog, open the **Gatekeeper** tab.
2. In the **MCU Prefix in Gatekeeper** field, enter the prefix the RealPresence Collaboration Server uses to register with the gatekeeper.



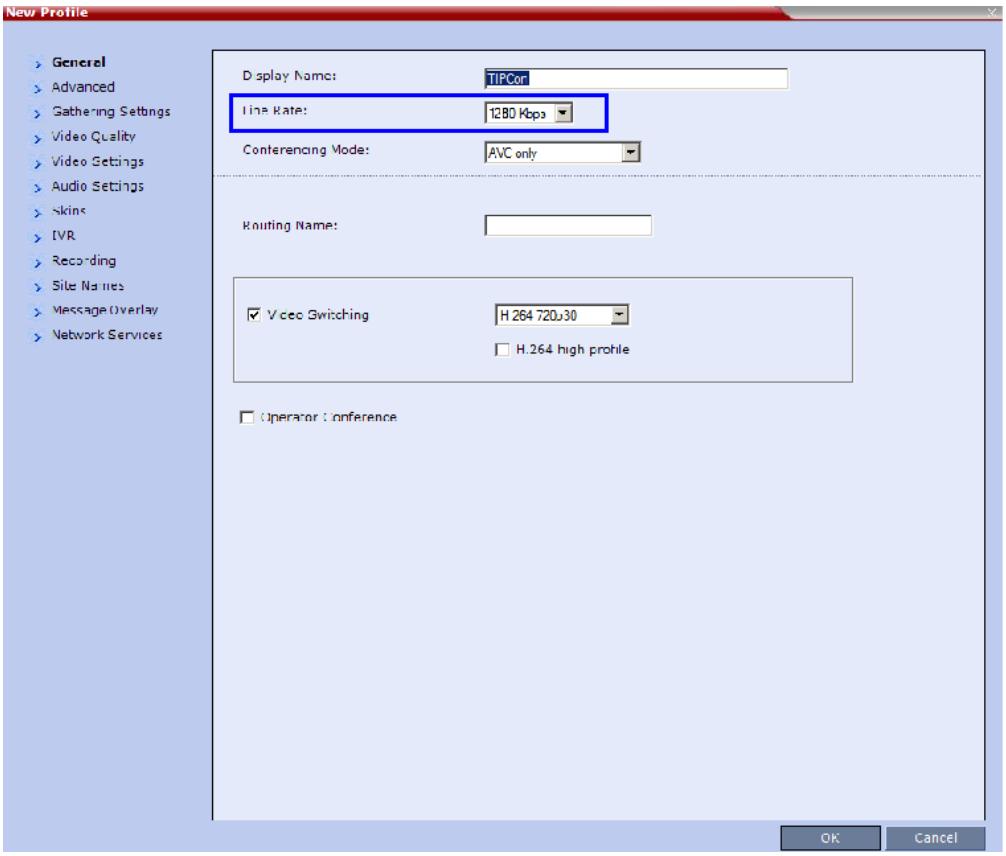
Configure a TIP Enabled Profile on the RealPresence Collaboration Server

Use the TIP enabled profiles for the Entry Queues and Meeting Rooms defined on the RealPresence Collaboration Server.

You can assign different Profiles to Entry Queues and Meeting Rooms, however they must be TIP enabled. When the Profile is TIP enabled, Gathering Settings and Message Overlay options are disabled.

Procedure

1. Create a New Profile for the Meeting Room.
2. In the **New Profile - General** tab, set the Line Rate to a value of at least that specified for the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag.



3. Open the **Advanced** tab.
4. Select Prefer TIP as the **TIP Compatibility** mode.
5. Open the **Video Quality** tab.

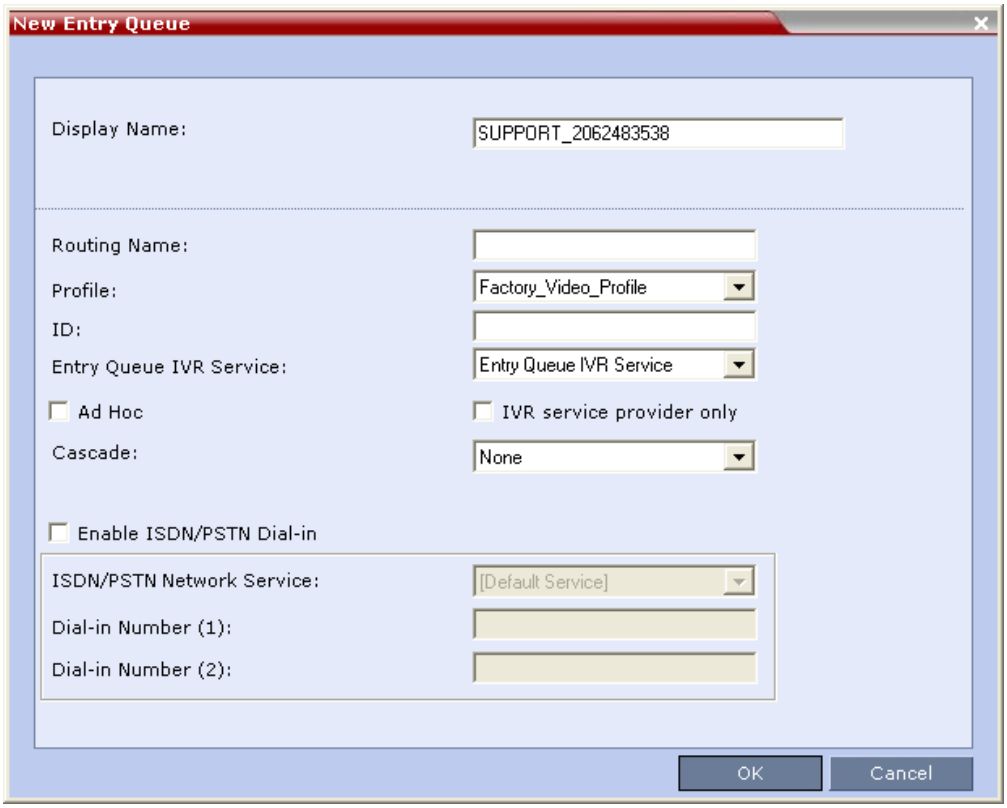
   Content Settings is disabled if **TIP Compatibility** is set to **Prefer TIP** in the **Advanced** tab.
6. Open the **Video Settings** tab.
7. Set the **Telepresence Mode** to **Auto**.
8. Assign the New Profile to the Meeting Room.

Configure an Ad Hoc Entry Queue on the RealPresence Collaboration Server

You can configure an Ad Hoc Entry Queue on the RealPresence Collaboration Server if Poly Clariti Core isn't in use.

Procedure

1. Create or select the Entry Queue as described in Entry Queues.
2. In the **New Entry Queue** or **Entry Queue Properties** dialog, select **Ad Hoc**.



3. Designate the Entry Queue as the Transit Entry Queue as described in **Transit Entry Queue**.

Configuring a Meeting Room on the RealPresence Collaboration Server

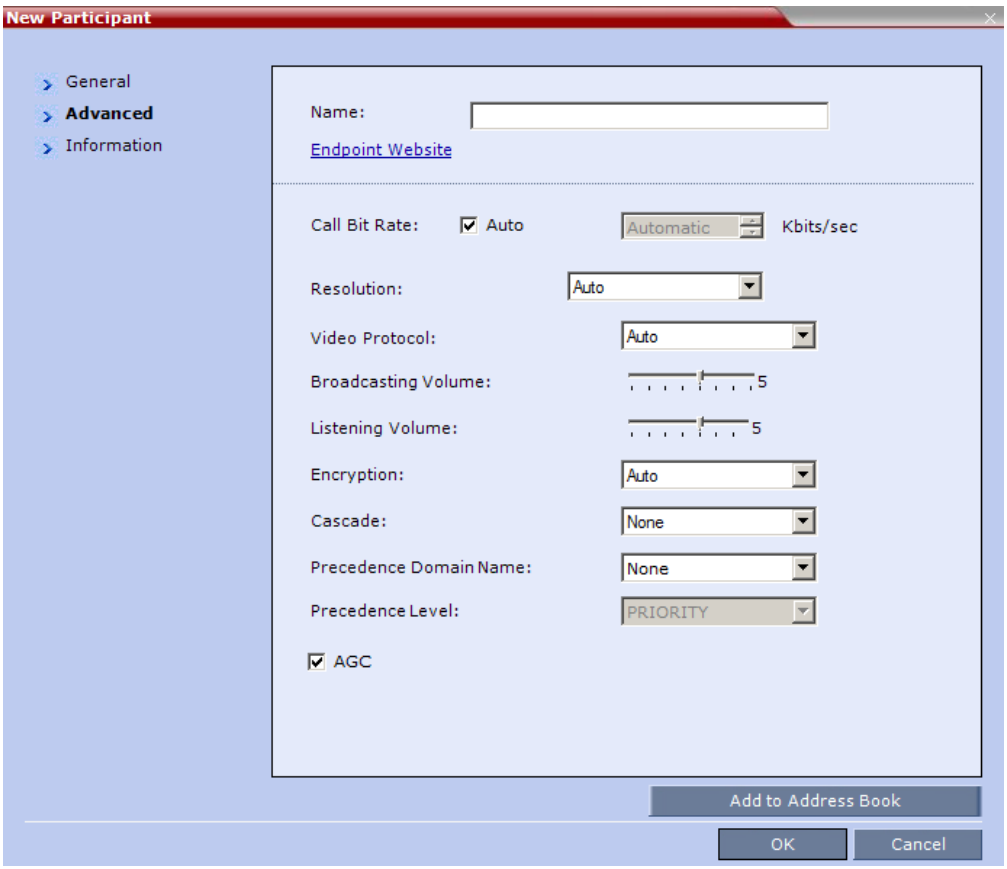
The Profile for the Meeting Room must be TIP enabled as described in Procedure 4.

Configure Participant Properties for Dial Out Calls

Configure the Participant Properties to ensure that defined participants inherit their TIP settings from the Profile assigned to the Meeting Room.

Procedure

1. Define the **New Participant - General** settings.
2. Select the **Advanced** tab.



3. Set the **Call Bit Rate** to Automatic or at least equal to or greater than the value specified by the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag.
4. Set the **Resolution** to **Auto** or at least **HD 720**.
5. Set the **Video Protocol** to **Auto** or at least **H.264**.

Collaboration with Microsoft and Cisco

This solution enables Poly, Microsoft and Cisco users, each within their own environment, to participate in the same conference running on an RealPresence Collaboration Server.

The RealPresence Collaboration Server natively interoperates with Microsoft Lync and Cisco Telepresence Systems, ensuring optimum quality multiscreen, multipoint calls between:

- Polycom Immersive Telepresence Systems (ITP) Version 3.1.1:
  - RPX 200
  - RPX 400
  - OTX 300
- Poly video conferencing endpoints
  - Standalone HDX
  - RealPresence Group Series 300/500
- Microsoft
  - MS Lync (using MS-ICE)

    - RTV 720p
- Cisco TelePresence® System (CTS) Versions 1.10
    - CTS 1300
    - CTS 3010

The deployment architecture in Single company with Poly and Cisco Infrastructure - Polycom endpoints using SIP, shows a company that has a mixture of Poly, Cisco and Microsoft endpoints, room systems, and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the RealPresence Collaboration Server as the conference bridge.

This solution enables Poly, Microsoft and Cisco users, each within their own environment, to participate in the same conference running on an MCU.

In the solution described in Single company with Poly and Cisco Infrastructure - Poly endpoints using SIP:

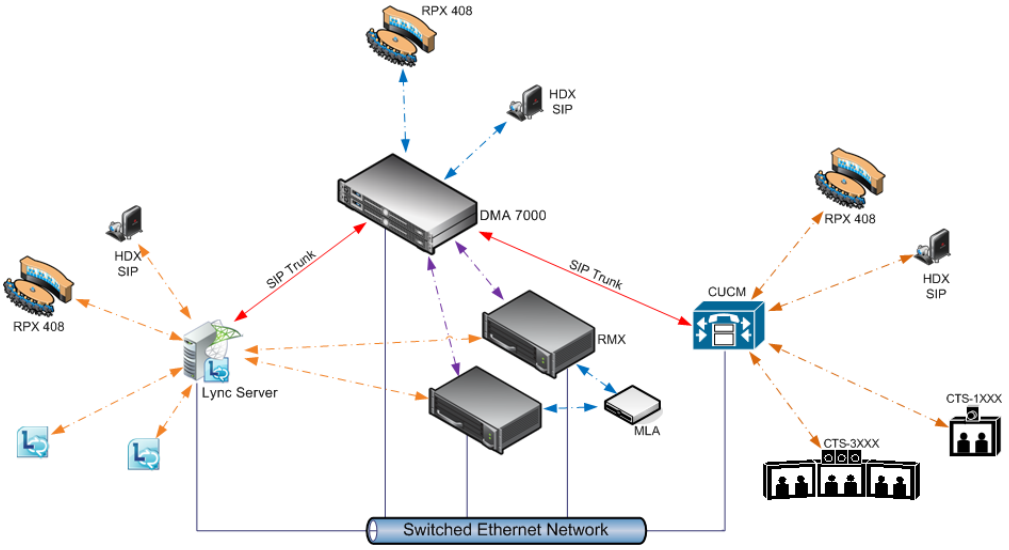
- It requires Poly Clariti Core as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the Poly Clariti Core.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- It doesn’t support dial-out calls directly from the RealPresence Collaboration Server (RMX).
- Lync Clients can’t share content with CTS
- It requires SIP trunks to the Poly Clariti Core from:
    - MS Lync as a Static Route.
    - CUCM

Deployment Architecture

Enter a short description.

- It requires Poly Clariti Core as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the Poly Clariti Core.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- Dial- out calls aren’t supported
- Lync Clients can’t share content with CTS
- It requires SIP trunks to the Poly Clariti Core from:
    - MS Lync as a Static Route.
    - CUCM

Figure 38: POCN Poly, Microsoft, and Cisco Infrastructure. Solution Architecture



POCN Poly, Microsoft, and Cisco Infrastructure. Solution Architecture Components

Component	Version
Poly	
HDX	3.0.5
Polycom® RealPresence® Media Suite	1.7
Poly Clariti Core	5.0
RealPresence Resource Manager	5.2.3, 6.0.1
ITP (OTX, RPX, ATX, TPX)	3.0.5
Conferencing for Outlook (PCO)	1.0.7
Touch Control	1.3
Microsoft	
Microsoft Lync 2010 Server	4.0.7577.223(CU10)
Microsoft Lync 2013 Server	5.0.8308.556 (CU3)
Microsoft Lync 2010 client	4.0.7577.4051 CU4
Exchange 2007 R2 SP3	8.3.213.1
Exchange 2010 SP2	14.2.247.5
Outlook 2007	12.0.6557.5001 SP2
Outlook 2010	14.0.6112.5000

Component	Version
Cisco	
CUCM	8.5, 8.6.2
Cisco Unified Personal Polycom Communicator	8.5(2),8.5(5)
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5 / CUCM 8.6(2) Compatible
CTS	1.7.4, 1.8.1
C90, C20	TC5.0

The following aren’t supported

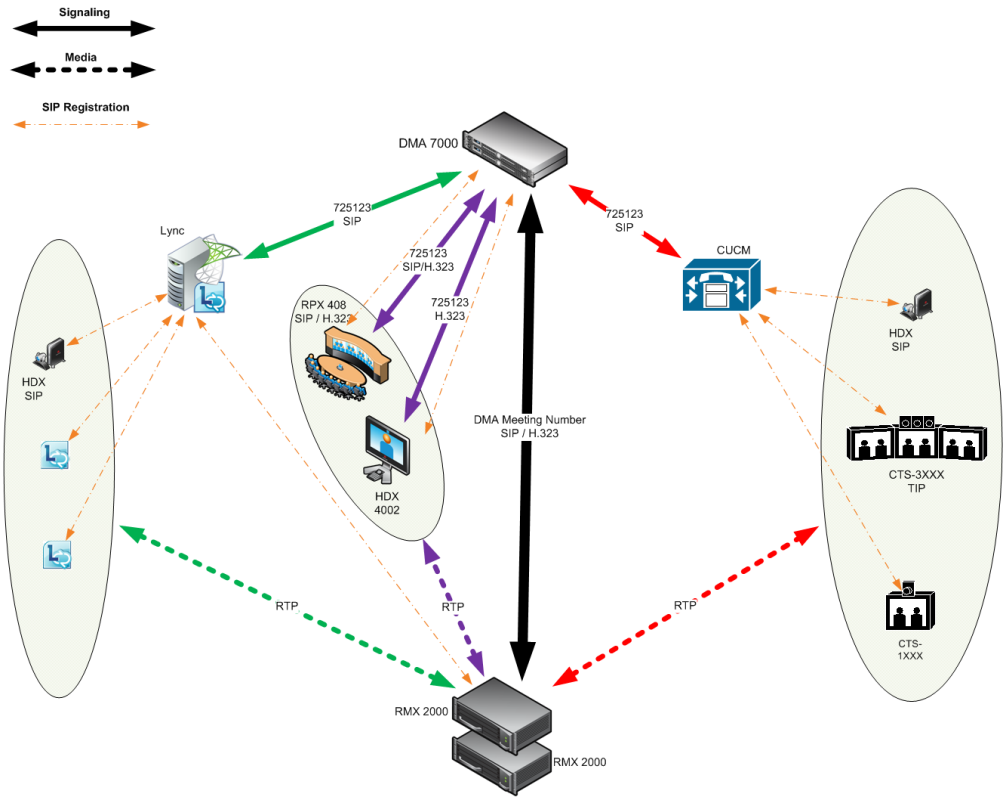
- In the Lync environment:
  - Sending or receiving Content.
  - Dial-out to Lync clients.
  - Presence of VMRs
- In the Cisco environment:
  - TLS and SRTP
  - OBTP

Call Flow - Multipoint Calls Using Poly Clariti Core

Enter a short description.

In this example:

- Endpoint registration: To either Poly Clariti Core, Lync or CUCM.
- Poly Clariti Core dial-in Prefix: 72
- Virtual meeting room in Poly Clariti Core: 725123
- Poly Clariti Core Meeting Number: Generated by Poly Clariti Core



Administration

The various deployment combinations and settings within the deployment architecture affects the administration of the system.

Poly Clariti Core

You can configure the Poly Clariti Core system as a SIP proxy and registrar for the environment as well as a Gatekeeper for dial-in H.323 calls.

When configured as a Gateway for dial-in H.323 calls, it enables H.323 endpoints to connect to the same VMR as SIP clients.

When using as a SIP peer, the Poly Clariti Core system can host video calls between Cisco endpoints registered with the CUCM, Lync Clients registered with the Lync Server, and Poly endpoints registered with the Poly Clariti Core system.

Microsoft Lync Server

Microsoft Lync Server manages presence for each registered Poly endpoint and enables video calls between Lync Clients and Poly endpoints. This allows calling of the Lync contacts without needing their addresses.

It supports RTV video, MS-ICE, and Lync-hosted conferencing when Poly endpoints are registered to Lync Server. Polycom endpoints use H.264, while Lync Clients use the RTV protocol.

CUCM

Registering Poly SIP endpoints (voice and video) directly with CUCM, you can take advantage of supported telephone functions.

CUCM may not support the full range of codecs and features available on the Poly equipment. CUCM supported codecs and features are used in such cases.

Solution Interoperability Tables

The following tables list components and versions of the RealPresence Collaboration Server, Microsoft, and Cisco Telepresence Systems (CTS) Integration Solution Architecture.

Cisco Solution Architecture Components

Component	Version	Description
CUCM	9.0.1	Cisco Unified Communication Manager: • Configure CUCM to route calls to ASR/SBC. Configure CUCM with a SIP trunk to the Service Provider's SBC. • All endpoints must register once with the CUCM • Configure SIP trunks from CUCM to Poly system components (for example, Poly Clariti Core) with Music on Hold disabled.
ASR (Cisco SBC)	100x	The Cisco Aggregation Services Routers (ASR) Series includes Cisco IOS Ex Software Internetwork Operating System - Gatekeeper. It controls and manages real-time multimedia traffic flows between IP/SIP network borders, handling signaling, data, voice, and video traffic.

Component	Version	Description
Poly Clariti Core	6.0.0_ATT_Build_25	• Poly Clariti Core is an optional component but is essential if Content sharing is to be enabled. • All SIP endpoints register to Poly Clariti Core as a SIP Proxy. • Configure Poly Clariti Core to route SIP calls (with CTS destination) to CUCM. • Configure Poly Clariti Core with a VMR (Virtual Meeting Room) to route incoming calls to the RealPresence Collaboration Server.
RealPresence Collaboration Server	8.1.1 and up	MCU: • Functions as the network bridge for multipoint calls between H. 323, SIP, and TIP endpoints. • Interface the RealPresence Collaboration Server to CUCM using a SIP trunk, enabling CTS to join multipoint calls on RealPresence Collaboration Server. Signaling goes through the CUCM while the media in TIP format goes directly between the CTS and RealPresence Collaboration Server. • Configure the RealPresence Collaboration Server to route outbound SIP calls to Poly Clariti Core. • Configure RealPresence Collaboration Server to send and receive RTP streams to and from the Service Provider's SBC.
MLA Server	3.0.5	Multipoint Layout Application Required for managing multiscreen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX, or OTX systems.

Component	Version	Description
HDX and ITP Endpoints	3.1.1.1	Telepresence, desktop, and room systems. • Poly SIP endpoints must register to Poly Clariti Core as SIP Proxy.

Microsoft Solution Architecture Components

Component	Version
Lync 2010	4.0.7577.183 CU4
Lync 2010 client	4.0.7577.4051 CU4
Exchange 2007 R2 SP3	8.3.213.1
Exchange 2010 SP2	14.2.247.5
Outlook 2007	12.0.6557.5001 SP2
Outlook 2010	14.0.6112.5000

TIP Layout Support & Resource Usage

Cisco Telepresence endpoints using TIP protocol support only one (CTS 1000) or three (CTS 3000) display screens. Therefore, Poly Telepresence endpoints adjust their display to use one or three screens as follows:

- OTX system - Works with three screens, therefore requires no adjustment and it is set to work in room switch Telepresence Layout Mode (while avoiding zooming in or out).
- RPX 2xx - This endpoint works with two screens, therefore it adjusts to use only one screen.
- RPX 4xx - This endpoint works with four screens, therefore it adjusts to use only three screens.
- Standalone HDX - behaves as the CTS 1000 and uses only one screen.
- Group system 300/500 - behaves as the CTS 1000 and uses only one screen.

The Polycom MLA Server manages the conference template layouts for Telepresence systems.

The number of screens used by each TIP-enabled endpoint is determined during the capabilities exchange phase of the dial-in connection. It affects the usage and allocation of resources used with TIP-enabled endpoints.

Resource Allocation

The MCU media processor (ART) supports up to three TIP-enabled screens as follows:

- One TIP-enabled endpoint with three screens
- Up to three TIP-enabled endpoints with one screen

TIP-enabled endpoint with three screens must be handled by the same media processor. This endpoint may fail to connect if there’s no one fully free media (ART) processor available.

The MCU always tries to fill up one media processor with up to three TIP-enabled endpoints with one screen, to save free media processors for TIP-enabled endpoint with three screens.

When monitoring an ongoing Telepresence conference with TIP-enabled endpoints (Cisco and Poly), virtual participants are used to indicate the additional screens in the Web Client. For example, if the endpoint has three screens, the system displays three participants, one for each screen.

An additional virtual Audio Only participant is used for the audio only telephone connected to the TIP endpoint.

Configuring Microsoft, Cisco and Poly Components

Carry out the following steps to configure the various system components to enable TIP.

Configure the Microsoft, Cisco and Poly Components

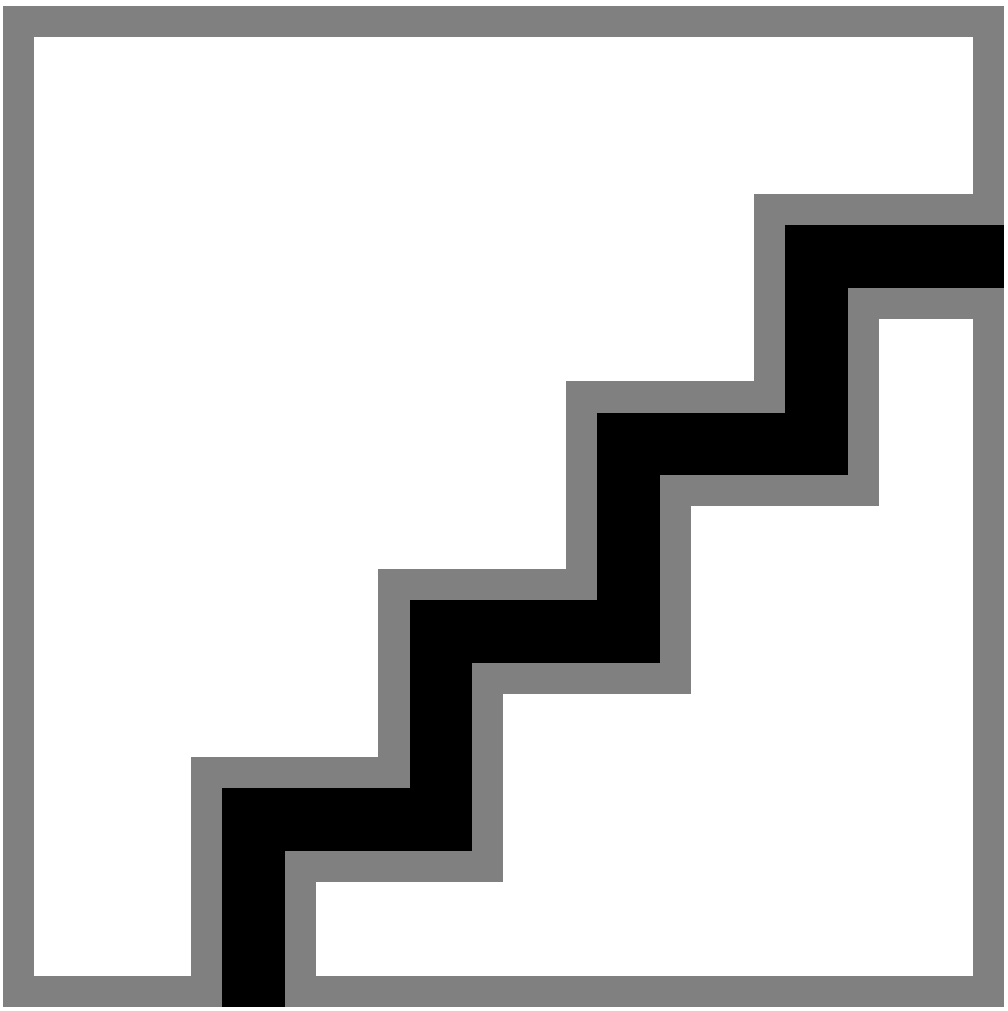
Configure the Microsoft, Cisco and Poly components to enable TIP.

Procedure

1. Configure a SIP Trunk connection between the Poly Clariti Core system and the Cisco Unified Communications Manager (CUCM).
2. Register the RealPresence Collaboration Server to the Lync Server
    a. Install a Security Certificate on the RealPresence Collaboration Server.

       You can obtain the Certificate from the System Administrator and saved on the Workstation.

    b. In the **SIP Servers** tab of the **IP Network Services Properties** dialog:
        1. Set **Certificate Method** to **PEM/PFX**.
        2. Click **Send Certificate** to display the **Install File** dialog.
        3. Browse to the saved Certificate on the Workstation, and click **Yes** to install it.



3. Register the RealPresence Collaboration Server with the Lync Server.
   a. In the IP Network Services Properties dialog, select the **SIP Servers** tab.
   b. Set SIP Server to **Specify**.
   c. Set SIP Server Type to **Microsoft**.
   d. Set Refresh Registration to every **3600** seconds.
   e. If not selected by default, change the Transport Type to **TLS**.
   f. In the SIP Servers table, enter the IP address of the Lync Server in both the **Server IP Address or Name** and **Server Domain Name** fields.
   g. In the SIP Servers table, set Port to **5061**.
   h. In the Outbound Proxy Servers table, enter the IP address in the **Server IP Address or Name** field. (The same value as entered in Step 3.f on page 124.)
   i. In the Outbound Proxy Servers table, set Port to **5061** (the same value as in Step 3.g on page 124).
4. Set the **ITP_CERTIFICATION** System Flag to **YES**.

   When set to **NO** (default), this flag disables the Telepresence features in the Conference Profile.

5. Set the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag.

   The **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag determines the minimum line rate at which a Profile can be TIP enabled.

   CTS version 1.7 requires a minimum line rate of 1024 kbps and rejects calls at lower line rates. Therefore, the System Flag value must be **1024** or higher.
6. If required, manually add and set the FORCE_720P_2048_FOR_PLCM_TIP System Flag using one of the following values:

   FORCE_720P_2048_FOR_PLCM_TIP (Default) - Forces HD 720p video resolution and a line rate of 2048kbps for all Polycom TIP-enabled endpoints that connect to the TIP-enabled Telepresence conference. This setting is the recommended setting.

   FORCE_2048_FOR_PLCM_TIP - Forces a line rate of 2048kbps for all Poly TIP-enabled endpoints connecting to the TIP-enabled Telepresence conference.

   NO_FORCE - No forcing is applied, and Poly TIP-enabled endpoints can connect to the TIP-enabled Telepresence conference at any line rate or resolution.
7. Reset the RealPresence Collaboration Server.
8. Register Poly Clariti Core to the Lync server.
9. Register the ITP endpoints to the Lync server.
10. Register Lync Clients to the Lync server.
11. Register Poly Clariti Core to the CUCM server.
12. Register CTS1000 and CTS3000 endpoints to the CUCM server.
13. Register ITP endpoints to the CUCM server.
14. Register HDX endpoints to Poly Clariti Core as Gatekeeper.
15. Open MLA to configure ITP Layouts.

    It requires MLA (Multipoint Layout Application) for managing CTS 3XXX layouts whether Polycom TPX, RPX, or OTX systems are deployed or not. MLA is a Windows® application that allows conference administrators to configure and control video layouts for multipoint calls involving Polycom Immersive Telepresence (ITP) systems.
16. Configure a TIP Enabled Profile on the RealPresence Collaboration Server.

    a. Create a New Profile for the Meeting Room.

    b. In the **New Profile - General** tab, set the Line Rate to a value of at least that specified for the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag in Procedure 1: Set the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag.

    c. Select the **Advanced** tab.

    d. Select **Prefer TIP** as **TIP Compatibility** mode.

Note: Selecting **Prefer TIP**, Video Switching, Gathering Settings, Skins, Message Overlay, Site Names, and Network Indications are disabled.

Video Resolutions

The resolution configuration dialog isn’t applicable to TIP-enabled conferences as it uses fixed settings.

HD video resolutions for TIP calls are determined according to the following table:

TIP HD Video Resolution by Line Rate

Line Rate	Video Resolution
Line Rate >=3Mbps	HD1080p30
3Mbps > Line Rate >= 936kbps	HD720p30
Line Rate < 936kbps	Call is dropped.

Content Sharing Behavior

The following tables list the system's content sharing behavior for the various combinations of TIP Compatibility mode settings and the following endpoints:

Polycom Immersive Telepresence Systems (ITP) Version 3.0.3

- RPX 200
- RPX 400
- OTX 300
- TPX HD 306
- ATX HD 300

Polycom Video Conferencing Endpoints (HDX) Version 3.0.3

- 7000 HD Rev C
- 8000 HD Rev B
- 9006
- 4500

Cisco TelePresence System (CTS) Versions 1.7 / 1.8

- CTS 1000
- CTS 3000

TIP Compatibility - None

None		Content Receiver HDX / ITP	Content Receiver	Content Receiver CTS
Content Sender	HDX / ITP	Media: Flow Control:	H.264 H.323 via H.239 SIP via BFCP	Not Connected
	CTS	Not Connected		Not Connected

TIP Compatibility - Prefer TIP

Prefer TIP		Content Receiver HDX / ITP	Content Receiver HDX / ITP	Content Receiver CTS
Content Sender	HDX / ITP	Media: Flow Control:	H.264 H.323 via H.239 SIP via BFCP TIP via Auto Collaboration	
	CTS (CTS Version 1.9.1 and higher support H.264 Content.)	Media: Flow Control:	H.264 H.323 via H.239 SIP via BFCP TIP via Auto Collaboration	

In **Prefer TIP** mode, its prerequisite that the CTS and CUCM versions support H.264 base profile content without restrictions and that the CTS version be 1.9.1 or higher and that CUCM version be version 9.0 or higher.

Content Sharing Resolutions

Endpoint registration and the dialing method affect the video and content sharing characteristics of a conference when using TIP or HDX.

Note: All systems require a TIP key for HDX; Lync also requires a TIP key for ITP.

Video and Content Sharing Resolutions

Dialing Method	Lync	CUCM	Poly Clariti Core
HDX to RealPresence Collaboration Server	• HD H.264 Video • SIP P+C • Content: XGA, 5fps • ICE	• HD H.264 Video • No Content • ICE not supported	• HD H.264 Video • SIP P+C • Content: XGA, 5fps • ICE not supported
Lync to RealPresence Collaboration Server	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints
CTS to RealPresence Collaboration Server	• HD1080p30 • TIP Content Sharing • Content: XGA, 5fps	• HD1080p30 • TIP Content Sharing • Content: XGA, 5fps	• HD1080p30 • TIP Content Sharing • Content: XGA, 5fps

Encryption

Encryption between the RealPresence Collaboration Server and CISCO environment is supported. Media is encrypted using SRTP, while control is encrypted using SRTCP.

TIP is encrypted using SRTCP. SIP is encrypted using TLS. When upgrading, the RealPresence Collaboration Server automatically creates a self-signed certificate to support encrypted communications with CISCO endpoints.

For media encryption, the RealPresence Collaboration Server first attempts to exchange keys using DTLS. If the RealPresence Collaboration Server fails to exchange keys using DTLS, SIP TLS encrypted with SDES is used to exchange media encryption keys.

Guidelines

Enter a short description.

- Ultra Secure Mode doesn't support this feature.
- Voice activity metrics and RTP aren't encrypted.
- In the event that DTLS negotiation fails, SIP is encrypted using TLS if enabled in the IP Management Network properties, SIP Servers tab. DTLS negotiation doesn't require SIP TLS.
    - In a mixed CISCO and Microsoft Lync environment, to assure encrypted communications with both CISCO endpoints and Microsoft Lync in the event of DTLS negotiation failure, the certificate defined in the IP Management Network Services properties dialog box, SIP Servers tab, should be issued by the same certificate authority that issued the certificates used by both the Microsoft Lync server and the CUCM server.
- Use the **SIP_ENCRYPTION_KEY_EXCHANGE_MODE** flag to control this feature. The possible values are:
    - AUTO (default): Normal encryption flow
    - DTLS: Only use DTLS for encryption
    - SDES: Only use SDES (SRTP) for encryption
    - NONE: Encryption is disabled
- The feature is tested using the following CISCO components:
    - Cisco CUCM Version 9.0
    - Cisco TPC Version 2.3
    - Cisco endpoints running Version 1.9.1

Enable DTLS Negotiation for Content Encryption

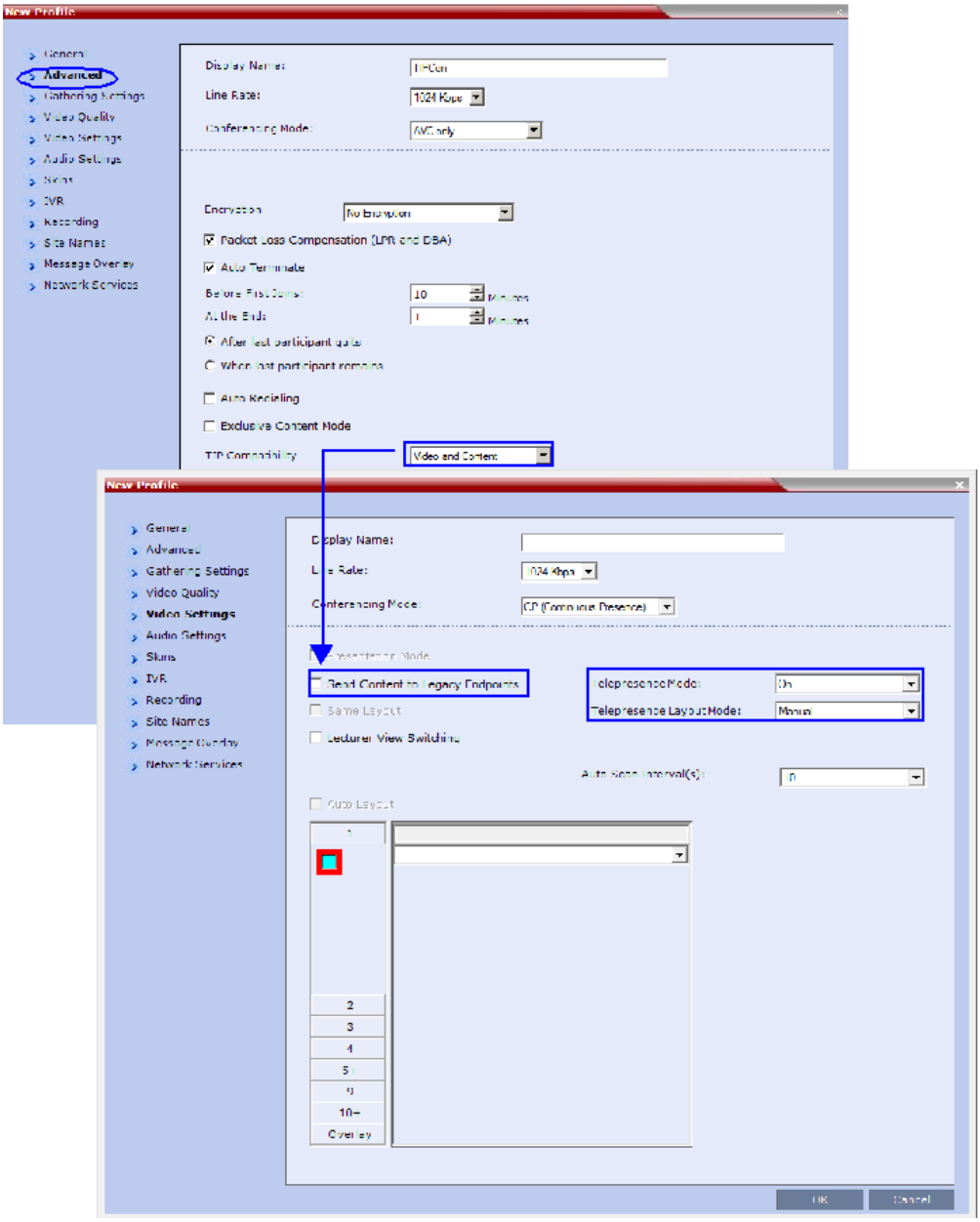
Procedure

1. In a new or existing **Profile**, open the **Advanced** tab.
2. Set **Encryption** to either **Encrypt All** or **Encrypt when possible**.
3. Set **FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE** System Flag to **NO**.

   These settings enable encrypted and nonencrypted H.323 participants to connect to encrypted or nonencrypted conferences.

    a. Open the **Video Quality** tab.

    b. Open the **Video Settings** tab.



c. Set the **Telepresence Mode to Auto/On** and select the **Telepresence Layout Mode**.

4. Assign the **New Profile** to the **Meeting Room**.
5. Configure a **Virtual Meeting Room (VMR)** on Poly Clariti Core.

Monitoring

This section describes the procedure to monitor CTS and Lync participants.

Monitor CTS Participants

You can monitor CTS participants in the **Participant List**.

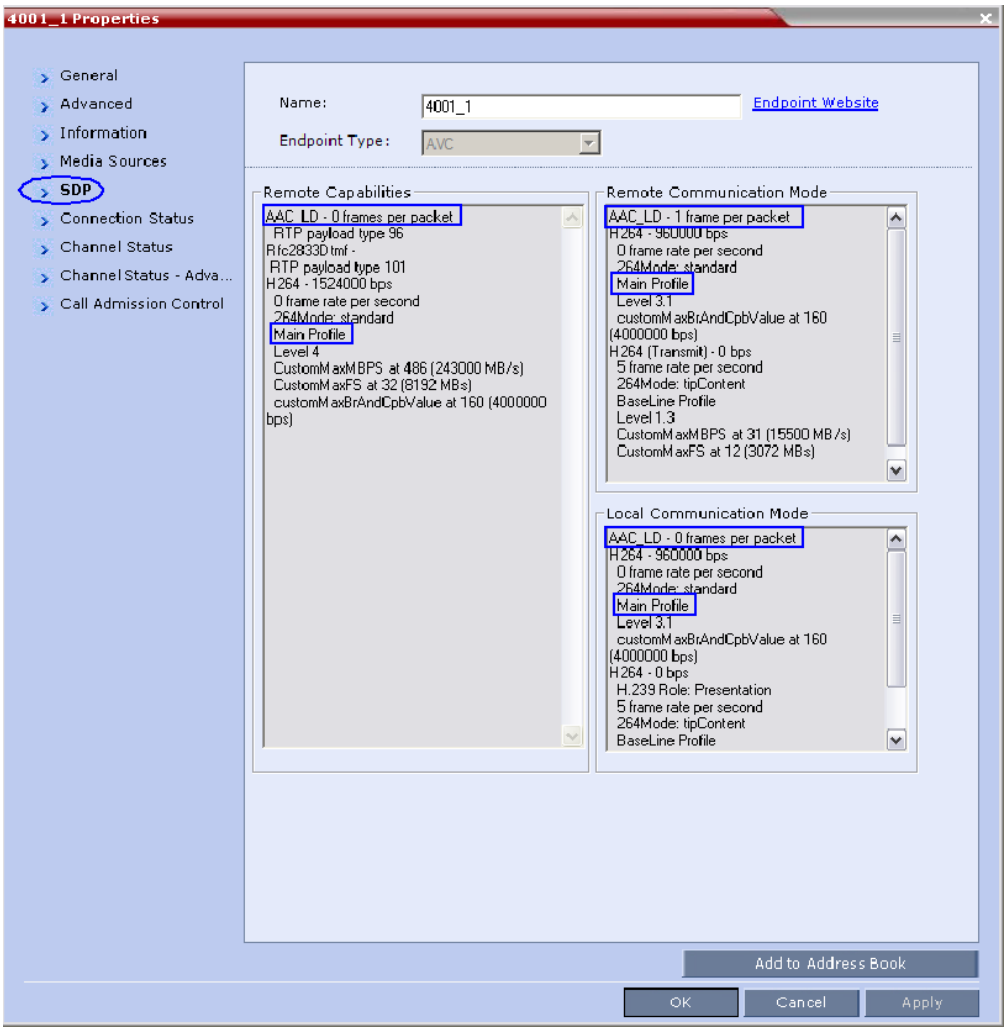
When viewing CTS systems in the Participants list, the individual video screens and the Audio Channel (AUX) of the CTS system are listed as separate participants.

Procedure

1. Do one of the following:
   - In the **Participant List** pane, double-click the participant entry.
   - Right-click a participant and select **Participant Properties**.

   The **Participant Properties - General** dialog box opens.
2. Select the SDP tab.

   The following is indicated in the **Remote Capabilities**, **Remote Communication Mode**, and **Local Communication Mode** panes:
   - **AAC_LD** - Audio protocol
   - **Main Profile** - Video protocol



Monitor Lync Participants

You can monitor CTS participants in the **Participant List**.

Procedure

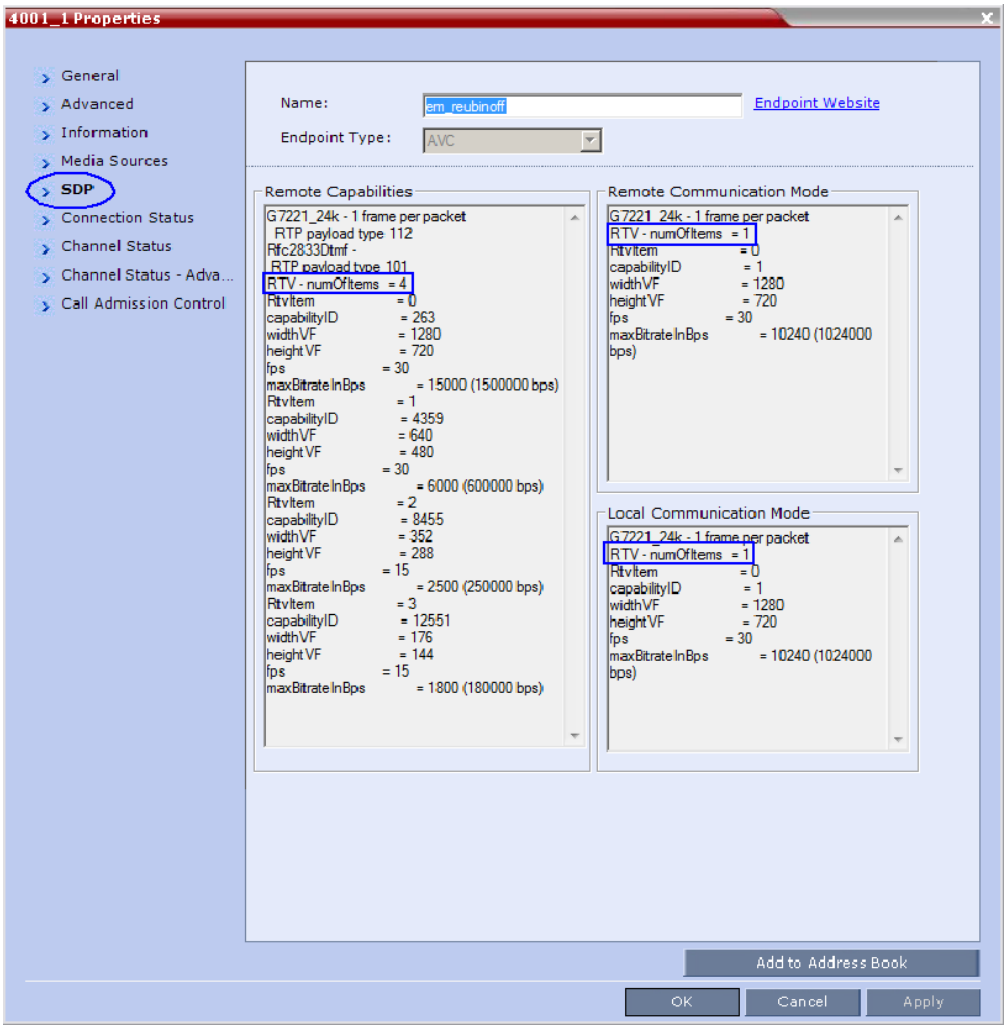
1. Do one of the following:

- In the **Participant List** pane, double-click the participant entry.
- Right-click a participant and select **Participant Properties**.

The **Participant Properties - General** dialog box opens.

2. Open the **SDP** tab.

   RTV is indicated in the **Remote Capabilities**, **Remote Communication Mode**, and **Local Communication Mode** panes:



3. Select the **Channel Status - Advanced** tab.
4. In the **Channel Info** drop-down menu, select **Video Out**.

   Media Info displays **RTV Channel Status** parameters

Known Limitations

The following may occur in the collaborative environment:

- Artifacts and ghosting may appear when Lync Clients and CTS endpoints connect to the VMR.

  Frequency: Seldom.
- Lync Client receives fast updates (Intra) from CTS 500 endpoints causing the screen to refresh repeatedly.

Frequency: Often.

- Audio volume and video quality decreases on CTS endpoints.

  Frequency: Seldom.

- CTS endpoint connects and then disconnects after a few seconds.

  Frequency: Seldom.

- Lync Clients always connect encrypted to nonencrypted conferences.
- Auto Layout sometimes ignored for CTS and Lync Clients calling through Poly Clariti Core.

  Frequency: Rarely.

- Content sent from HDX endpoint is received by all endpoints for 1 second before stopping. Conference is Content to Legacy enabled and TIP Compatibility is Prefer TIP.

  Frequency: Often.

Customizing the User Interface

Topics:

You can customize the RMX Manager user interface according to your preferences.

Each user's customizations are automatically saved for them.

Switch the RMX Management Section View

You can view the RMX Management section either as a list or as a toolbar.

Procedure

» In RMX Manager, go to the **RMX Management** section and toggle the upward or downward arrow to change from list view to toolbar view respectively.

Move Items in the RMX Management Section

You can move items between the **Frequently Used** and **Rarely Used** sections, depending on the operations you most commonly perform and the way you prefer to work with RMX Manager.

Procedure

1. In RMX Manager, go to the **RMX Management** section.
2. Drag and drop the icon of the item you wish to move to the desired position.

Restore the Default RMX Manager User Interface

You can restore the RMX Manager user interface to its factory default configuration when needed.

Procedure

» In RMX Manager, go to **View** > **Restore RMX Display Defaults**.

Customizing Multilingual Settings

Each supported language is represented by a country flag in the welcome and can be selected as the language for the RMX Manager.

The languages available for selection in the login screen of the RMX Web Client can be modified using the **Multilingual Setting** option.

Procedure

1. In RMX Manager, go to **Setup** > **Customize Display Settings** > **Multilingual Setting**.
2. Select the check boxes of the languages to be available for selection, and click **OK**.
3. Log out from the RMX Web Client and log back in for the customization to take effect.

Enable Japanese Font Display in a Meeting Room (MR) Conference

RealPresence Collaboration Server 1800/2000/4000 and Virtual Edition can now display Japanese characters in site name, message overlay, and Gathering slides using the appropriate font and style, based on the system configuration.

Procedure

1. Go to the RMX Manager, then select Japanese in **Setup** > **Customize Display Settings** > **Multilingual Setting**.
2. If Gathering Phase is enabled for the conference, go to the corresponding conference profile and select **Japanese** from the drop-down menu under **Profile Properties** > **Gathering Settings** > **Displayed language**.

Enable Japanese Font Display in a VMR Conference

RealPresence Collaboration Server can display Japanese characters in site name, message overlay, and Gathering slides using the appropriate font and style, based on the system configuration.

Procedure

1. Log in to the Poly Clariti Core system that hosts the VMR meeting.
2. Go to **DMA Service Config** > **Conference Manager Settings** > **Conference Templates**.
3. In the conference template settings, select **Japanese** for the **Font for text over video** option.
4. Optional: If **Gathering Phase** is enabled for the conference, select **Japanese** from the drop-down menu under **Polycom MCU Gathering Settings** > **Displayed language**.

Customizing the Banner Display

The login screen and main screen of the RMX Manager can display informative or warning text banners.

These banners can include general information or they can caution users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

Procedure

» In RMX Manager, go to **Setup** > **Customize Display Settings** > **Banners Configuration**.

Conference Management

Topics:

This section includes information on common and advanced tasks for managing conferences.

- Conference Profiles and Templates
- Advanced Conferencing Profile Features
- Configuring the Address Book
- Scheduling and Starting Conferences
- Working with Active Conferences
- Cascading Conferences
- Operator Conferences and Assistance
- Entry Queues, Ad Hoc Conferences, and SIP Factories

Conference Profiles and Templates

Topics:

Use conference profiles and conference templates to enable a *standalone* RealPresence Collaboration Server to implement standard and manageable conferencing experiences for your conferencing community.

Note: If you have a Poly Clariti Core system, create conference templates and manage conferencing parameters on the Poly Clariti Core system and not on the RealPresence Collaboration Server.

The Poly Clariti Core system has more flexibility, as it can associate conferencing experiences with users, conference rooms, or enterprise groups. It also offers more features and functions.

Related Links

Move Participants Between Conferences on page 181

Conference Profiles

This section describes the Conference Profile features and capabilities.

In a standalone RealPresence Collaboration Server environment, you can enable the following conferencing capabilities and features using conference profiles:

- Conferencing mode - Continuous Presence (CP) and Advanced Video Coding (AVC), Video Switching, Scalable Video Codec (SVC), or mixed CP and SVC
- Video line rate
- Conference skin and screen layout
- Entry queue (EQ) and interactive voice response (IVR) experiences
- Content sharing features
- Recording features
- Endpoint protocols supported
- Conference messaging
- Polycom Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA)
- Encryption

View the List of Conference Profiles

A RealPresence Collaboration Server has three default conference profiles based on conferencing mode.

The three default conference profiles are:

- Factory_Video_Profile
- Factory_SVC_Video_Profile

- Factory_Mix_Video_Profile

Procedure

» In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.

Add a Conference Profile

Conference profiles specify the parameters best suited for your conferencing software and hardware environments.

Use the default profiles or add new profiles specific to your conferencing environment.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** pane, click **New Profile**  .
3. In the **Display Name** field, enter a unique and identifiable name for the profile and select the required **Conferencing Mode**.

   The **New Profile** tabs and options change based on the selected conferencing mode and the MCU model (Appliance Edition or Virtual Edition). Only supported options are available on each tab.

   - When you select **CP (Continuous Presence)**, all tabs are available.
   - When you select **SVC Only**, the **General**, **Advanced**, **Video Quality**, **Video Settings**, **Audio Settings**, **IVR**, and **Network Settings** tabs are available.
   - When you select **CP and SVC**, all tabs except the **Gathering Settings** tab are available.
4. Select and edit the parameters you wish to define.
   - General Parameters
   - Advanced Parameters
   - Gathering Settings - Not available when you select **CP and SVC** or **SVC Only** conferencing modes.
   - Video Quality Parameters
   - Video Settings Parameters
   - Audio Settings Parameters
   - IVR Parameters
   - Recording Parameters - Not available when **SVC Only** conferencing mode is selected
   - Site Names Parameters - Not available when **SVC Only** conferencing mode is selected
   - Message Overlay Parameters - Not available when **SVC Only** conferencing mode is selected
   - Network Services Parameters
   - Layout Indications Parameters - Not available when **SVC Only** conferencing mode is selected
5. Click **OK** to save the new profile.

Related Links

Conference Profile Parameters on page 138

Conference Profile Parameters

The following tables list the conference parameters that you can enable on the RealPresence Collaboration Server.

General Parameters

Field/Option	Description
Display Name	Provide a meaningful name for the profile.
Line Rate	Specifies the maximum bit rate at which endpoints can connect to conferences. The line rate is the combined video, audio and content rate. **Note:** It doesn't support down-speeding. As a result, ISDN-video calls consume bandwidth resources according to the line rate specified in the conference profile. For example, if the conference line rate is 512 Kbps, ISDN-video calls connecting at lower line rates (256 Kbps) consume the bandwidth resources of 512 Kbps calls. When no bandwidth resources are available, it rejects ISDN-video calls before it exhausts media card resources.
Conferencing Mode	Choose one of the following: • **Continuous Presence (CP)** - (also known as Advanced Video Coding (AVC)) This mode supports the H.264 AVC compression standard. In CP mode, the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. • **SVC Only** - This mode supports an extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC). You can tailor the number of enhancement layer streams sent to a device to fit the bandwidth available and device capabilities. SVC conferencing is only possible with endpoints that support H.264 SVC. Enabling this setting disables many of the other template settings. • **CP and SVC** (also known as or mixed mode) - This mode enables both AVC-only endpoints and endpoints supporting SVC to join a conference.
Routing Name	Assign a routing name or allow the system to assign one automatically. • Entering all ASCII text in the **Display Name**, the server also uses the same as the **Routing Name**. • Entering any combination of Unicode and ASCII text (or full Unicode text) in the **Display Name**, the server uses the ID (such as Conference ID) as the **Routing Name**.
Video Switching	Available only for Appliance Editions. An alternative to **Continuous Presence (CP)** mode, this option provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen while the current speaker sees the previous speaker. When enabled: • The minimum available line rate is 768 Kbps. • All endpoints must connect at the same line rate. The endpoints not supporting the specific line rate connect in voice-only mode. • You can also enable H.264 high profile, which allows the conference to use Poly's bandwidth-conserving H.264 High Profile codec.

Field/Option	Description
Operator Conference	Not available in **Video Switching** mode. Enable this option to define the profile of an operator conference.

Advanced Parameters

Field/Option	Description
Encryption	Specifies the media encryption setting: • **No encryption** - All endpoints join unencrypted. • **Encrypt when possible** - Endpoints supporting encryption join encrypted; others join unencrypted. • **Encrypt all** - Endpoints supporting encryption join encrypted; others can't join.
Packet loss compensation	Enables Polycom Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA). • Polycom Lost Packet Recovery (LPR) creates additional packets containing recovery information. Use this information to reconstruct packets lost during transmission. By default, Polycom Lost Packet Recovery (LPR) is in enable mode for CP conferences and it is in disable mode for Video Switching (VSW) Conferences. You can enable it for VSW conferences but H.320 and SIP participants won't be able to connect. • DBA allocates the bandwidth needed to transmit the additional packets.
Auto Terminate	Not available in **Operator Conference** mode. Not recommended for **SVC Only** conferences. When enabled, the MCU automatically ends the conference after meeting the specified termination conditions. Terminate conditions include: • Minutes **Before First Joins** • Minutes **At the End** ◦ **After last participant quits** ◦ **When last participant remains**
Auto Redialing	Enables the MCU to automatically redial H.323 and SIP participants that disconnect abnormally from a conference.
Exclusive Content Mode	When enabled, if a participant is broadcasting content, it prevents other participants from interrupting with their own content if the current content stream is active.
Enable FECC	When enabled, participants can control the zoom and PAN of other endpoints in the conference via the FECC channel.
FW NAT Keep Alive	Specifies the intervals for the MCU to send media stream keep-alive messages to the RTP, UDP, and BFCP channels. It sends these messages when receiving calls through a firewall or session border controller (SBC). The acceptable interval is within the range of 1 - 86400 seconds.

Field/Option	Description
TIP Compatibility	Available only in **CP (Continuous Presence)** conferencing mode. Enables compatibility with Cisco Telepresence Systems (CTS) and Telepresence Interoperability Protocol (TIP), either for video only or for both video and content. Setting **Prefer TIP**, for endpoints supporting TIP it uses TIP content and for endpoints not supporting TIP it uses non-TIP content. Requires a minimum line rate of 1024 Kbps and HD resolution (720 or better). **Note:** Enabling an option other than **None**, disables the **Gathering Settings** options.
MS AVMCU Cascade Mode	When integrated with a Microsoft Skype for Business environment, controls behavior of the cascade link with the Skype for Business AVMCU. • **Resource Optimized** - It limits the cascade link between both the server's AVMCU to SD video resolutions. This helps to conserve MCU resources. • **Video Optimized** - The cascade link between the RealPresence Collaboration Server and the Skype for Business server's AVMCU is capable of HD video resolutions, increasing MCU resource usage.

Gathering Settings - Not Available When CP and SVC or SVC Only Conferencing Modes Are Selected

Field	Description
Enable Gathering	Available only in **CP (Continuous Presence)** conferencing mode. Enabling this causes the MCU to implement a Gathering Phase. This is the time at the beginning of a conference when participants are connecting to the conference. During the Gathering Phase, all endpoints receive a slide containing a mix of live video from with both static and variable textual information about the conference.
Displayed Language	Language for the Gathering Phase page.
Dial-in Number 1	Applies to Appliance Editions only. Optional access numbers to display on the gathering phase slide.
Dial-in Number 2	Applies to Appliance Editions only. Optional access numbers to display on the gathering phase slide.
Info 1	Optional free-form text fields to display on the gathering phase slide. On a 16:9 endpoint, it can display a maximum of 96 characters for each field, and fewer on a 4:3 endpoint.
Info 2	Optional free-form text fields to display on the gathering phase slide. On a 16:9 endpoint, it can display a maximum of 96 characters for each field, and fewer on a 4:3 endpoint.

Field	Description
Info 3	Optional free-form text fields to display on the gathering phase slide. On a 16:9 endpoint, it can display a maximum of 96 characters for each field, and fewer on a 4:3 endpoint.

Video Quality Parameters

Field	Description
People Video Definition	
Video Quality	Available only in **CP (Continuous Presence)** conferencing mode. Specifies two video optimizations: • **Motion** - higher frame rate without increased resolution • **Sharpness** - higher video resolution that requires more system resources **Note:** Selecting **Sharpness**, causes the MCU to send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30 fps.
Maximum Resolution	Available only in **CP (Continuous Presence)** conferencing mode. Overrides the **Maximum Resolution** setting of the **Resolution Configuration** dialog box. Select one of the following options: • **Auto** - It retains the selection of **Maximum Resolution** in the **Resolution Configuration** dialog box. • **CIF** • **SD** • **HD720** • **HD1080**
Polycom Video Clarity	Applies to Appliance Editions only. Available only in **CP (Continuous Presence)** conferencing mode. Not available in **Video Switching** conference mode. This parameter applies a video enhancement algorithm. This algorithm sends clearer images with sharper edges and higher contrast to endpoints at the highest possible resolution that each endpoint supports. It supports all layouts, including 1x1.
Auto Brightness	Applies to Appliance Editions only. Enabling this causes the color changes in computer-based VGA content sent by HDX endpoints through the People video channel.
Content Video Definition	

Field	Description
Content Settings	Specifies the transmission mode for the content channel based on the type of content most often shared. • **Graphics** - Basic mode, intended for normal graphics. • **Hi-res Graphics** - A higher bit rate intended for high-resolution graphic display. • **Live Video** - Content channel displays live video. • **Customized Content Rate** - Manual definition of the Conference Content Rate, mainly for cascading conferences. If you choose a custom content rate, specify the line rate reserved for the content.
AS SIP Content	Available only in **CP (Continuous Presence)** conferencing mode. Enables content sharing using AS-SIP security and the **Multiple Content Resolutions** option. Any other content sharing mode doesn't support this.
Multiple Content Resolutions	Available only in **CP (Continuous Presence)** conferencing mode. Enables content sharing in multiple streams, one for each video protocol: H.263 and H.264. This allows endpoints with different protocols to connect and disconnect without having to restart content sharing. When enabled, choose which content protocols and resolutions to use for each stream of content. • **Content Protocol** ◦ **Transcode to H.264** is always selected ◦ **Use H.263** ◦ **Use H.264 if available, otherwise use H.263** ◦ **Use H.264 cascade and SVC optimized** ◦ **Use H.264 HD** • **Content Resolution** - Specify the fixed resolution and frame rate of the content channel for content sharing in cascaded conferences. Available only when **Content Protocol** is **H.264 cascade and SVC optimized**. The content resolutions available for selection depend on the content sharing mode, line rate, and content settings of the conference.
Send Content to Legacy Endpoints	Available only in **CP (Continuous Presence)** conferencing mode. Enabling this you can send content over the video (people) channel to H.323/SIP/ISDN-video endpoints that don't support H.239 content. Select this option when Avaya IP Softphone is connecting to the conference.
H.264 High Profile	Applies to Appliance Editions only. This displays only when conferencing mode is VSW (Video Switching), or the Content Protocol is **H.264 Cascade Optimized**. In scenarios where the conference contains endpoints not supporting high profile (such as HDX), it's recommended to clear this check-box to enable them to share content.

Field	Description
Enable MS RDP Content	Enabling this causes the MCU to start conferences on Modular MCUs (MMCU) that have sufficient soft blade resources. You can configure the MMCUs with an RDP translator that converts H.264 content to RDP content to deliver to a Skype ASMCU. Likewise, when a Skype client shares RDP content, the RDP translator delivers H.264 content to the MMCU. **Note:** • For Polycom RealConnect calls to work, set **AllowMultiView** to **TRUE** on the Skype for Business Front-End Server. This enables the participants to connect and receive multiple video streams. • You can use this option in place of a separate Polycom® ContentConnect™ gateway solution.

Video Settings Parameters

Field/Option	Description
Presentation Mode	Available only in **CP (Continuous Presence)** conferencing mode. Enabling this causes the conference to change to lecture mode when the current speaker speaks for 30 seconds. When another participant starts talking, it returns to the previous video layout.
Same Layout	Available only in **CP and SVC** conferencing mode. Not available in **Presentation Mode** or **Video Switching** mode, or if **Telepresence Mode** is **Yes**. Forces the layout to all participants. It disables the personal selection of the video layout.
Lecturer View Switching	Available only in **CP (Continuous Presence)** conferencing mode. Not available in **Same layout** mode or **Telepresence Mode** is **Yes**. When in lecture mode, enables the lecturer's view to automatically switch among participants while the lecturer is talking.
Telepresence Mode	Available only in **CP (Continuous Presence)** conferencing mode. Supports telepresence conference rooms joining the conference: • **Auto** - The conference automatically converts to telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins. Recommended setting. • **On** - Telepresence mode is on, regardless of whether a telepresence endpoint is present. • **Off** - Telepresence mode is off, regardless of whether a telepresence endpoint is present.

Field/Option	Description
Telepresence Layout Mode	Available only in **CP (Continuous Presence)** conferencing mode. Not available if **Telepresence Mode** is **No**. Specifies the layout for telepresence conferences: • **Manual** - Conference operator manually controls the layout using the Multipoint Layout Application (MLA) interface. • **Continuous Presence (MLA)** - Tells the MLA to generate a multipoint view (standard or custom). • **Room Switch** - Tells the MLA to use Voice Activated Room Switching (VARS). The others can only see the speaker's site. **Speaker Priority** - Ensures that the current speaker is always displayed in the video layout. It also displays the previous speakers if there's room in the layout. Each endpoint reserves screen space to display the active speaker.
Auto Scan Interval(s)	Available only in **CP (Continuous Presence)** conferencing mode. Specifies the time interval (between 5 - 300 seconds) that **Auto Scan** uses to cycle the display of participants not in the layout in the selected cell. Use **Auto Scan** along with **Customized Polling** so that you can set the cyclic display to a predefined order for a predefined time period.
Auto Layout	Available only in **CP (Continuous Presence)** conferencing mode. This parameter selects the conference layout based on the number of participants currently in the conference. When a new video participant connects or disconnects, the conference layout changes to reflect the new number of video participants.

Audio Settings Parameters

Field/Option	Description
Audio Clarity	Available only for Appliance Editions. When enabled, improves the voice quality in conference of a PSTN endpoint.
Mute participant except lecturer	When enabled, the MCU automatically mutes all participants except the lecturer upon connection to the conference.
Speaker Change Threshold	Specifies the amount of time a participant must speak continuously before becoming the speaker.
Auto mute noisy endpoints	Also known as NoiseBlock™. When enabled, the MCU automatically detects and mutes AVC endpoints that have a noisy audio channel.

IVR Parameters

Field/Option	Description
Conference IVR Service	Lists the conference IVR services available on the MCU.

Field/Option	Description
Conference Requires Chairperson	Enabling this causes the conferences to start only after the chairperson joins. It places all the callers who arrive early on hold. If you enable Terminate conference after chairperson leaves, the conference ends when the last chairperson leaves. If there's no input for chairperson passcode, the system ignores this option. For enterprise users, chairperson passcodes/passwords can come from the Active Directory, but you can override the Active Directory value. For local users, you can add or change chairperson passcodes/passwords when you create or edit them. **Note:** Enabling this parameter for a Polycom RealConnect conference, causes the Skype for Business presenter to act as the chairperson for the conference.

Recording Parameters - Not Available When SVC Only Conferencing Mode Is Selected

Parameter	Description
Enable Recording	Enables recording of conferences.
Dial Out Recording Link	Conference recording requires a recording system such as a Polycom RealPresence Media Suite or Polycom Capture Server. Select the recording link for the device you want to use for conference recording.
Start Recording	Select when to start the recording: • **Immediately** - Conference recording starts as soon as the first participant joins. • **Upon Request** - The operator or chairperson must initiate the recording (manual).
Audio Only	When enabled, limits recording to the audio channel of the conference.
Display Recording Icon	Enabling this parameter causes the MCU to display a recording indicator (a red dot) to all participants as it starts conference recording. It displays a recording icon in the video layout of Skype for Business users when another Skype for Business user starts recording the meeting.
Play recording message	When enabled, the MCU plays a recording message into the conference when recording starts and ends.

Site Names Parameters - Not Available When SVC Only Conferencing Mode Is Selected

Field	Description
Display Mode	Specifies the settings to display the endpoint name on each video participant's section. • **Auto** - Whenever the video layout changes, display the name for 10 seconds in the font size, background color, and screen position specified. • **On** - For the duration of the conference, display the name in the font size, background color, and screen position specified. • **Off** - Don't display the site names and all other fields in this tab are inactive.

Message Overlay Parameters - Not Available When SVC Only Conferencing Mode Is Selected

Field	Description
Enable	When enabled, specifies a message to display on selected conference participant's video display.
Content	Enter the message text (up to 50 characters) to display and specify the properties for the text display. You can also specify the speed at which the text should move (static, slow, or fast) and how often it should repeat.

Network Services Parameters

Parameter	Description
SIP Registration	When enabled, registers the conference with the SIP server of the selected network service.
Accept Calls	When enabled, allows dial in participants to connect to a conference via a network service.

Layout Indications Parameters - Not Available When SVC Only Conferencing Mode Is Selected

Field	Description
Position	Use the drop-down menu to set the display position of the indication icons group.
Recording	Available in **Enable Recording** mode on the **Recording** tab. When enabled, the MCU displays a recording indicator (a red dot) to all participants to inform them that of the recording of the conference. It displays a recording icon in the video layout of Skype for Business users when another Skype for Business user starts recording the meeting.
Audio Participants	When enabled, displays the count of audio participants on each video participant's display. You can display the count constantly or when participants join and leave the conference.
Video Participants	When enabled, displays the count of video participants on each video participant's display.
Network Quality	When enabled, it displays the network quality reading on each video participant's display.

Field	Description
Custom Logo	When enabled, displays an uploaded custom logo to your conferences.

Related Links

View the Properties of an Active Conference on page 176
Add a Conference Profile on page 137
Edit a Conference Profile on page 147
Enable Recording in the Conference Profile on page 153
Schedule a Conference on page 169
System Flags on page 264
Start an Ad Hoc Conference on page 172
Create a Conference Profile for Operator Conferences on page 199
Overlay a Custom Logo on Conference Displays on page 155

Edit a Conference Profile

You can edit an existing conference profile but you can't rename it.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** list, double-click the profile to edit.
3. Edit one or more required profile parameters and click **OK**.

Related Links

Conference Profile Parameters on page 138

Delete a Conference Profile

You can delete profiles from the MCU.

However, you can't delete a conference profile if it's currently used by meeting rooms, reservations, entry queues, or SIP factories. A profile that is assigned to only one ongoing conference and no other conferencing entity can be deleted.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** list, select the conference profile to delete.
3. Click **Delete Profile** ( ) and click **OK**.

Export a Conference Profile

If your environment includes multiple MCUs, you'll likely want all of the same conference profiles available on all MCUs, so conferences can successfully cascade over multiple MCUs.

The RealPresence Collaboration Server allows you to export conference profiles from one MCU as a single XML file and import them to other MCUs.

Note: Only RealPresence Collaboration Server administrators can export and import conference profiles. Operators can only export conference profiles.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** section:
   - To export all conference profiles, click **Export Conference Profiles**  .
   - To export just selected conference profiles:
     1. In the **Conference Profiles** list, select the required conference profiles.
     2. Right-click and select **Export Selected Conference Profiles**.
3. **Browse** to the location to which to save the exported file.
4. In the **Profiles file name** field, enter the file name prefix and click **OK**.

   The file is saved to the location specified with the name specified. The file will have the **_confProfiles.xml** suffix predefined and required by the MCU.

Import a Conference Profile

If your environment includes two or more MCUs, you most likely want all of the same profiles available on all MCUs so conferences can successfully cascade over multiple MCUs.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** section, click **Import Conference Profiles** .
3. **Browse** to the location of previously exported _confProfiles.xml file.
4. Select the file, and click **OK**.

   Note that a conference profile isn’t imported when:
   - A conference profile with that name already exists
   - The conference profile requires an IVR service that isn’t present on the MCU.

Conference Templates

Administrators and operators can create, save, schedule, and activate identical conferences using conference templates.

A conference template does the following:

- Saves the conference profile
- Saves all participant parameters including the Personal Layout and Video Forcing settings
- Simplifies telepresence conference setup where precise participant layout and video forcing settings are crucial

The MCU initially displays the conference templates list as a closed tab in the RMX Manager main screen. The tab indicates the number of saved conference templates.

Note that you can't edit conference templates.

Related Links

Start an Operator Conference from a Template on page 204
Save an Operator Conference to a Template on page 204

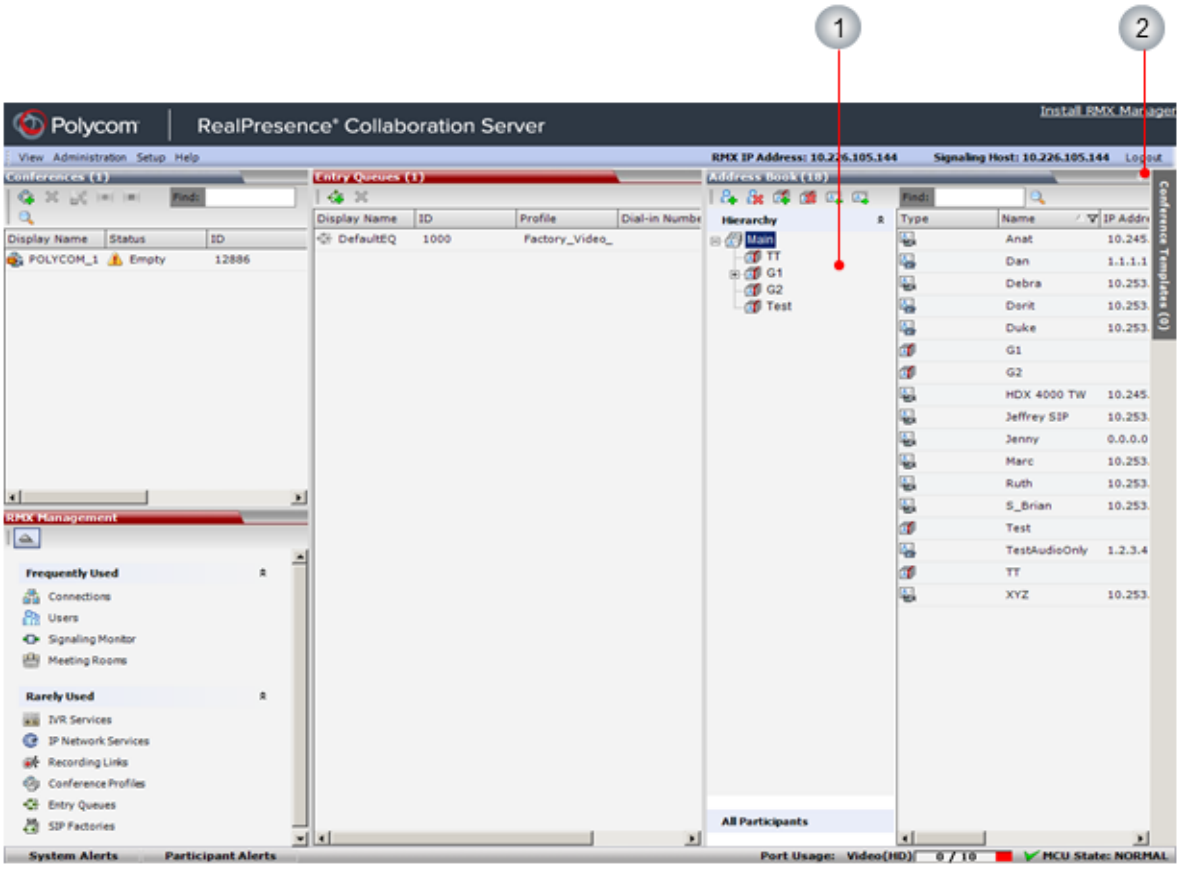
View the List of Conference Templates

A RealPresence Collaboration Server doesn't have default conference templates because they require information that isn't standard.

Procedure

1. Open the RMX Manager.

   The list of conference templates displays in the main **RMX Manager** pane.
2. If the list is hidden, double-click the **Conference Template** tab on the right.



Add a Conference Template

Create conference templates to start and replicate successful conferences.

Conference templates do the following:

- Identify the desired conference profile (and thus, parameters) for a conference
- Identify that participants and participant parameters (including their personal layout and video forcing settings) for a conference

- Simplify the setup of telepresence conferences, where precise participant layout and video forcing settings are crucial.

Procedure

1. In RMX Manager, click **Conference Templates**.
2. Click **New Conference Template** ().
3. In the **General** tab:
   a. In the **Display Name** field, enter the new template name.
   b. Specify the duration of the conference in hours and minutes and enable **Permanent Conference** to create a standard recurring conference.
   c. Assign a **Routing Name** and **ID** or allow the system to assign them automatically.
   d. Select the required **Profile**.
   e. As required, assign a **Conference Password** that users must enter to join the conference or a **Chairperson Password** that the chairperson must enter to take on the chairperson responsibilities.
4. Go to the **Participants** section and do one of the following:
   - Click **Add from Address Book**, select the required groups and participants, and click **Add.**
   - Click **New**, enter the required information for the new participant, and click **Add**.
5. To assign a lecturer for Lecture Mode conferences, select a **Lecturer** from the participant's list, and if required, enable **Dial Out Manually** so the MCU can initiate the dial out. (AVC dial-outs only.)

   Note: Dial-out and dial-in participants are two separate participants even if they have the same IP address/number; therefore, if a dial-out participant is added to the conference, but that participant dials in before the MCU dials out to him, the MCU creates a second participant in the Participants list and still attempts to dial out to the participant. If the dial-out participant was designated as the conference lecturer, the MCU can't replace that participant with the dial-in participant that is connected to the conference.

   ---

6. To override the layout identified in the selected conference profile, click **Media Sources** and enable **Override layout from profile**.

   For information on how to change the conference layout, see <reference here>.
7. To add optional conference information, click **Information** and enter the required text into the **Info1**, **Info2**, **Info3**, or **Billing Info** text boxes.
8. Click **OK** to create the new conference template.

Delete a Conference Template

You can delete one or several conference templates at a time.

Procedure

1. In RMX Manager, click **Conference Templates**.
2. In the **Conference Templates** list, select one or more templates to delete.
3. Right-click and select **Delete Conference Template**.
4. Click **OK**.

Export a Conference Template

You can export conference templates from one MCU as a single XML file and import them to other MCUs in your environment.

When you export conference templates, you should also export the profiles associated with the templates to ensure that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

Note: Only RealPresence Collaboration Server administrators can export and import conference templates. Operators are only allowed to export conference profiles.

Procedure

1. In RMX Manager, click **Conference Templates**.
2. In the **Conference Templates** pane:
   - To export all conference profiles, click **Export Conference Templates**  .
   - To export just selected conference templates,
     1. In the **Conference Templates** list, select one or more required conference templates.
     2. Right-click and select **Export Selected Conference Templates**.
3. **Browse** to the location to which to save one or more exported files.
4. In the **Templates file name** field, enter the file name prefix for the exported templates.
5. To export the conference profile as part of this export, enable **Export includes Conference Profiles** and in the **Profiles file name** field, type the file name prefix for the exported profiles.
6. Click **OK**.

   The conference templates are saved to the specified location with the specified name and a **_confTemplates.xml** suffix predefined as required by the MCU.

   The conference profiles are saved to the specified location with the specified name and a **_confProfiles.xml** suffix predefined as required by the MCU.

Import a Conference Template

You can import conference templates (and associated conference profiles) from one to multiple MCUs in your environment.

Procedure

1. In RMX Manager, click **Conference Templates**.
2. In the **Conference Templates** pane, select **Import Conference Templates**.
3. If required, enable **Import includes conference profiles** to include the conference profile as part of the import.
4. **Browse** to the location of the previously exported **_confTemplate.xml** and **_confProfiles.xml** files.
5. Select one or more files to import and click **OK**.

   The imported conference templates and profile are added to their respective lists.

Save an Ongoing Conference as a Template

You can save any ongoing conference as a template.

Consider the following when saving an ongoing conference as a template:

- If the profile assigned to a conference is deleted while the conference is ongoing the conference cannot be saved as a template.
- Only defined participants can be saved to the conference template. Before saving a conference to a template ensure that all undefined participants have disconnected. Undefined participants aren't saved in conference templates.
- Conference templates saved from an ongoing conference don't include Message Overlay text messages.

Procedure

1. In the RMX Manager **Conferences List**, select the conference to be saved as a template.
2. Right-click and select **Save Conference to Template**.

   The MCU saves the template with a name derived from the ongoing conference display name. Operator conference templates are displayed with the operator conference icon.

Advanced Conferencing Profile Features

Topics:

This section describes specific conferencing features you may wish to enable or disable.

You usually enable or disable features via the conferencing profile. Occasionally, you may need to enable or disable features using system flags.

Note: If you have a Poly Clariti Core system, create conference templates and manage conferencing parameters on the Poly Clariti Core system and not on the MCU.

The Poly Clariti Core system has more flexibility, as it can associate conferencing experiences with users, conference rooms, or enterprise groups. It also offers more features and functions including MCU cascading and integration with Polycom RealConnect.

Enable Recording in the Conference Profile

Enable conference recording on the RealPresence Collaboration Server as part of the conference profile by first configuring the dial-out recording link.

The recording link defines the connection between the MCU and the recording system. Then you must modify the configuration profile recording settings

The default Conference IVR Service associated with the RealPresence Collaboration Server includes the recording-related voice messages and default DTMF codes. This allows the conference chairperson to control the recording process from the endpoint. However, you can associate change these default settings if desired.

Procedure

1. In RMX Manager, go to **RMX Management** > **Recording Links** .
2. In the **Recording Links** list, click **New Recording Link** .
3. Enter a unique and recognizable **Name** for the recording system and link and select the network environment: **H.323** or **SIP**.
4. Enter the **IP Address** and/or the Alias Name of the recording system.

- If no gatekeeper is configured, you must enter the recording system's IP Address. If you're using the HARMAN RealPresence Media Suite, enter its IP address. Then enter the virtual recording room (VRR) number in the **Alias Name** field.
- If a gatekeeper is configured, you can enter the recording system's IP Address or its alias.
- If a SIP server is configured, enter its IP address instead of the IP address of recording system.

5. If using **Alias Name**, select the **Alias Type** for the recording system.
   - If you're associating this recording link to a VRR on the HARMAN RealPresence Media Suite, if the Alias Type is set to H.323 ID, enter the RealPresence Media Suite IP address and the VRR number in the format: `<Media Suite IP Address>##<VRR number>`

     For example: If the RealPresence Media Suite IP is 173.26.120.2 and the VRR number is 5555, enter `173.26.120.2##5555`. Define the following recording link parameters on the default IP network service to enable recording.
   - Depending on the format used to enter the information in the IP address and Alias fields, select H.323 ID or E.164 (for multiple Recording links). Email ID and Participant Number are also available.
6. Click **OK**.

   The recording link is added to the RealPresence Collaboration Server unit.
7. In RMX Manager, go to **RMX Management** > **Conference Profiles**  .
8. From the **Conference Profile** list, select the profile to enable for recording.
9. Right click and select **Profile Properties**.
10. In the **New Profile Properties** section, go to **Recording** and click **Enable Recording**.
11. Enter the required recording parameters.
12. Click **OK**.

Related Links

Conference Profile Parameters on page 138

Change Position of the Conference Indicators

During a conference, when enabled, participants see a variety of indicators that provide information about the conference.

If required, you can change the position of these indicators in the conference layout.

Conference indicators include:

- Audio and video participant indicators

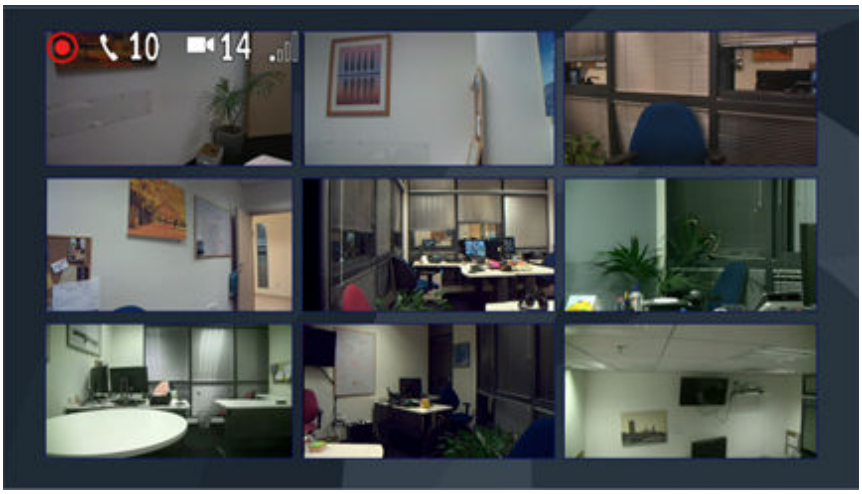
  During an ongoing conference, participants see the number of audio-only and video participants who are connected to the conference. The system displays a maximum of 99 participants of each type. The icon group is displayed for AVC endpoints only.
- Recording indicator

  When Display Recording Icon is selected in either the Recording or Layout Indications tab of the Conference Properties dialog, the recording status is indicated by the standard recording icon.
- Network quality indicator

  Network quality is determined by the percentage of packet loss according to the following default threshold values:
  - Packet loss less than **1%** is considered Normal

- Packet loss in the range of **1% - 5%** is considered Major
- Packet loss above **5%** is considered Critical

Conference indicators, shown below, are displayed on AVC endpoints only for CP or mixed conferences.



Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** pane, double click on the profile to edit.
3. Select the **Layout Indications** tab.
4. From the **Position** drop-down menu, select a new position for the indicators. Options are **Left Top**, **Top**, **Right Top**, **Left Bottom**, **Bottom**, or **Right Bottom**.
5. Click **OK**.

Related Links

Polycom RealPresence Collaboration Server Features and Capabilities on page 13

Indicators for Microsoft Skype for Business Users

Microsoft Skype for Business and Lync users see the same conference indicators as other Polycom RealConnect conference participants, provided the video stream sent to their endpoint is compatible.

However, the indications aren't embedded in the video sent to the link, so as to preserve the Skype for Business or Lync user experience.

Overlay a Custom Logo on Conference Displays

You can add a custom logo to the conferencing display for your organization's video conferences.

The custom logo must meet the following specifications:

- File type must be .jpg, .jpeg, or .bmp.
- File size must be no more than 1 megabyte.
- Image resolution must be no more than 256 pixels × 256 pixels.
- Image area (width * height) must not be smaller than 64 pixels × 64 pixels.

Note the following:

- This feature isn’t supported on RealPresence Collaboration Server 1800 with no DSP card.
- You can only display a custom logo on AVC endpoints in CP or mixed CP/SVC conferences (similar to the layout indication icons).
- If you enable the custom logo in a conference profile, then the logo displays throughout the entire duration of a conference.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. Choose the conference profile you want to edit.
3. On the **Layout Indications** tab, select the **Custom Logo** check box and choose the **Logo Position** from the drop-down menu.

   The logo position options are identical to those supported for the Layout Indication icons.
4. Click **OK**.
5. In RMX Manager, go to **Setup** > **Custom Logo**.
6. Select the logo image file to upload and click **OK**.

   The RealPresence Collaboration Server validates the logo and prompts you to reboot. You must reboot the server before it starts using the uploaded logo.

Related Links

Conference Profile Parameters on page 138

Enable Multiple Content Resolutions (Transcoding) on TIP Endpoints

The RealPresence Collaboration Server supports content transcoding for TIP endpoints in Prefer TIP virtual meeting room (VMR) conferences.

TIP endpoints in Prefer TIP VMR conferences support the following content resolutions and frame rates:

- XGA 5fps @512K (default)
- 720p5 @768K
- 1080p5 @1Mbps
- 720p30 @2.25Mbps
- 1080p30@4Mbps (Not supported on RealPresence Collaboration Server, Virtual Edition)

TIP endpoints work at one of the above resolutions only. Any TIP endpoint not supporting the selected rate and resolution is unable to receive the content. TIP endpoints supporting Version 7 don't receive any content in content transcoding mode if the selected resolution is other than XGA 5fps @512K.

To set the multiple content resolution for TIP endpoints, you must set the **TIP Compatibility** option to **Prefer TIP** in the Conference Profile under **Profile Properties** > **Advanced** tab.

Note: In a **TIP Compatibility** > **Prefer TIP** conference, if a TIP endpoint doesn't have the required capabilities to meet the content threshold based on the conference line rate, the RealPresence Collaboration Server considers that TIP endpoint as legacy and sends content to it over the video channel.

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** pane, double click on the profile to edit.
3. Go to **Video Quality** and in the **Content Video Definition** section enable **Multiple Content Resolutions**.
4. Select the appropriate content resolution and frame rate from the drop-down menu for the **TIP Encoder**.
5. Click **OK**.

Hide Participant Count in TIP-Enabled Conferences

If you set the **TIP Compatibility** mode to **Prefer TIP**, RealPresence Collaboration Server displays the audio and video participant count on each video participant's display by default. However, you can disable this feature.

Procedure

» Set the system flag `DISABLE_TIP_ICONS_INDICATIONS` to `YES`.

Enable Exclusive SVC Mode

You can configure the MCU to host SVC Meeting Room (MR) conferences only.

Because the connection is set up directly between the MCU and the endpoint(s) in Exclusive SVC Mode, Poly Clariti Core systems don't support these calls. Therefore, you must disable RealPresence Clariti licensing on the RealPresence Collaboration Server before enabling Exclusive SVC Mode.

For more information, see the *Polycom RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Getting Started Guide* and the *Poly Clariti Manager System Operations Guide*.

In Exclusive SVC Mode, the MCU rejects AVC and mixed-mode conferences, as well as any Virtual Meeting Room (VMR) conferences made on a Poly Clariti Core system. In this mode, the RealPresence Collaboration Server can accept dial-in SVC calls and make dial-out SVC calls.

Procedure

» In RMX Manager, add the following system flag(s):

`ENABLE_SVC_ONLY`

Enables or disables the option for the MCU to host SVC Meeting Room (MR) conferences only.

NO - Disables the feature.

YES - Enables the feature.

Loopback Video in Telepresence Conferences

If you set set the **Telepresence Layout Mode** option as **Speaker Priority** or **CP-Auto**, when there is only one endpoint present in a conference, RealPresence Collaboration Server displays the participant's loopback video in telepresence conferences by default.

However, for multiscreen endpoints, the loopback video displays for the center screen only.

NoiseBlock

The RealPresence Collaboration Server uses NoiseBlock, a heuristic algorithm, to monitor and lessen the audio of AVC endpoints with high levels of nonspeech background noise.

This helps prevent those endpoints from becoming the active speaker by mistake, which could detract from the overall video conferencing experience.

The NoiseBlock feature is supported for AVC endpoints only in Continuous Presence (CP) and in Mixed CP and SVC conferences. In mixed CP and SVC conferences, the RealPresence Collaboration Server blocks audio towards AVC-based endpoints only. It doesn't affect SVC-based endpoints.

If the noisy endpoint is SVC-based, its audio channel isn't sent to the AVC-based endpoints, but it's sent to the other SVC-based endpoints.

Note that NoiseBlock doesn't guarantee exact identification of nonspeech originated sounds and when the endpoints are automatically muted by the MCU, no indication is displayed in RMX Manager or at the endpoint.

- When upgrading from a version before 8.1, the **Auto mute noisy endpoints** option isn't automatically selected.

  In Profiles created after the upgrade, the **Auto mute noisy endpoints option** is automatically selected.
- You need to manually add the **ENABLE_SELECTIVE_MIXING** system flag, and enable/disable the function by changing the value to **YES**/**NO**. MCU reset isn't required when changing the system flag value.
- If your conferencing environment includes Poly Clariti Core, the conferences started from the Poly Clariti Core system don't include the NoiseBlock parameter as it isn't part of the Poly Clariti Core profiles. In such a case, when the parameter setting is unknown, the system enables/disables the NoiseBlock according to the system flag setting - if the flag is set to **YES**, it's enabled in the conference.

Disable NoiseBlock

The NoiseBlock feature is enabled by default.

The NoiseBlock feature is based on the interaction of two following configuration elements:

- The **ENABLE_SELECTIVE_MIXING** flag value and
- The **Auto mute noisy endpoints** setting

Procedure

1. In RMX Manager, go to **RMX Management** > **Rarely Used** > **Conference Profiles**.
2. In the **Conference Profiles** pane, select the conference profile.
3. Deselect the **Auto mute noisy endpoints** checkbox.
4. Click **OK**.
5. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
6. In the **MCMS_PARAMETERS_USER** tab, select the **ENABLE_SELECTIVE_MIXING** system flag and set its value to **NO**.
7. Click **OK**.

Configuring the Address Book

Topics:

You can use the RealPresence Collaboration Server (RMX) address book to store information about conference participants to quickly and efficiently include participants in conferences.

If you have a Poly Clariti Manager system, Poly recommends that you integrate your RealPresence Collaboration Server with it and manage users and conference participants in the Poly Clariti Manager system instead of using the RealPresence Collaboration Server address book.

Note: When you use the Poly Clariti Manager system to manage your participant information:

- Integration with the Poly Clariti Manager global address book is not supported by RealPresence Collaboration Server (RMX) 1800 with no DSP cards.
- To fetch the address book from a Poly Clariti Manager system over a secure connection, you must use RMX Manager.

Related Links

Integrate with the Poly Clariti Manager System on page 30
Start an Operator Conference on page 200

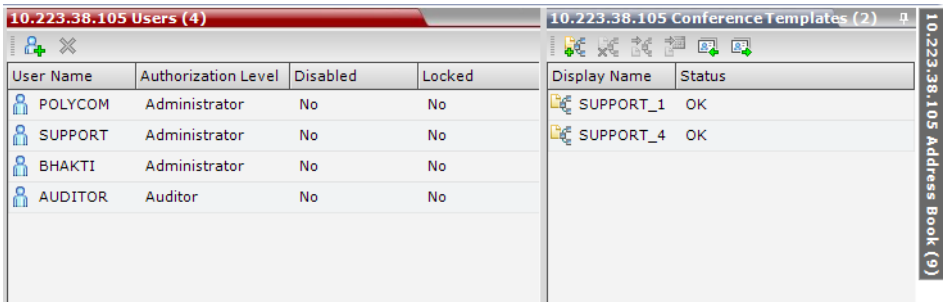
View the Address Book

You can view the RealPresence Collaboration Server address book using RMX Manager.

Procedure

1. Open the RMX Manager.

   The address book displays in the main **RMX Manager** pane.
2. If the list is hidden, double-click the **Address Book** tab on the right.



Add a Participant to the Address Book

This sections lists the steps to add a Participant to the Address Book.

You can add participants directly to the address book or by moving or saving a participant from an ongoing conference to the address book.

Procedure

1. In RMX Manager, click **Address Book**.
2. Right-click the group to which to add the participant and select **New Participant**.
3. Select and edit the properties you wish to define.
4. To add general information about the participant, such as email address or company name, click **Information** and enter the necessary details in the **Info 1-4** fields.
5. Click **OK**.

Related Links

Participant Properties on page 160

Participant Properties

The following tables list the participant properties that you can enable on the RealPresence Collaboration Server.

General Participant Properties

Field	Description
Name	Unique name that identifies the participant or the participant's endpoint within RMX Manager. If configured, this name may display in the video layout. The maximum field length for the display name is approximately: • 80 ASCII characters • 40 European or Latin text characters • 25 Asian text characters **Note:** Don’t use commas or semicolons in this field.

Field	Description
Endpoint Website	Hyperlink that connects to the internal website of the participant's endpoint, which enables you to perform administrative, configuration and troubleshooting activities if required. The connection is available only if the IP address of the endpoint's internal website is defined in the **Website IP Address** field.
Dialing Direction	Select the dialing direction: • **Dial-in** - The participant dials in to the conference. This field applies to IP participants only. • **Dial-out** - The MCU dials out to the participant.
Type	The network communication protocol used by the participant’s endpoint to connect to the conference: H.323 or SIP. The fields in the dialog box change according to the selected network type.
IP Address (H.323 and SIP)	IP address of the participant's endpoint. • For H.323 participants, enter either the endpoint IP address or the endpoint alias. • For SIP participants, enter either the endpoint IP address or the endpoint SIP address. For RealPresence Collaboration Servers registered to a gatekeeper, you can configure the MCU to dial and receive calls to and from H.323 endpoints using the IP address in the event that the gatekeeper isn’t functioning.
Alias Name/Type (H.323 Only)	The type of alias for the endpoint (based on communication protocol). Although all types are supported, the type of alias is dependent on the gatekeeper’s capabilities. The most commonly supported alias types are H.323 ID and E.164. • H.323 ID (alphanumeric ID) • E.164 (digits 0–9, * and #) • Email ID (email address format such as `abc@example.com`) • Participant number (digits 0–9, * and #) Use this field to enter the entry queue ID, target conference ID, and conference password when defining a cascaded link. To use the E.164 number, you must set the `REMOVE_IP_IF_NUMBER_EXISTS` system flag.

Field	Description
SIP Address/Type (SIP Only)	Select the format of the SIP address and then enter the endpoint's SIP address: • **SIP URI**: Uses an email address format, typically containing a user name and a host name, for example, `sip:dan@polycom.com`. **Note:** If the **SIP Address** field contains an IPv6 address, you must surround it by square brackets, for example, `[::1]`. • **TEL URI**: Used when the endpoint doesn't specify the domain that should interpret a telephone number that a user has input. Instead, each domain through which the request passes gets that opportunity. For example, if a user in an airport logs in and sends requests through an outbound proxy in the airport (the user enters `411`, the phone number for local directory assistance in the United States), then this number must be interpreted and processed by the outbound proxy in the airport and not by the user's home domain. In this case, telephone number 411 is the correct choice.
Endpoint Website IP Address (IP only)	IP address of the endpoint's internal site to enable connection to it for management and configuration purposes. This field is automatically completed the first time that the endpoint connects to the RealPresence Collaboration Server. If the field is blank, you can manually configure it or even modify it while the endpoint is connected.
Audio Only	Select this check box to define the participant as a voice participant with no video capabilities.
Extension/Identifier String	Dial-out participants that connect to an external device such as cascaded links or recording links may be required to enter a conference password or an identifying string to connect. (AVC dial-outs only.) Enter the required string as follows: `[p]...[p][string]`, for example: `pp4566#` • `p` (optional): Indicates a pause of one second before sending the DTMF string. Enter several concatenated [p]s to increase the delay before sending the string. The required delay depends on the configuration of the external device or conference IVR system. • `string`: The required string using the digits 0–9 and the characters * and #. The maximum number of characters that you can enter is identical to the H.323 alias length. If the information required to access the device or conference is composed of several strings (such as the conference ID and conference password), you can enter all the information as one string and add pauses between the strings for required delays. Enter the multiple information string as follows: • `[p]...[p][string][p]...[p] [string]...` • For example: `p23pp*34p4566#` The RealPresence Collaboration Server automatically sends this information upon connection to the destination device or conference. The information is sent by the RealPresence Collaboration Server as DTMF codes to the destination device or conference, simulating the standard IVR procedure.

Advanced Participant Properties

Field	Description
Video Bit Rate / Auto (IP Only)	The **Auto** check box is automatically selected to use the line rate defined for the conference. **Note:** You can't clear this check box when defining a new participant during an ongoing conference. To specify the video rate for the endpoint, clear this check box, and then select the required video rate.
Video Protocol	The video compression standard that the MCU uses on the endpoint when connecting to the conference: H.261, H.263, H.264, or RTV. Select **Auto** to let the MCU select the video protocol according to the endpoint's capabilities.
Resolution	The **Auto** check box is automatically selected to use the resolution defined for the conference. To specify the resolution for the participant, select the required resolution from the drop-down menu.
Broadcasting Volume + Listening Volume	Adjusts the volume which the participant broadcasts to the conference or the volume the participant hears at the conference, by moving the slider. Each unit represents an increase or decrease of 3 dB. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5.
Encryption	Selects whether the endpoint uses encryption for its connection to the conference. **Auto** (default setting) indicates that the endpoint connects according to the conference encryption setting.
AGC	The Auto Gain Control (AGC) mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. Select this check box to enable the AGC mechanism for participants with weaker audio signals. • To enable AGC, set the value of the `ENABLE_AGC` system flag in `system.cfg` to `YES`. • If the system flag doesn't exist in the system, add it to the system configuration. • Enabling AGC may result in amplification of background noise.
Cascaded (IP Only)	Enables the connection of one conference directly to another conference using an H.323 connection only. The conferences can run on the same MCU or different MCUs. If you use this participant as a link between conferences, select one of the following options:: • **Secondary**: the participant is defined in a conference running on a secondary MCU. • **Primary**: the participant is defined in a conference running on the primary MCU.

Related Links

System Flags on page 264

Basic Cascading on page 223
Edit a Participant in the Address Book on page 164
Add an Existing Participant to a Group Entry on page 165
Add a New Participant Through a Group Entry on page 166
View Information for Active Conference Participants on page 176
Add a Participant or Group to an Active Conference on page 180
Add a Group to the Address Book on page 165
Add a Participant in an Active Conference to the Address Book on page 180
Add a Participant to the Address Book on page 160
Cascade-Enabled Participant Links on page 232
View Participant Alerts on page 462

Edit a Participant in the Address Book

When required, you can edit a participant's address book information or properties.

Procedure

1. In RMX Manager, click **Address Book**.
2. In the **Find** field, enter the name of the participant to edit.
3. Click **Search** and select the participant from the resulting list.
4. Select and edit the properties you wish to define.
5. Click **OK**.

Related Links

Participant Properties on page 160

Delete a Participant from the Address Book

You can delete a participant from the address book.

You can also delete all participants from the address book by performing a Comprehensive Restore.

Procedure

1. In RMX Manager, select **Address Book**.
2. In the **Find** field, enter the name of the participant to delete.
3. Select **Search** and select the participant from the resulting list.
4. Select **Delete Participant** .

   A confirmation message displays depending on the participant’s assignment to groups in the address book.
5. Do one of the following:
   - If the participant belongs to only one group, select **Yes** to permanently delete the participant from the address book.
   - If the participant belongs to multiple groups, select **Current group** to delete the participant from the selected group.

- If the participant belongs to multiple groups, select **Address Book** to permanently delete the participant from all groups in the address book.

6. Select **OK**.

Copying or Moving a Participant in the Address Book

You can copy or move a participant from one group to another group using the **Copy**, **Cut**, and **Paste** options; however, the cut and copy actions aren't available when selecting multiple participants.

A participant can belong to multiple groups; however, there's only entity for a participant. Groups that contain the same participants link to the same participant entity. You can also move a participant from one location in the address book to another by dragging and dropping the participant to its new location.

Add a Group to the Address Book

You can add a group to the address book via the RMX Manager.

Procedure

1. In RMX Manager, click **Address Book** and then click **New Group** .
2. Enter a unique and meaningful name for the group and click **OK**.

Related Links

Participant Properties on page 160

Add an Existing Participant to a Group Entry

You can add an existing participant in the address book to a group entry.

Procedure

1. In RMX Manager, click **Address Book**.
2. Select the participant from the participant list.
3. Right click and select **Copy Participant**.
4. Select the group from the group list.
5. Right click and do one of the following:
   - Select **Paste Participant**.
   - Select **Paste Participant as New** and configure the participant properties.
6. Click **OK**.

Related Links

Participant Properties on page 160

Add a New Participant Through a Group Entry

You can add a new participant to the address book through a group entry.

Procedure

1. In RMX Manager, click **Address Book**.
2. Select the group from the list.
3. Right click and select **New Participant**.
4. Enter the **New Participant** information required.
5. Click **OK**.

Related Links

Participant Properties on page 160

Filter the Address Book

Filter the address book to display only the entries (participants or groups) that meet criteria you specify.

This allows you to select and work with a subset of **address book** entries.

The filter applies to the displayed group. If **All Participants** is selected, it applies to all the listed participants.

Filtering can be done using:

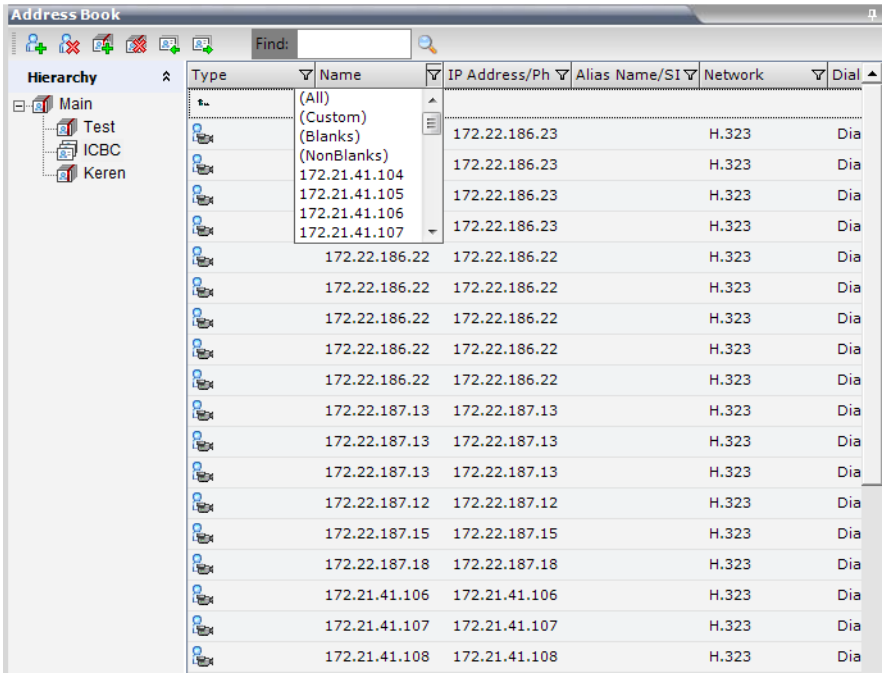
- A predefined pattern
- Customized pattern

When you use the Find dialog box to search filtered data, only the data that is displayed is searched; data that isn't displayed isn't searched. To search all the data, clear all filters.

Procedure

1. In RMX Manager, click **Address Book**.
2. From the **Hierarchy**, select the group to filter.
3. In the **Address Book**, click **Filter** for the column by which to filter.

   The MCU displays a drop-down menu that includes all of the patterns by which the column can be filtered.



4. To filter by a predefined pattern, select the pattern to use for filtering.
5. To filter by a custom pattern:
   a. Select **Custom**
   b. In the **Condition - Column text matches** field, enter the custom filtering pattern. For example, to list only endpoints that include the numerals 41 in their name, enter 41.
   c. Click **Add Condition**.

      The MCU displays the filtered list with a filter indicator next to the column name.
6. To further filter the list, click **Filter** for the additional columns by which to filter.
7. To clear a filter, click **Filter** for the column from which filtering is to be removed and select **All**.

Export an Address Book

If your environment includes multiple MCUs, you might want all MCUs to use the same address book. You can export the address book from MCU into a proprietary XML file and import it into other MCUs.

Procedure

1. In RMX Manager, select **Address Book**.
2. Select **Export Address Book** and browse to a location to save the exported file.
3. In the **File Name** field, enter a name for the exported file.

   If you don't assign a name to the exported address book, the system saves it with the default file name of `EMA.DataObjects.OfflineTemplates.AddressbookContent_.xml`
4. Select **Save**.
5. Select **OK**.

Import an Address Book

This sections describes how to import an address Book and also import a multilevel address book to single-level address book.

When importing a multilevel address book to an MCU that has only a single-level address book, the MCU does the following:

- Creates a new multilevel address book with a different name. By default, the new address book contains at least two levels:
  - The top level (root) named Main.
  - Second level - All address book groups from the single-level address book are placed under the Main group with their associated participants.
- Places all participants that weren't previously associated with a group in the single-level address book in the Main group.
- All participants in the address book appear in the **All Participants** group.
- Saves a copy of the single-level address book to allow you to restore the MCU back to its original single-level address book (if required).

Procedure

1. In RMX Manager, click **Address Book**.
2. Click **Import Address Book** () and **Browse** to the location of the previously exported address book.

   Note: When importing an address book, participants with exact names in the current address book will be overwritten by participants defined in the imported address book.

3. Click **Open** and then click **OK**.

   The MCU displays a confirmation message when the address book is imported.
4. Click **Close**.

Add Participants from the Address Book to a Conference

You can add individual participants or a group of participants from the address book to a conference using a drag-and-drop operation.

Note: Multiple selections of group levels is not available.

Procedure

1. In RMX Manager, click **Address Book**.
2. From the **Hierarchy**, select the group from which to add participants.
3. Select one or more participants to be added to the conference and drag them to the **Participants** list.

Scheduling and Starting Conferences

Topics:

If your environment has a standalone RealPresence Collaboration Server, you can use it to schedule and start conferences.

Note: If your environment includes a Poly Clariti Manager system, which has a Web Scheduler feature, or another scheduling application such as Microsoft Outlook or the Polycom Conferencing Add-in for Microsoft Outlook, Polycom recommends that you create and schedule conferences using one of these standard scheduling applications and not the MCU.

This section on conference management discusses how to schedule and start conferences and the available operations to perform on active conferences.

View Scheduled Conferences

Each RealPresence Collaboration Server maintains its own calendar of scheduled conferences in the Reservation Calendar.

Procedure

» In RMX Manager, go to **RMX Management** > **Rarely Used** > **Reservations**.

Schedule a Conference

You can schedule a conference by making a reservation on the RealPresence Collaboration Server.

The system reserves the required resources using the following criteria:

- The number of participants at the time and duration you specify
- The highest video resolution supported by the line rate specified in the conference profile associated with the reservation
- At or up to the maximum system video resolution specified for the system

Procedure

1. In RMX Manager, go to **RMX Management** > **Reservations**.
2. In the **Reservation List**, select the date and time for the future conference. Drag the cursor across the calendar to extend the duration of the conference.
3. Right-click and select **New Reservation**.
4. Select and edit the conference parameters you wish to define.

General Conference Parameters

Field	Description
Display Name	Unique name that identifies the conference within RMX Manager. If left blank, the MCU automatically generates a display name for the conference, which you can then modify. The maximum field length for the display name is approximately: • 80 ASCII characters • 40 European or Latin text characters • 25 Asian text characters **Note:** Don't use commas or semicolons in this field.
Duration	Identifies the duration of the conference in HH:MM format.
Permanent Conference	Displayed in the **New Conference** dialog only. Enable this option to create this conference as a standard recurring conference.
Routing Name	Unique name the MCU uses to register the conference with network devices such as gatekeepers and SIP servers. Enter a name using ASCII text only. If left blank, the MCU automatically generates a routing name using the following options: • If you use only ASCII characters in the display name, the MCU uses the **Display Name** as the routing name. • If you use a combination of Unicode and ASCII characters or full Unicode text in the display name, the MCU uses the **ID** as the routing name. **Note:** Poly recommends that you allow the MCU to assign this field automatically.
Profile	Choose the predefined conference profile that best identifies the conferencing mode, line rate, media settings, and general settings suitable for your conferencing environment.
ID	Unique ID number for the conference on the MCU. If left blank, the MCU automatically assigns an ID number once you submit the reservation. **Note:** Poly recommends that you allow the MCU to assign this field automatically. Communicate this conference ID to dial-in participants to enable them to dial in to the conference.
Conference Password	Password that participants must enter (if configured) to join the conference. If left blank, participants can join the conference without entering a password. By default, this password is 4 numeric characters. You can configure the MCU to automatically generate a password when you leave this field blank.

Field	Description
Chairperson Password	Password that the chairperson must enter (if configured) to join the conference with chairperson responsibilities. If left blank, chairperson functionality is not enabled for the conference. By default, this password is 4 numeric characters. You can configure the MCU to automatically generate a password when you leave this field blank.
Reserve Resources for Video Participants (Appliance Edition only)	Number of video participants for which the system must reserve resources. Default: 0 participants. Maximum participants: • MPMRx-D / RMX 1800: 100 • MPMRx-S: 30
Reserve Resources for Audio Participants (Appliance Edition only)	Number of audio participants for which the system must reserve resources. Default: 0 participants. Maximum participants: • MPMRx-D / RMX 1800: 300 • MPMRx-S: 90
Maximum Number of Participants	Total number of participants that can join to the conference. Choose **Automatic** to allow resource availability to determine the maximum number of participants that can join the conference. **Note:** If you specify a number, it should be large enough to accommodate the participants specified in the **Reserve Resources for [Video/ Audio] Participants** fields.
Enable ISDN (audio/ video) Dial-in	Allows ISDN-video and ISDN-voice participants to join directly to the conference.
ISDN (audio/video) Network Service	Identifies the predefined network service that best suites your conferencing environment.
Dial-in Number (1)	Unique dial-in number for the conference. Choose this number from the dial-in number range defined for the selected network service. If left blank, the MCU automatically assigns a number from the dial-in range defined for the selected ISDN (audio/video) network service.
Dial-in Number (2)	Second unique dial-in number for the conference. Choose this number from the dial-in number range defined for the selected network service. By default, the second dial-in number is not defined.

5. Click **Participants** and do one of the following:
   - Click **Add from Address Book** to invite participants already in your address book.
   - Click **New** and enter the required information for new participants.

6. Optional: Choose a participant as a lecturer and, if needed, enable **Dial Out Manually** so the MCU can dial out to the lecturer. (AVC dial-outs only.)

Note: Dial-out and dial-in participants are two separate participants even if they have the same IP address or number. If you add a dial-out participant to the conference, but that participant dials in before the MCU dials out to them, the MCU creates a second participant in the **Participants** list and still attempts to dial out to the participant. If you designated the dial-out participant as the conference lecturer, the MCU can't replace that participant with the dial-in participant that is already connected to the conference.

---

7. Optional: To make the conference recurring, click **Schedule** and enter the required scheduling and recurrence information.
8. Optional: To add additional conference information, click **Information** and enter your information in the following fields:
   - **Info1**
   - **Info2**
   - **Info3**
   - **Billing Info**
9. Optional: To override the layout identified in the selected conference profile, click **Media Sources** and select the **Override layout from profile** check box.
10. Click **OK**.

    Unless otherwise specified, the system automatically assigns an ID to the conference when you submit the reservation.
11. Communicate the conference ID to conference dial-in participants.

Related Links

System Flags on page 264
Conference Profile Parameters on page 138

Start an Ad Hoc Conference

You can create and start an ad hoc conference immediately.

Procedure

1. In the **Conferences** section of RMX Manager, click **New Conference** ().
2. Select and edit the conference parameters you wish to define.
3. Click **Participants** and add participants from the **Address Book** or click **New** and enter the required information for new participants.
4. If required, choose a participant as a lecturer and as needed enable **Dial Out Manually**, so the MCU can dial out to the lecturer. (AVC dial-outs only.)

Note: Dial-out and dial-in participants are two separate participants even if they have the same IP address/number; therefore, if a dial-out participant is added to the conference, but that participant dials in before the MCU dials out to him, the MCU creates a second participant in the Participants list and still attempts to dial out to the participant. If the dial-out participant was designated as the conference lecturer, the MCU can't replace that participant with the dial-in participant that is connected to the conference.

---

5. To override the layout identified in the selected conference profile, click **Media Sources** and enable **Override layout from profile**.
6. To add optional conference information, click **Information** and enter the required text into the **Info1**, **Info2**, **Info3**, or **Billing Info** text boxes.
7. Click **OK** to start the conference.

   Unless otherwise specified, the system automatically assigns the conference an ID when the conference starts.
8. Communicate the conference ID to conference dial-in participants.

Related Links

Conference Profile Parameters on page 138

Other Ways to Start a Conference

The RealPresence Collaboration Server provides many ways to start a conference.

The most common method is documented previously. The other ways include:

- By dialing into a meeting room
- By dialing into an ad hoc entry queue
- By clicking on a reservation in the calendar
  - If the reservation start time is past due, the conference starts immediately.
  - If the reservation start time is in the future, the conference starts at the specified date and time.
- By clicking on a conference template and selecting **Start Conference from Template**
- By copying and pasting a conference in the Conferences list.
- From Microsoft Outlook using the Polycom Conferencing Add-in for Microsoft Outlook.
  - Polycom Conferencing for Microsoft Outlook is an add-in that enables users to easily organize and invite attendees to video-enabled meetings via Microsoft Outlook.
  - This feature is applicable to Continuous Presence (CP) conferences only.

Working with Active Conferences

Topics:

If your environment has a standalone RealPresence Collaboration Server, you can use it to manage active conferences.

Note: If your organization uses another conference management application such as a Poly Clariti Manager system, Poly recommends that you create and schedule conferences using that application and not the MCU.

This section discusses the actions available to administrators, operators, and chairpersons as they interact with active conferences.

General Conference Management Tasks

An RealPresence Collaboration Server (RMX) administrator or operator may be required to perform these general conference management tasks on an active conference.

View the List of Active Conferences

You can view the list of active conferences using RMX Manager.

Procedure

» Open the RMX Manager.

The list of active conferences displays in the **Conferences** pane.

Viewing of Ongoing SVC Conference Properties

You can view the properties of ongoing SVC conference.

Procedure

1. In the ***Conference*** list pane, double-click the SVC conference or right-click the SVC conference and select **Conference Properties**.

   The ***Conference Properties*** **- General** dialog opens.

   The parameters in the **General** tab are identical to those of CP and Mixed conferences.
2. Open the **Advanced** tab.

   The parameters in the ***Advanced*** tab are identical to those of CP and Mixed conferences.
3. Open the **Video Quality** tab.

The parameters in the **Video Quality** tab are identical to those of CP and Mixed conferences.

4. Open the **Video Settings** tab to view the video parameters defined for the conference.

   In SVC conferences, only Auto Layout is enabled and cannot be disabled. All other video settings are disabled.
5. Open the **Audio Settings** tab to view the audio parameters defined for the conference.

   In SVC conferences, all Audio Settings options are disabled.
6. Open the IVR tab to monitor the conference IVR settings.
7. Open the Network Services tab to monitor the conference network services definitions.
8. Open the Layout Indications tab to view (only) the layout indications set for the conference.

   In SVC conferences, Layout Indications are inapplicable.
9. Click **OK** to close the ***Conference Properties*** dialog.

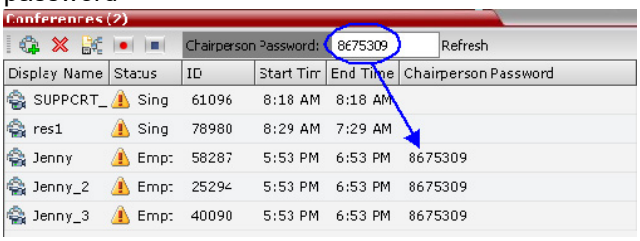
Search for an Ongoing Conference by Chairperson Password

If you are logged in as a chairperson, the Chairperson Password field is displayed.

It enables you to search for, and display a list of, ongoing conferences for which you have the password.

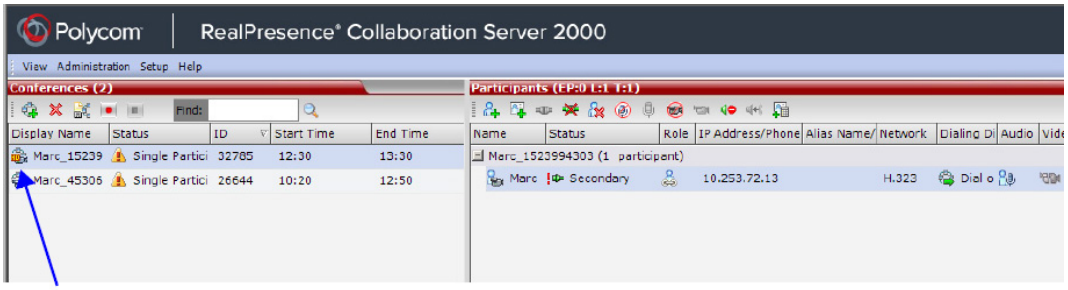
Procedure

1. In the **Chairperson Password** field, enter the password, to be used for the search.
2. Click **Refresh** to refresh the **Conferences** list and display ongoing conferences with the requested password



You can also click the blinking **Participant Alerts** indication bar to view participants that require attention.

Note that Video Switching conferences appear with the HD ( ) icon in the conferences list to differentiate between CP and VSW conferences.



VSW Conference

Monitoring is done in the same way as for CP conferences.

View the Properties of an Active Conference

In general, a conference's properties are derived from the conference profile and conference template used to define the conference.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.
2. Right-click and select **Conference Properties**.

Related Links

Conference Profile Parameters on page 138

Lock a Conference

You must be logged in as a chairperson, operator, or administrator to lock an active conference.

Locking the conference hides the list of conference participants in the Participants pane. If the conference is locked, a voice prompt informs users that the conference is secured and they cannot join.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to lock.
2. Right-click and select **Lock Conference**.

Unlock a Conference

You must be logged in as a chairperson, operator, or administrator to access this feature.

When the conference is unlocked, a voice prompt informs users that they can join the conference and all participants taking part in the conference are displayed.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference to want to unlock.
2. Right-click and select **Unlock Conference**.

Participant Management Tasks

An RealPresence Collaboration Server (RMX) administrator or operator may be required to perform participant management tasks for participants who are in an active conference.

View Information for Active Conference Participants

You can view the list of participants in an active conference, including information about the conference participant’s state and other participant properties.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.

   RMX Manager displays the **Participants List** and the status of each participant including the following information:

Column	Icon/Description
Name	Displays the name and type of the participant: • **Audio Participant**: Connected via IP phone or ISDN (audio/video).
Status	Displays the connection status of the participant. • **Connected**: The participant is successfully connected to the conference. • **Disconnected**: The participant is disconnected from the conference. This status applies only to defined participants. • **Waiting for Dial-in**: The system is waiting for the defined participant to dial into the conference. • **Partially Connected**: The connection process isn't yet complete; the video channel hasn't connected. • **Faulty Connection**: The participant is connected, but problems occurred in the connection, such as synchronization loss. • **Secondary Connection**: The endpoint's video channel can't connect to the conference and the participant is connected only via audio. • **Awaiting Individual Assistance**: (AVC-based connection) The participant has requested the user's (operator's) assistance. • **Awaiting Conference Assistance**: (AVC-based connection) The participant has requested the operator's assistance for the conference. This usually means that the user (operator) has been requested to join the conference. • **Connected, Noisy**: Participant's endpoint is requesting too many intras, resulting in the MCU ceasing to send intras to the endpoint to preserve conference quality for all other participants.

Column	Icon/Description
Role	Displays the participant's role or function in the conference. • **Chairperson**: The participant is defined as the conference chairperson. The chairperson can manage the conference using touch-tone signals (DTMF codes). • **Lecturer**: (AVC-based connection) The participant is defined as the conference lecturer. • **Lecturer and Chairperson**: The participant is defined as both the conference lecturer and chairperson. • **Cascade-enabled Dial-out Participant**: (AVC dial-outs only.) A special participant functioning as a link in a cascaded conference. • **Recording**: (AVC-based connection) A special participant functioning as a recording link. **Note:** The Recording participant doesn't support H.264 High Profile. If recording a conference set to H.264 High Profile, the Recording participant connects as Audio Only and records the conference Audio while displaying the recording icon for the conference. • **Request to speak**: (AVC-based connection) Participants that were muted by the conference organizer or system operator can enter a DTMP code (default 99) to indicate that they want to be unmuted. The icon displays for 30 seconds.
IP Address/Phone	An IP participant's IP address or an ISDN (audio/video) participant's phone number.
Alias Name/SIP Address	The participant's alias name or SIP URI. The alias of a RealPresence Media Suite if the participant is functioning as a recording link.
Network	The participant's network connection type: **H.323**, **SIP**, or **ISDN (audio/video)**.
Dialing Direction	How the participant connected to the conference. • **Dial-in**: The participant dialed the conference. • **Dial-out**: The MCU dialed the participant.

Column	Icon/Description
Audio	Displays the status of the participant's audio channel. If the participant's audio is connected and the channel is not muted or blocked, no indication displays. • **Disconnected** : Participant's audio channel is disconnected. This is a defined participant who is waiting to be connected to the conference. • **Muted** : Participant's audio channel is muted. Indicates who initiated the mute: participant, RealPresence Collaboration Server Operator, or MCU. The participant can still hear the conference. • **Blocked** : Transmission of audio from the conference to the participant is blocked. • **Muted and Blocked** : Audio channel is muted and blocked.
Video	Displays the status of the participant's video channel. If there is no problem with the participant's video connection and the channel is not suspended or secondary, no indication displays. • **Disconnected** : Participant's video channel is disconnected. This is a defined participant who is waiting to be connected to the conference. • **Suspended** : Video transmission from the endpoint to the conference is suspended. • **Secondary** : Participant is connected only through the audio channel due to problems with the video channel.
Encryption	: (AVC-based connection) Indicates that the endpoint is connected to the conference using encryption.
Service Name	Displays the IP Network Service used to connect this participant to the conference.
FECC Token	: Participant is the holder of the Far End Camera Control (FECC) token and has FECC capabilities. The FECC token can be allocated to only one participant at a time and remains unallocated if no participant requests it. **Note:** FECC isn't supported with ISDN-video.
Content Token	: Participant holds the content token and has content sharing permission. The content token can be allocated to only one participant at a time and remains unallocated if no participant requests it.

2. For more information about a participant, select the participant whose information you want to view.
3. Right-click and select **Participant Properties**.

Related Links

Participant Properties on page 160

Add a Participant or Group to an Active Conference

Operators and administrators can add participants to active conference.

If no participants were defined for the conference or as long as no participants are connected, the indication **Empty** and a warning icon () appear in the **Status** column in the **Conferences** pane.

The conference status changes when participants connect to the conference.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.
2. Click **Participants** and then do one of the following:
   - Click **Add from Address Book**, select the required groups and participants, and click **Add**.
   - Click **New**, enter the required information for the new participant, and click **Add**.

   If any of the participants added to the conference are dial-out participants, the MCU initiates a call to the participant.

Related Links

Participant Properties on page 160

Add a Participant in an Active Conference to the Address Book

You can add a participant of an active conference to the Address Book, thus saving their information for future conferences.

In this case, the participant is always added to the Main group in the Address Book.

Procedure

1. In the **Conferences** list of RMX Manager, select the active conference you want to view.
2. In the **Participant** list, select the participants to add.
3. Right-click and select **Add Participant to Address Book**.

Related Links

Participant Properties on page 160

Viewing the Properties of Participants

You can view the participant properties.

Procedure

» In the **Participant List** pane double-click the participant entry.

Alternatively, right-click a participant and select **Participant Properties**.

The ***Media Sources*** dialog box enables you to mute participant's audio, suspend participant's video transmission and select a personal Video Layout for the participant.

Move Participants Between Conferences

A RealPresence Collaboration Server (RMX) administrator or operator can move participants between active Continuous Presence (CP) Only conferences or between an Entry Queue and active CP conference (if the participant failed to enter the correct conference ID or conference password).

A RealPresence Collaboration Server (RMX) administrator or operator can't move participants from Polycom Lost Packet Recovery (LPR) enabled, Video Switching, or Telepresence conferences. Moving participants between encrypted and nonencrypted conferences depends on the **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF** flag setting, as described in the following table:

Participant Move Capabilities vs. ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF Flag Setting

Flag Setting	Source Conference /Entry Queue Encrypted	Destination Conference Encrypted	Move Enabled?
NO	Yes	Yes	Yes
NO	Yes	No	Yes
NO	No	Yes	No
NO	No	No	Yes
YES	Yes	Yes	Yes
YES	Yes	No	Yes
YES	No	Yes	Yes
YES	No	No	Yes

Note the following:

- When moving participants, IVR messages and slide display (if enabled for the conference) are skipped.
- When moving dial-out participants, they'll be disconnected from the original conference, and then the MCU automatically dials out to connect them to the destination conference (AVC dial-outs only).
- Moving participants is not supported when the MCU is in SVC-only mode.
- Participants in cascaded conferences links cannot be moved between conferences.
- Paticipants that require Modular MCU (MMCU) translator cannot be moved between conferences.
- Participants cannot be moved to a conference if the move will cause the number of participants to exceed the maximum number of participants allowed for the destination conference.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.
2. In the **Participant** list, select the participant to move.
3. Right-click and select one of the following options:
   - **Move to Operator Conference** - To move one or more participants to an Operator conference.
   - **Move to Conference** - To move the participant to another ongoing CP conference.

- **Back to Home Conference** - If the participant was moved to another conference or to an Operator conference, this option returns the participant back the original conference.

  This option isn't available if the participant was moved from an Entry Queue to an active conference.

4. In the **Move to Conference** option, select the destination conference and click **OK**.

Related Links

Operator Conferences and Assistance on page 194
User Management on page 257
Conference Profiles and Templates on page 136

Configure a Participant's Conference Display Name

Administrators and operators can configure the MCU to display participants' names (as found in the Address Book) into an active conference rather than their endpoint system names as found in the endpoint (which is often the endpoint site name).

When enabled, the MCU retrieves the endpoint system data (name, alias, number, or IP address) for each dial-in participant and compares it first with the conference dial-in participants list. If the endpoint isn't found there, the MCU then compares the data to entries in the Address Book. If a match is found, the system displays the participant's name as defined in the Address Book.

The system compares the following endpoint data with the Address Book entries:

- For H.323 participants, the system compares the IP address, Alias, or H.323 number.
- For SIP participants, the system compares the IP address or the SIP URI.

Note: This feature is supported for IPv4 participants only.

Procedure

1. In RMX Manager, go to **Setup** > **Customize Display Settings** > **Ongoing Conferences**.
2. Select **Obtain display name from address book** and click **OK**.

Send a Message to Participants During a Conference

Using the Message Overlay feature, an RealPresence Collaboration Server (RMX) administrator or operator can send messages to a single conference participant, a number of selected participants, or all conference participants.

The RealPresence Collaboration Server (RMX) user can enable or modify the Message Overlay feature for active conferences or for future conferences as part of the conference profile.

The Message Overlay feature isn't available in the following circumstances:

- In Video Switching (VSW) conferences.
- In Lecture Mode.
- When the PCM menu is active.
- On endpoints that have their video suspended.

Note: The content streams sent by the RealPresence Collaboration Server towards SVC endpoints are AVC (H.264 encoded) streams. Enabling content transcoding in a Mixed mode conference causes the RealPresence Collaboration Server to use a single content encoder for sending content to H.264 AVC and SVC endpoints. Similar to the AVC endpoints, all SVC endpoints joining a conference with message overlay on content stream enabled, receive the configured message overlay on their content streams in content transcoding mode. But SVC endpoints don't receive the same message overlay on their people video, as by design RealPresence Collaboration Server doesn't support message overlay on SVC video streams.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.
2. In the **Participant** list, select the participants to receive the message.
3. Right-click and select **Send Text Message to Participant**.
4. In the **Conferences** list, select the conference again.
5. Right click and select **Conference Properties**.
6. Go to **Message Overlay** and select the **Enable** check box.
7. In the **Content** field, enter the message text (up to 50 characters) to be displayed to selected conference participants.

   Note that the number of characters that can be included in a message varies according to the language and the type and size of font used.
8. Specify the font size, color, position, and transparency.
9. Specify the speed at which the text should move (static, slow, or fast) and how often it should repeat.
10. Click **OK**.

    Changes to the Message Overlay content or display characteristics (position, size, color, and speed) are immediately visible to all participants.

Cancel a Message Overlay

You can cancel the messages being sent to conference participants whether the message is part of the conference profile or not.

Procedure

1. In the **Conferences** list of RMX Manager, select the active conference of interest.
2. Right click and select **Conference Properties**.
3. Go to **Message Overlay** and clear the **Enable** check box.

Secure Meeting Lobby

You can configure your RealPresence Collaboration Server to include a secure meeting lobby to hold callers that try to join an active locked conference.

When you implement the secure meeting lobby, the MCU routes callers who try to join an active locked conference into the secure meeting lobby, using a designated IVR message and slide. The MCU then sends a notification to all conference chairpersons (with AVC endpoints) that one or more callers are waiting in the meeting lobby. The notification provides the following information:

- A list of the most recent five callers to join the lobby (by user or site name).
- The total number of callers waiting in the lobby.

Callers stay in the meeting lobby until a chairperson unlocks the conference, the caller's designated time-duration elapses, or the conference ends.

- When a chairperson unlocks the conference, all callers in the meeting lobby join the meeting. Chairpersons can't choose which waiting callers join the meeting.

  Important: Once a chairperson unlocks a conference to allow users to join from the meeting lobby, the conference remains unlocked until a chairperson explicitly relocks the conference.

- If a chairperson doesn't unlock the conference before a caller's wait time expires, RealPresence Collaboration Server immediately disconnects the caller from the meeting lobby.
- When the conference ends (for any reason), RealPresence Collaboration Server disconnects all waiting callers from the meeting lobby.

Chairpersons can lock or unlock conferences using RMX Manager or DTMF tones.

Note the following:

- Because the RealPresence Collaboration Server only sends the meeting lobby notification to conference chairpersons with AVC endpoints, at least one chairperson for the conference must connect with an AVC endpoint if you enable this option.
- To use this option, the conference can't be in **Prefer TIP** or **Lecture** mode.

Configure Secure Meeting Lobby Settings

You can enable the secure meeting lobby feature and configure the lobby wait time and notifications using system flags.

If you enable or disable this feature during an ongoing conference, the current conference is not affected.

Procedure

» In RMX Manager, add the following system flag(s):

ENABLE_LOBBY_FOR_LOCKED_CONFERENCE

Enables or disables the secure meeting lobby feature.

NO - Disables the feature.

YES - Enables the feature.

WAITING_IN_LOBBY_DURATION

The number of seconds users wait in the secure meeting lobby before RealPresence Collaboration Server disconnects them.

Range of Values: 60 to 300

WAITING_IN_LOBBY_MESSAGE_OVERLAY_REPETITIONS

The number of times the secure meeting lobby notification displays to chairpersons in a locked conference.

Range of Values: 1 to 10

Designate a Participant as the Lecturer in an Active Conference

During an ongoing conference, you can change the conference to Lecture Mode by designating a participant the lecturer.

In Lecture Mode, all participants see the lecturer in full screen, while the conference lecturer sees all the other conference participants in the selected layout. When the number of participants in a conference is greater than the number of cells in the conference layout, switching between participants occurs every 15 seconds. Automatic switching is suspended when one of the participants begins talking, and it's resumed automatically when the lecturer resumes talking.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference of interest.
2. Right click and select **Conference Properties**.
3. Go to **Video Settings**, and in the **Lecturer** field, select the lecturer from the list of the connected participants.
4. To enable automatic switching between participants viewed on the lecturer's screen, enable Lecturer View Switching.
5. To change the video layout for the lecturer, select another video layout option.
6. Click **OK**.

Related Links

Polycom RealPresence Collaboration Server Features and Capabilities on page 13

Mute Participants Other Than Lecturer

During an ongoing conference (including a cascaded conference) that is set to Lecture Mode, you can mute all participants other than the lecturer.

This prevents conference participants from interrupting the lecture.

You can enable or disable the **Mute Participants Except Lecturer** option at any time after the start of the conference. When enabled, conference participants aren't muted until the lecturer joins the conference.

Muted participants can only be unmuted by:

- A RealPresence Collaboration Server administrator or operator.
- When the **Mute Participants Except Lecturer** option is enabled, the mute indicator on the participant video endpoint display is not visible because the mute participant was initiated by the MCU. You may wish to inform participants that their audio is muted by using the Message Overlay functions.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference of interest.
2. Right-click and select **Profile Properties**.
3. Go to **Audio Settings** and enable the **Mute Participants Except Lecturer** option.
4. If a lecturer isn't identified in the **Lecturer** field, select the lecturer from the list of the connected participants.
5. Click **OK**.

   When the **Mute Participants Except Lecturer option** is enabled and a conference has started, the **Mute by Operator** icon is displayed in the Participants pane.

Preview a Participant's Video

You can preview the video sent from a participant to the conference (MCU) and the video sent from the conference to a participant by selecting the appropriate option from the Participant pop-up menu.

This allows you to monitor the quality of the video sent and received by participant's in conference and identify possible quality degradation. The video preview is displayed in a separate independent window with no disruption to the conference and the video preview window size and resolution are adjusted to the resolution of the PC on which it is displayed.

To display the video preview window, the display system must meet the following minimum system requirements:

- DirectX is installed
- DirectDraw Acceleration is enabled and no other application is using the video resource
- Hardware acceleration is enabled

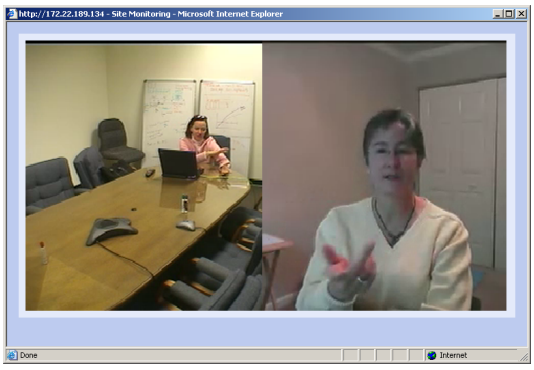
Refer to the system documentation for information about how to enable these options. If the video card installed in the PC doesn't support DirectDraw Acceleration, a black window may be viewed.

Note the following:

- RealPresence Collaboration Server supports Video Preview in AVC CP conferences only.
- Live video shown in the preview window doesn't include shared content being sent by the participant.
- Video preview is supported in cascaded conferences.
- Video preview is disabled in encrypted conferences.
- Video preview isn't displayed when the participant's video is suspended.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view.
2. From the conference **Participants** pane, select the participant whose video you want to preview.
3. Right-click and select one of the following options:
   - **View Participant Sent Video** - Display the video sent from the participant to the conference.
   - **View Participant Received Video** - Display the video sent from the conference to the participant.The **Video Preview** window opens.



Related Links

Polycom RealPresence Collaboration Server Features and Capabilities on page 13

Enable Auto Scan

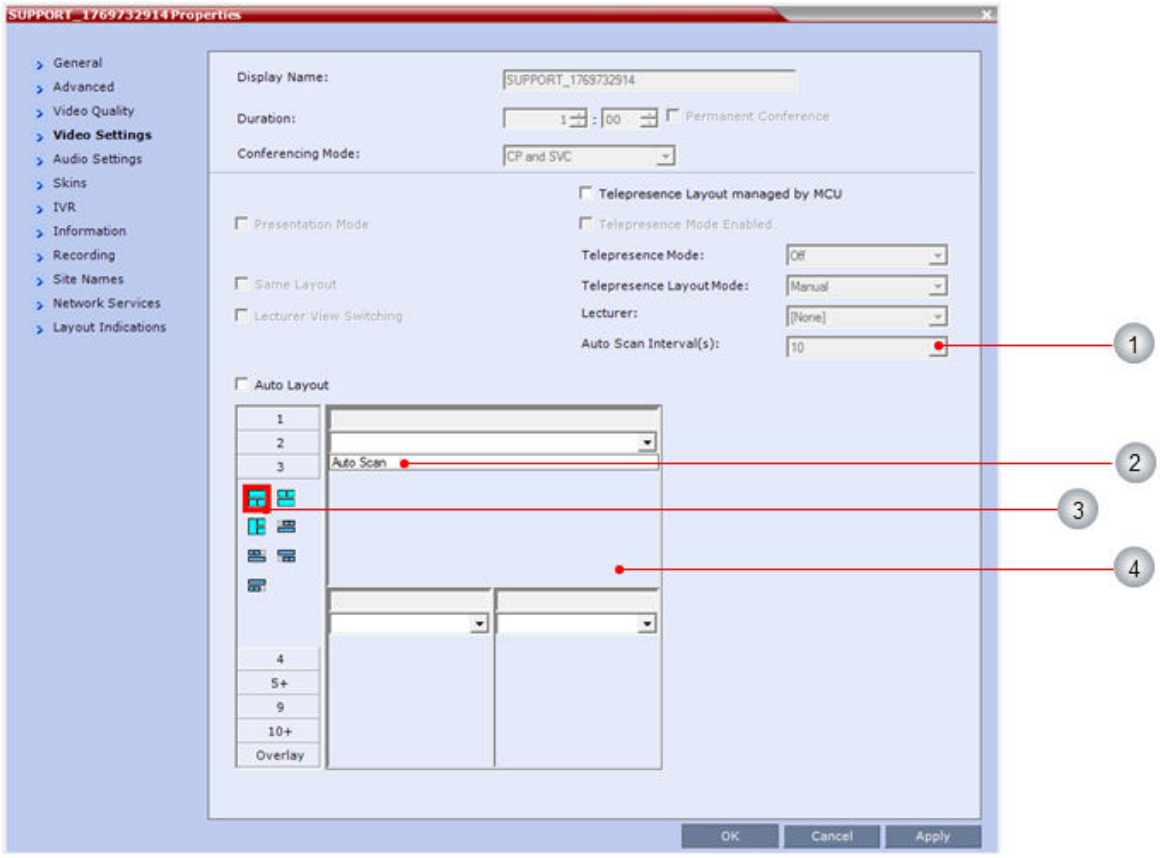
When the number of participants in a conference is greater than the number of cells in the conference layout, you can display those extra participants within a single designated cell in the conference layout.

Auto Scan only takes effect when the number of participants is larger than the number of cells in the conference layout. RealPresence Collaboration Server supports Auto Scan in AVC CP conferences only.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference you want to view and click **Conference Properties**.
2. Right-click and in the **Conference Properties - General** dialog, click **Video Settings**.

   The **Video Settings** dialog displays.



Reference Number	Description
1	Auto Scan interval
2	Auto Scan option
3	Selected Video Layout
4	Selected video layout cell

3. If the **Auto Layout** check box is selected, clear it.

4. In the video layout cell to be designated for Auto Scan, select **Auto Scan** from the drop-down menu.
5. Select the scanning interval from the **Auto Scan Interval(s)** list.
6. Click **Apply** or **OK**.

Define the Scan Order in the Customized Polling Tab

Customized Polling allows you to define an Auto Scan order and an Auto Scan time interval.

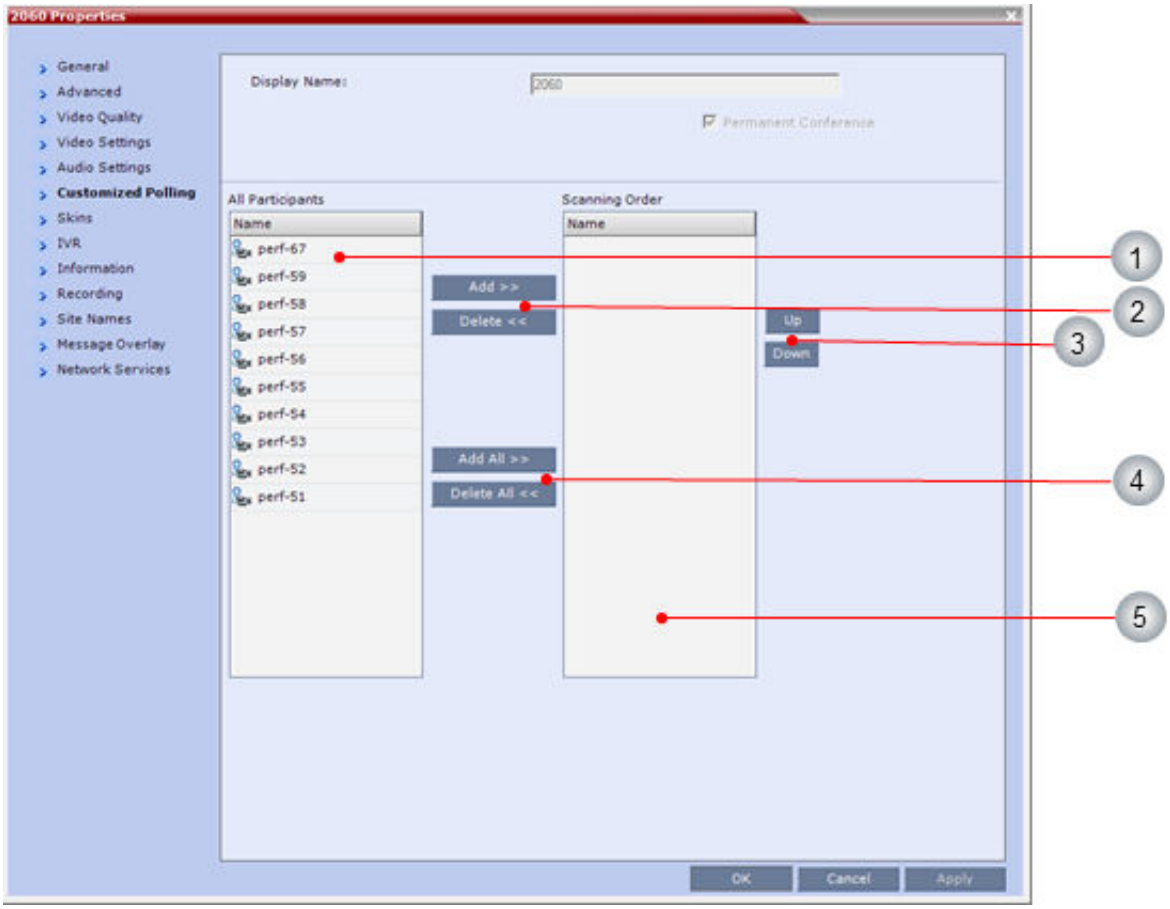
Customized Polling only takes effect when the number of participants is larger than the number of cells in the layout.

Note the following:

- RealPresence Collaboration Server supports Auto Scan and Customized Polling in AVC CP conferences only.
- If Customized Polling isn't defined, the RealPresence Collaboration Server will Auto Scan based on the order in which participants connected to the conference.

Procedure

1. In the RMX Manager **Conferences List**, select the active conference of interest, and click **Conference Properties**.
2. Right-click and in the **Conference Properties - General** dialog, click **Customized Polling**.



Reference Number	Description
1	All conference participants
2	Add/Delete
3	Move Participant up or down in Scanning Order
4	Add All/Delete All
5	Scanning order

All conference participants are listed in the left pane (**All Participants**) whereas the participants to be displayed in the Auto Scan enabled cell are listed in the right pane (**Scanning Order**).

3. Use the buttons in the dialog to select the participants and determine their scanning order.
4. Click **Apply** or **OK**.

Monitoring ISDN (audio/video) Participants

Using the **Participant Properties** dialog, you can monitor and verify the properties of an ISDN (audio/video) participant.

The dialog tabs contain information that is relevant to the participant's status only while the conference is running and is used to monitor the participant's status when connection problems occur.

Note: Maximum line rate ISDN-video endpoints can connect to a conference is 768 kbps.

Procedure

1. In the **Participants** list, right click the desired participant and select **Participant Properties**.

   The **Participant Properties - Media Sources** dialog is displayed.

   ISDN (audio/video) Participant Properties - Media Sources

Field	Description
Mute/Suspend	Indicates if the endpoint's audio and/or video channels from the endpoint have been muted/suspended. The entity that initiated audio mute or video suspend is also indicated. • MCU - Audio or Video channel has been muted/suspended by the MCU. • User - Channels have been muted/suspended by the Collaboration Server user. • Participant - Channels have been muted/suspended by the participant from the endpoint. You can also toggle mute/suspend states using these check boxes.
Block (Audio)	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.

2. Open the H.221 tab to view additional information that can help to resolve connection issues.

Column	Description
Remote Capabilities	Lists the endpoint’s capabilities as retrieved from the remote site
Remote Communication Mode	Displays the endpoint’s actual capabilities as used for the connection

Participant Properties - H.221 Parameters

Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

3. Open the Connection Status tab to view general information regarding the participant connection/disconnection causes of the participant to the conference.

ISDN (audio/video) Participant Properties - Connection Status

Field	Description
Status	Indicates the connection status of the participant to the conference. If there is a problem, the appropriate status is displayed, for example, Disconnected.
Connection Time	The date and time the participant connected to the conference.
Disconnection Time	The date and time the participant was disconnected from the conference.
Connection Retries Left	Indicates the number of retries left for the system to connect the participant to the conference.
Call Disconnection Cause	Indicates the reason of call disconnection.

4. Open the Channel Status tab to view the status of a participant channels.

ISDN (audio/video) Participant Properties - Channel Status

Field	Description
Connected Media	Indicates if the participant is connected with Audio, Video and Content media channels.

Field	Description
Channels Used	• Channel - Indicates the channel used by the participants and whether the channel is connected (indicated with a check mark) or disconnected. • Participant Phone Number - In a dial-in connection, indicates the participant's CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, indicates the participant's phone number dialed by the MCU for each channel. • MCU Phone Number - In a dial-in connection, indicates the MCU number dialed by the participant. In a dial-out connection, indicates the MCU (CLI) number as seen by the participant. This is the number entered in the MCU Number field in the Network Service.
Content Token	A check mark indicates that the participant is the current holder of the Content Token.

View the List of Participants Awaiting Help

The **Participant Alerts** section at the bottom of RMX Manager flashes when participants are awaiting help.

Procedure

» Double-click on the **Participant Alert** title to view the list of participants awaiting help.

Content Sharing Management Tasks

An RealPresence Collaboration Server (RMX) administrator or operator may be required to perform these tasks to manage content sharing into an active conference.

Give Exclusive Content Sharing Ownership

When not in Exclusive Content Mode, all conference participants with capable devices can share content with the conference.

As an RealPresence Collaboration Server (RMX) administrator or operator, you can give a participant the exclusive right to share content.

Procedure

1. In the **Participants** list, select the participant to define as the exclusive content token owner.
2. Right-click and select **Change To Content Token Owner**.

   If another participant is currently sharing content, he's requested to release the token, and the participant selected as the token owner is marked as exclusive. RMX Manager displays a content indicator icon in the Role column of the participant's entry in the **Participants** list.

Cancel Exclusive Content Sharing Ownership

An RealPresence Collaboration Server (RMX) administrator or operator can cancel a participant's right to exclusive content sharing.

Doing this returns the conference to its original conference sharing state.

Procedure

1. In the **Participants** list, select the participant currently defined as the exclusive content token owner.
2. Right-click and select **Cancel Content Token Owner**.

Stop a Content Sharing Session

An RealPresence Collaboration Server (RMX) administrator or operator can immediately stop a content sharing session.

Procedure

1. In the **Conferences** list of RMX Manager, select the active conference you want to view.
2. Right-click and select **Abort H.239 Session**.

Restrict Content Sharing in Lecture Mode

You can restrict content sharing/broadcasting to the conference lecturer.

Restricting content sharing/broadcasting prevents the accidental interruption or termination of H.239 content while it's shared in a conference.

Procedure

» Set the **RESTRICT_CONTENT_BROADCAST_TO_LECTURER** system flag to **ON**.

Related Links

System Flags on page 264

Conference Recording Management Tasks

You can only start and stop recording for an active conference when the conference profile assigned to the conference has recording enabled and has a recording link set up.

If you edit the conference profile that is being used for active conferences to enable recording, that change applies to the active conference, but it also applies to all other active conferences and future conferences using that profile, which may not be desirable.

To Record a Conference with Codian IP VCR

Note: This Feature is applicable only to non-virtual MCUs.

Conference recording is available with Codian VCR 2210, VCR 2220 and VCR 2240.

Recording between the Collaboration Server and the Codian VCR is enabled by adding an IP participant to the recorded conference that acts as a link between the conference and the recording device. This

participant is identified as a recording link to the Codian VCR according to the product ID sent from the VCR during the connection phase, in the call setup parameters.

The video channel between the conference and the recording device is unidirectional where the video stream is sent from the conference to the recorder.

If the Codian VCR opens a video channel to the conference - this channel is excluded from the conference video mix.

Procedure

- In the conference, define or add a dial-out participant using the Codian VCR IP address as the address for dialing.

Once added to the conference, the MCU automatically connects the participant (the link to Codian VCR) and the recording is automatically started on the Codian VCR.

A connection can also be defined on the Codian VCR, dialing into the recorded conference using the MCU prefix and the Conference ID as for other dial-in participants in the conference.

This connection is monitored as any other participant in the conference. The connection can also be monitored in the Codian VCR web client.

Operator Conferences and Assistance

Topics:

An Operator conference is a special conference that enables the RealPresence Collaboration Server user acting as an operator to assist participants without disturbing the ongoing conferences and without being heard by other conference participants.

The operator can move a participant from the Entry Queue or ongoing conference to a private, one-on-one conversation in the Operator conference.

Note: Operator conferences and moving participants are supported in AVC CP Conferencing Mode only.

In attended mode, the RealPresence Collaboration Server user (operator) can perform one of the following actions:

- Participants connected to the Entry Queue who fail to enter the correct destination ID or conference password can be moved by the user to the Operator conference for assistance.
- After a short conversation, the operator can move the participant from the Operator conference to the appropriate destination conference (Home conference).
- The operator can connect participants belonging to the same destination conference to their conference simultaneously by selecting the appropriate participants and moving them to the Home conference (interactively or using the right-click menu).
- The operator can move one or several participants from an ongoing conference to the Operator conference for a private conversation.
- The operator can move participants between ongoing Continuous Presence conferences.

Operator assistance to participants is available when:

- Participants have requested individual help (using *0 DTMF code) during the conference.
- Participants have requested help for the conference (using 00 DTMF code) during the conference.
- Participants have problems connecting to conferences, for example, when they enter the wrong conference ID or password.

In addition, the user (operator) can join the ongoing conference and assist all conference participants.

Operator assistance is available only when an Operator conference is running on the MCU.

The Operator conference offers additional conference management capabilities to the RealPresence Collaboration Server users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch.

Related Links

Move Participants Between Conferences on page 181

Operator Conference Guidelines

Use the following guidelines when setting up an operator conference.

- An Operator conference can only run in Continuous Presence mode.
- Operator conference is defined in the Conference Profile. When enabled in Conference Profile, High Definition Video Switching option is disabled.
- An Operator conference can only be created by a User with Operator or Administrator Authorization level.
- Operator conference name is derived from the User Login Name and it cannot be modified.
- Only one Operator conference per User Login Name can be created.
- When created, the Operator conference must include one and only one participant - the Operator participant.
- Only a defined dial-out participant can be added to an Operator conference as an Operator participant. (AVC dial-outs only.)
- Once running, the RealPresence Collaboration Server user can add new participants or move participants from other conferences to this conference. The maximum number of participants in an Operator conference is the same as in standard conferences.
- Special icons are used to indicate an Operator conference in the Ongoing Conferences list and the operator participant in the Participants list.
- An Operator conference cannot be defined as a Reservation.
- An Operator conference can be saved to a Conference Template. An ongoing Operator conference can be started from a Conference Template.
- The Operator participant cannot be deleted from the Operator conference or from any other conference to which she/he was moved to, but it can be disconnected from the conference.
- When deleting or terminating the Operator conference, the operator participant is automatically disconnected from the MCU, even if participating in a conference other than the Operator conference.
- Participants in Telepresence conferences cannot be moved from their conference, but an operator can join their conference and help them if assistance is required.
- Moving participants from/to an Operator conference follows the same guidelines as moving participants between conferences.
- When a participant is moved from the Entry Queue to the Operator conference, the option to move back to the source (Home) conference is disabled as the Entry Queue is not considered as a source conference.
- The conference chairperson cannot be moved to the Operator conference following the individual help request if the Auto Terminate When Chairperson Exits option is enabled, to prevent the conference from automatically ending prematurely. In such a case, the assistance request is treated by the system as a conference assistance request, and the operator can join the conference.

Prerequisites for Operator Assistance

This section describes the prerequisites for Operator Assistance for conferences.

To enable operator assistance for conferences, the following conferencing components must be adjusted or created:

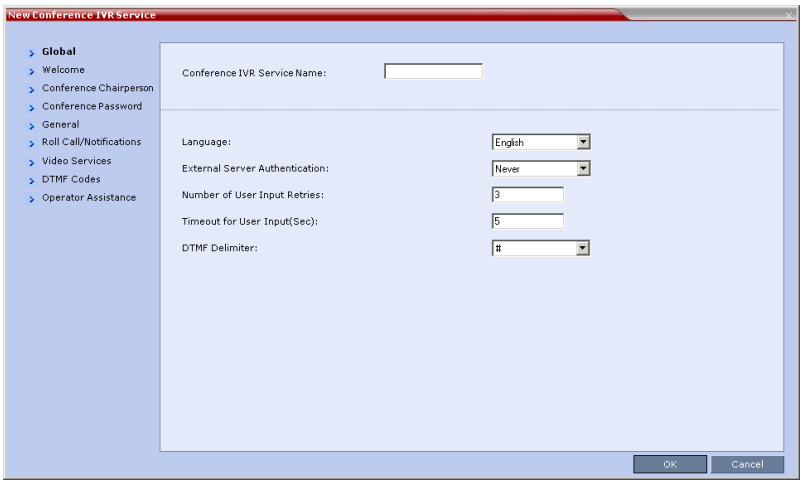
- IVR Service (Entry Queue and Conference) in which Operator Assistance options are enabled.
- A Conference Profile with the Operator Conference option enabled.
- An active Operator conference with a connected Operator participant.

Create a Conference IVR Service for Operator Conferences

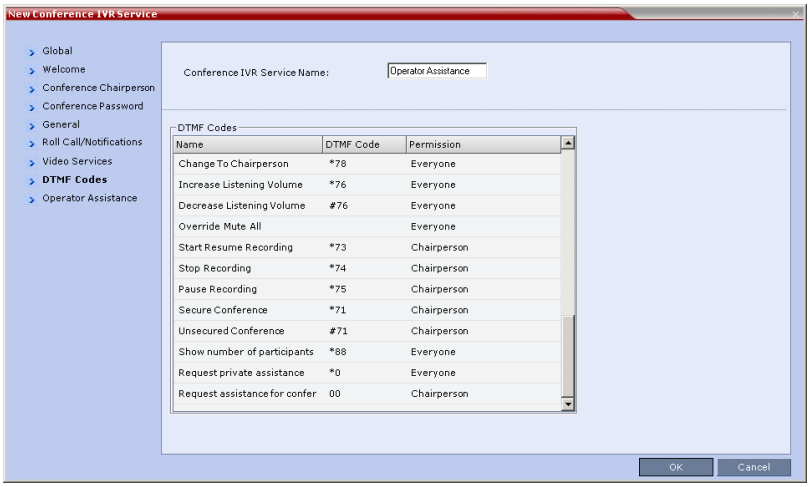
You must create a conference IVR service before you can enable operator assistance during conferences.

Procedure

1. In the **RMX Management** pane, expand the **Rarely Used** list and select **IVRServices**.
2. On the **IVR Services** toolbar, click **New Conference IVR Service**.

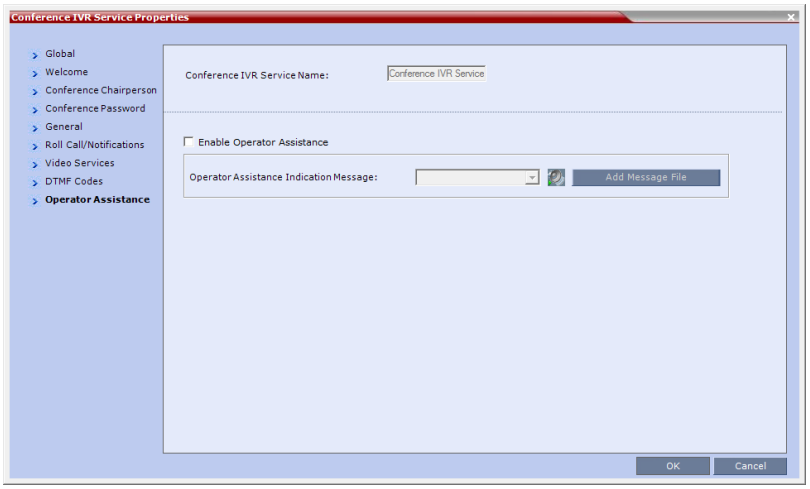


3. Enter the **Conference IVR Service Name**.
4. Define the **Conference IVR Service - Global** parameters.
5. Open the **Welcome** tab and define the system behavior when participants enter the Conference IVR queue.
6. If required, open the **Conference Chairperson** tab, enable the chairperson functionality, and select the various voice message and options for the chairperson connection.
7. If required, open the **Conference Password** tab, enable the request for conference password before moving the participant from the conference IVR queue to the conference.
8. Set the MCU behavior for password request for Dial-in and Dial-out participant connections.
9. Select the various audio messages to play in each scenario.
10. Open the **General** tab and select the messages to play during the conference.
11. Open the **Roll Call/Notifications** tab and enable the Roll Call feature and assign the appropriate audio file to each message type.
12. Open the **Video Services** tab and define the **Video Services** parameters.
13. Open the **DTMF Codes** tab.



The default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson are listed.

14. If required, modify the default DTMF codes and the permissions for various operations including Operator Assistance options:
    - `*0` for individual help - the participant requested help for himself or herself. In such a case, the participant requesting help is moved to the Operator conference for one-on-one conversation. By default, all participants can use this code.
    - `00`for conference help - the conference chairperson (default) can request help for the conference. In such a case, the operator joins the conference.
15. Open the **Operator Assistance** tab.



16. Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.
17. In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.

Note: If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click Add Message File to upload the appropriate audio file to the RealPresence Collaboration Server.

---

18. Click **OK** to complete the IVR Service definition.

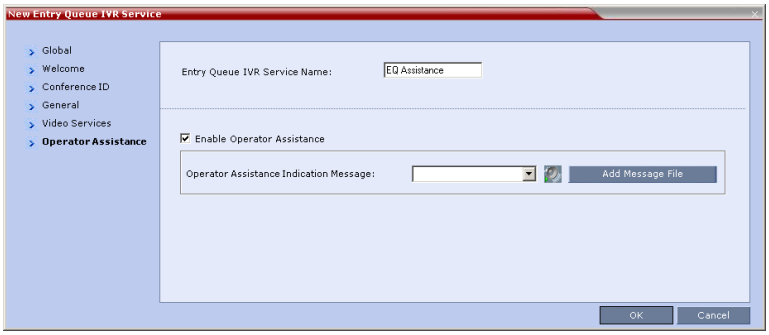
The new Conference IVR Service is added to the **IVR Services** list.

Create an Entry Queue IVR Service for Operator Conferences

You must create an entry queue IVR service before you can enable operator assistance during conferences.

Procedure

1. In the RMX Management pane, select **IVR Services**.
2. In the IVR Services list, click the **New Entry Queue IVR Service** button.
3. Define the Entry Queue Service **Name**.
4. Define the Entry Queue IVR Service Global parameters.
5. Open the **Welcome** tab.
6. Define the system behavior when the participant enters the Entry Queue. This dialog box contains options that are identical to those in the **Conference IVR Service - Welcome Message** dialog box.
7. Open the **Conference ID** tab.
8. Select the required voice messages.
9. Open the **Video Services** tab.
10. In the **Video Welcome Slide** list, select the video slide to display to participants connecting to the Entry Queue. The slide list includes the video slides previously uploaded to the MCU memory.
11. Open the **Operator Assistance** tab.



12. Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.
13. In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

Note: If the audio file wasn't uploaded before the definition of the IVR Service or if you want to add new audio files, click Add Message File to upload the appropriate audio file to the RealPresence Collaboration Server.

---

14. Click **OK** to complete the Entry Queue IVR Service definition.

    The new Entry Queue IVR Service is added to the **IVR Services** list.

Related Links

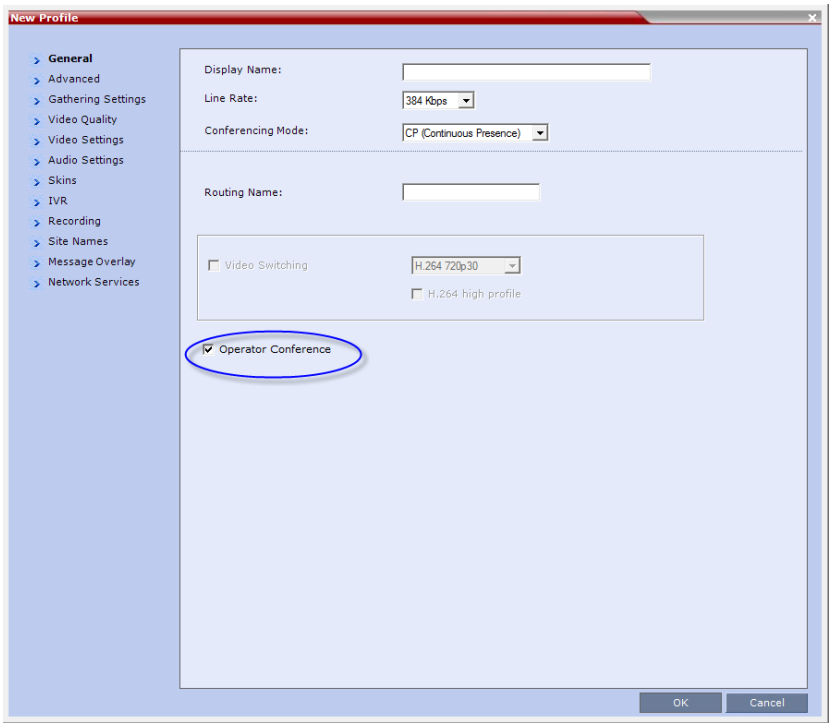
Entry Queues on page 210
Cascading via Entry Queue on page 234

Create a Conference Profile for Operator Conferences

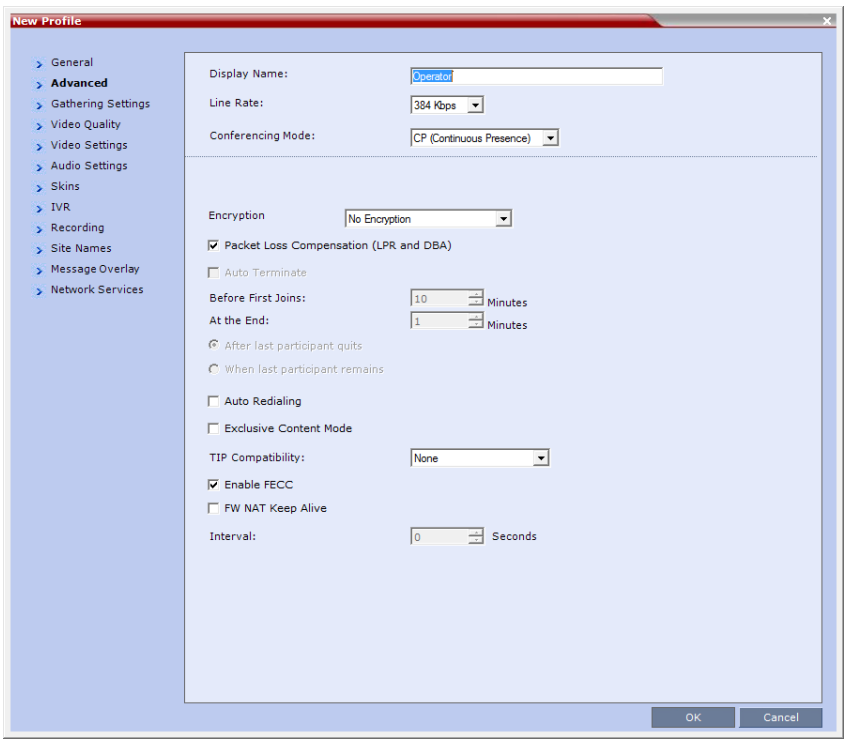
You must define a conference profile before you can enable operator assistance during conferences.

Procedure

1. In the **RMX Management** pane, select **Conference Profiles**.
2. In the **Conference Profiles** pane, click **New Profile**.
3. Define the Profile name and, if required, the Profile general parameters.
4. Select the **Operator Conference** check box.



5. Open the **Advanced** tab.



6. Define the **Profile - Advanced** parameters.

   Note that when Operator Conference is selected, the **Auto Terminate** selection is automatically cleared and disabled and the Operator conference can't automatically end unless it is terminated by the RealPresence Collaboration Server User.
7. Open the **Video Quality** tab.
8. Define the Video Quality parameters.
9. Open the **Video Settings** tab.
10. Define the video display mode and layout.
11. Define the remaining Profile parameters.
12. Click **OK** to complete the Profile definition.

    A new Profile is created and added to the Conference Profiles list.

Related Links

Conference Profile Parameters on page 138

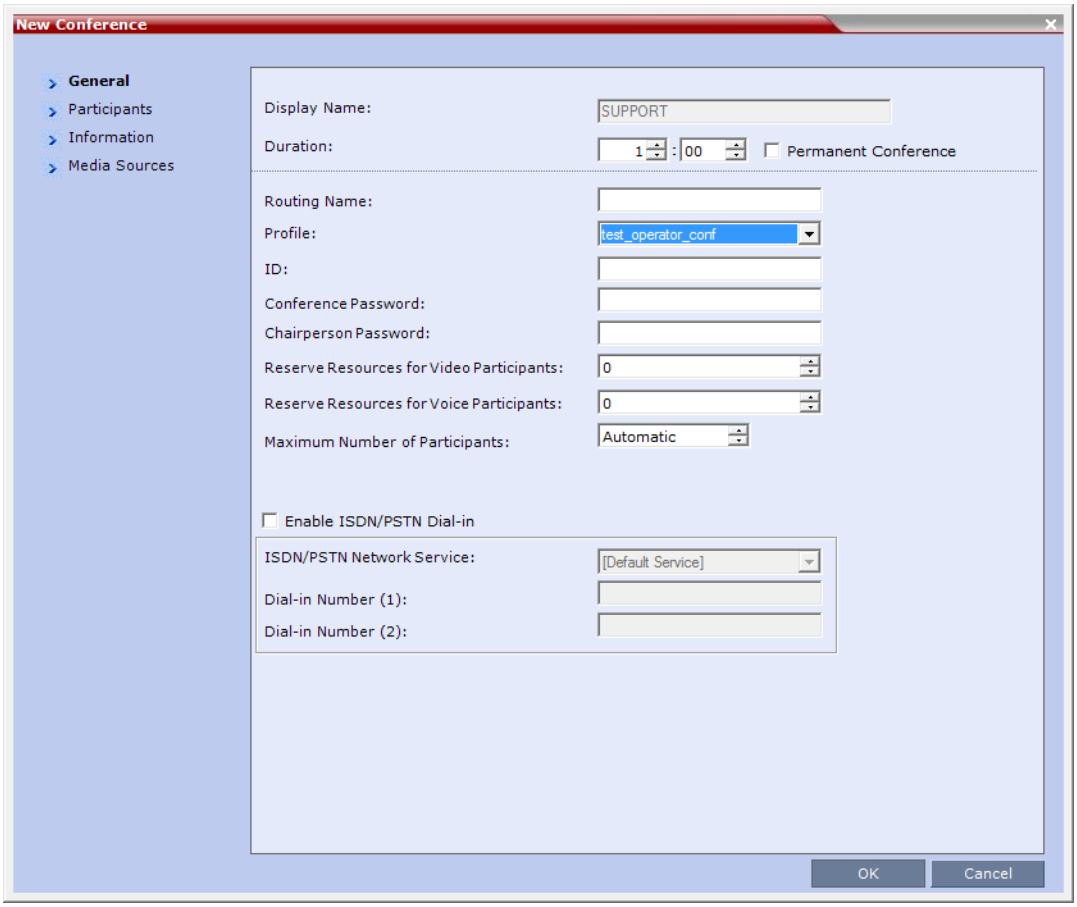
Start an Operator Conference

Once you complete the prerequisites, you can start an operator conference from the MCU.

Procedure

1. In the **Conferences** pane, click **New Conference**.

   In the **Profile** field, select a Profile in which the **Operator Conference** option is selected.



Upon selection of the Operator Conference Profile, the **Display Name** is automatically taken from the RealPresence Collaboration Server User Login Name. This name cannot be modified.

Only one Operator conference can be created for each User Login name.

2. Define the following parameters:

Field	Description
Duration	Define the duration of the conference in hours using the format HH:MM (default 01:00). **Note:** • The Operator conference is automatically extended up to a maximum of 168 hours. Therefore, the default duration can be used. • This field is displayed in all tabs.

Field	Description
Routing Name	The name with which ongoing conferences, Meeting Rooms, Entry Queues, and SIP Factories register with various devices on the network such as gatekeepers and SIP servers. This name must be defined using ASCII characters. Comma, colon, and semicolon characters cannot be used in the **Routing Name**. The **Routing Name** can be defined by the user or automatically generated by the system if no **Routing Name** is entered as follows: • If ASCII characters are entered as the **Display Name**, it's used also as the **Routing Name** • If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the **Display Name**, the ID (such as Conference ID) is used as the **Routing Name**. If the same name is already used by another conference, Meeting Room or Entry Queue, the RealPresence Collaboration Server displays an error message and requests that you to enter a different name.
Profile	Select an operator profile from the Profile drop-down list.
ID	Enter the unique-per-MCU conference ID. If left blank, the MCU automatically assigns a number once the conference is launched. This ID must be communicated to conference participants to enable them to dial in to the conference.
Conference Password	Leave this field empty when defining an Operator conference.
Chairperson Password	Leave this field empty when defining an Operator conference.
Reserve Resources for Video Participants	Enter the number of video participants for which the system must reserve resources. Default: 0 participants. When defining an Operator conference, it's recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance). **Note:** This option isn't supported with RealPresence Collaboration Server 1800.

Field	Description
Reserve Resources for Voice Participants	Enter the number of audio participants for which the system must reserve resources. Default: 0 participants. When defining an Operator conference and the operator is expected to help voice participants, it's recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance). **Note:** This option isn't supported with RealPresence Collaboration Server 1800.
Maximum Number of Participants	Enter the maximum number of participants that can connect to an Operator conference (you can have more than two), or leave the default selection (Automatic).
Enable ISDN (audio/video) Dial-in (Not relevant to Virtual Edition MCUs.)	Select this check box if you want ISDN-video and ISDN-voice participants to be able to connect directly to the Operator conference. This may be useful if participants are having problems connecting to their conference and you want to identify the problem or help them connect to their destination conference.
ISDN (audio/video) Network Service and Dial-in Number (Not relevant to Virtual Edition MCUs.)	If you have enabled the option for ISDN (audio/video) direct dial-in to the Operator conference, assign the ISDN (audio/video) Network Service and a dial-in number to be used by the participants, or leave these fields blank to let the system select the default Network Service and assign the dial-in Number. **Note:** The dial-in number must be unique and it cannot be used by any other conferencing entity.

3. Open the **Participants** tab.

   The **New Conference - Participants** dialog opens.

   You must define or add the Operator participant to the Operator conference.

   This participant must be defined as a **dial-out** participant.

   Define the parameters of the endpoint that will be used by the RealPresence Collaboration Server User to connect to the Operator conference and to other conference to assist participants.
4. To insert general information, open the **Information** tab.
5. Enter the required information in the **Information** dialog.
6. Click **OK**.

   The new Operator conference is added to the ongoing Conferences list with a special icon.

   The Operator participant is displayed in the Participants list with an **Operator participant** icon and the system automatically dials out to the Operator participant.

Related Links

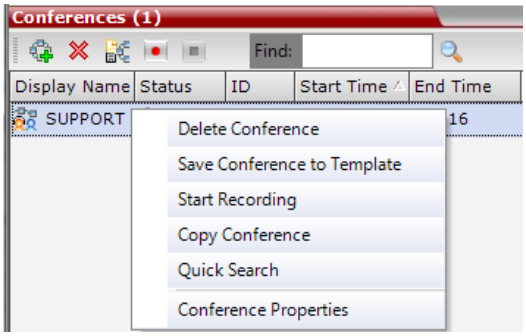
Configuring the Address Book on page 159

Save an Operator Conference to a Template

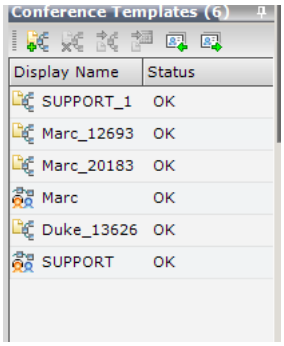
The Operator conference that is ongoing can be saved as a template.

Procedure

1. In the Conferences list, select the Operator conference you want to save as a Template.
2. Do one of the following:
   - Click **Save Conference to Template**.
   - Right-click and select **Save Conference to Template**.



The conference is saved to a template whose name is taken from the ongoing conference Display Name (the Login name of the RealPresence Collaboration Server User). The Template is displayed with the **Operator Conference** icon.



Related Links

Conference Templates on page 148

Start an Operator Conference from a Template

An ongoing Operator conference can be started from an Operator Template saved in the **Conference Templates** list.

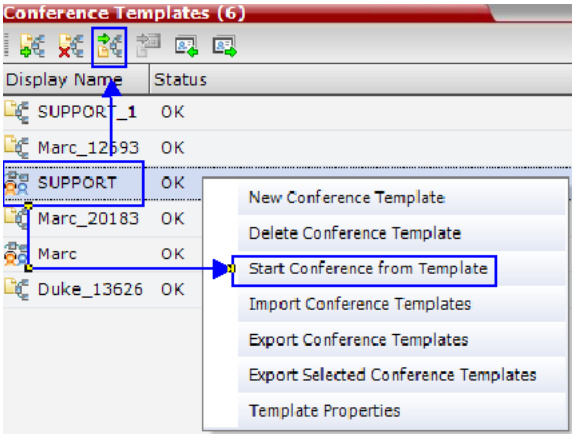
Procedure

1. In the **Conference Templates** list, select the Operator Template to start as an ongoing Operator conference.

Note: You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.

If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you can't start another Operator conference with the same login name.

2. Do one of the following:
   - Click **Start Conference from Template**.
   - Right-click and select **Start Conference from Template**.



The conference starts.The name of the ongoing conference in the **Conferences** list is taken from the conference template **Display Name**.

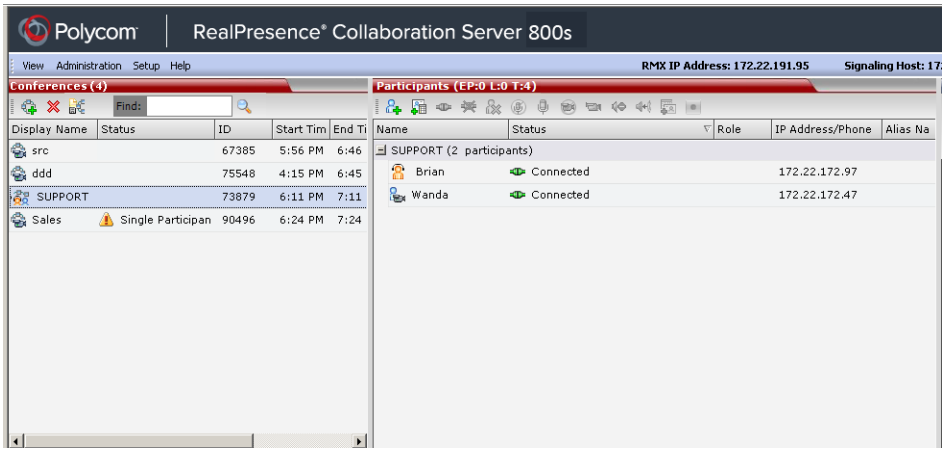
Related Links

Conference Templates on page 148

Monitoring Operator Conferences and Participants Awaiting Assistance

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.



View Operator Conference Properties

You can view the properties of the Operator conference in the RMX Manager.

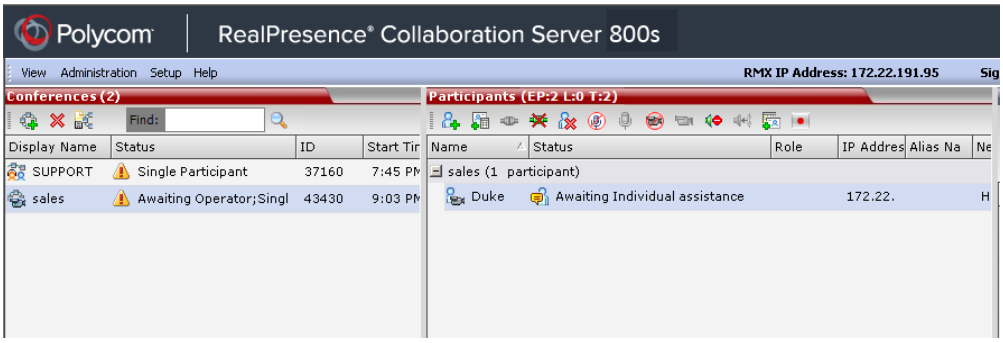
Procedure

1. Open the **Conferences** list in the RMX Manager.
2. Do one of the following:
   - Double-click the conference entry in the **Conferences** list.
   - Right-click the conference entry and select **Conference Properties**.

Monitoring Participants That Are Requesting Help

Participants can request help by enteriung the apropriate DTMF code.

When requiring or requesting operator assistance, the RealPresence Collaboration Server management application displays the following:



- The participant's connection Status changes, reflecting the help request.
- The conference status changes and it's displayed with the exclamation point icon and the status **Awaiting Operator**.
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

When the Operator moves the participant to the Operator conference for individual assistance the participant Status indications are cleared.

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

The following icons and statuses are displayed in the **Participant Status** column:

Participants List Status Column Icons and Indications

Icon	Status Indication	Description
	Awaiting Individual Assistance	The participant has requested the operator's assistance for himself/herself.
	Awaiting Conference Assistance	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

Request assistance during conference

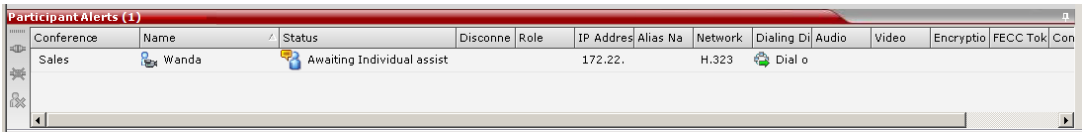
A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device.

Procedure

» In the ongoing conference, choose one of the following to request assistance:
- Enter ***0** for **Individual Assistance**.
- Enter **00** for **Conference Assistance**.

Participant Alerts List

The **Participant Alerts** list contains all the participants who are currently waiting for operator assistance.



Participants are automatically added to the **Participants Alerts** list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator's assistance
- The participant requests Operator's Assistance during the ongoing conference

This list is used as reference only. Participants can be assisted and moved to the Operator conference or the destination conference only from the **Participants** list of the Entry Queues or ongoing conference where they're awaiting assistance.

The participants are automatically removed from the **Participant Alerts** list when moved to any conference (including the Operator conference).

Audible Alarm for Required Assistance Notification

In addition to the visual cues used to detect events occurring on the RealPresence Collaboration Server, an audible alarm can be activated and played when participants request Operator Assistance.

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU via either the RMX Web Client or RMX Manager.

When an Audible Alarm is activated, the *.wav file selected is played and is repeated according to the number of repetitions defined.

If more than one RealPresence Collaboration Server is monitored in the RMX Manager, the Audible Alarm must be enabled separately for each RealPresence Collaboration Server installed in the site/ configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, Audible Alarms are synchronized and played one after the other. Note that when clicking **Stop Repeating Alarm** in the toolbar, all activated Audible Alarms are immediately halted.

An operator/administrator can configure the Request Operator Assistance audible alarm, however Users with different authorization level have different configuration capabilities as shown in the following table:

Audible Alarm Permissions

Option	Operator	Administrator
User Customization	Yes	Yes
Download Audible Alarm File	No	Yes
Stop Repeating Alarms	Yes	Yes

Customize Audio Alerts

The audible alert plays the alert when participants request Operator Assistance.

The operators and administrators can:

- Enable/Disable the Audible Alarm.
- Select whether to repeat the Audible Alarm.
- Define the number of repetitions and the interval between the repetitions.

Procedure

1. In RMX Manager, go to **Setup** > **Audible Alarms** > **User Customization**.
2. Define the following parameters:

Audible Alarm - User Customization Options

Option	Description
Enable Audible Alarm	Select this check box to enable the Audible Alarm feature and to define its properties. When this check box is cleared, the Audible Alarm functionality is disabled.

Option	Description
Repeat Audible Alarm	Select this check box to play the Audible Alarm repeatedly. When selected, it enables the definition of the number of repetitions and the interval between repetitions. When cleared, the Audible Alarm will not be repeated and will be played only once.
Number of Repetitions	Define the number of times the audible alarm will be played. Default number of repetitions is 4.
Repetition interval in seconds	Define the number of seconds that the system will wait before playing the Audible Alarm again. Default interval is 20 seconds.

3. Click **OK**.

Replace Audio Alarm File

Each RealPresence Collaboration Server is shipped with a default tone file in *.wav format that plays a specific tone when participants request Operator Assistance.

This file can be replaced by a *.wav file with your own recording. The file must be in *.wav format and its length cannot exceed one hour.

Only users with Administrator permission can download the Audible Alarm file.

Procedure

1. In RMX Manager, go to **Setup** > **Audible Alarms** > **Download Audible Alarm File**.

   The **Download Audible Alarm File** window opens.
2. Click **Browse**, to select the audio file (*.wav) to download, and click **Open**.

   The selected file name is displayed in the **Install Audible Alarm File** dialog.
3. You can play the selected file or the currently used file by clicking **Play**:

   a. Click **Play Selected File** to play a file saved on your computer.

   b. Click Play **RealPresence Collaboration Server File** to play the file currently saved on the RealPresence Collaboration Server.
4. In the **Download Audible Alarm File** dialog, click **OK** to download the file to the MCU.

The new file replaces the file stored on the MCU. If multiple RealPresence Collaboration Servers are configured in the RMX Manager, the file must be downloaded to each of the required MCUs separately.

Entry Queues, Ad Hoc Conferences, and SIP Factories

Topics:

You can configure entry queues, ad hoc conferences, and SIP factories for your conferencing needs.

Note: When using the Polycom RealPresence Platform, define virtual entry queues and ad hoc conferences in the Poly Clariti Manager system and virtual meeting rooms in the Poly Clariti Core system. Don’t define them directly in the RealPresence Collaboration Server.

Entry Queues

An entry queue (EQ) is a special single-dial routing lobby to participants use access conferences. The entry queue remains in a passive state until participants dial in.

Participants move from the entry queue to the destination conference as long as they have the same conferencing mode, line rate, and video parameters set. For example, participants move from an SVC-only EQ to an SVC-only conference.

The conference profile assigned to the EQ contains the defined conference parameters (bit rate and video properties). Participants connect to the EQ and destination conferences using the same configured values. For example, if the profile bit rate is set to 384 Kbps, all endpoints connect using this bit rate, even if they’re capable of connecting at higher bit rates. You can create different entry queues to accommodate different conferencing modes, parameters, or IVR prompts in different languages.

Related Links

Dial In to an Entry Queue on page 224
Create an Entry Queue IVR Service for Operator Conferences on page 198

Default Entry Queue Properties

RealPresence Collaboration Server contains a default entry queue.

Default Entry Queue Properties

Parameter	Value
Display Name	DefaultEQ You can change the name if required.

Parameter	Value
Routing Name	DefaultEQ You can't change the default routing name.
ID	1000
Profile name	• In appliance MCUs: **Factory_Video_Profile**, with a 384 Kbps bit rate. • In virtual edition MCUs: **Factory_Mixd_CP_SVC_Video_Profile**, with 1920 Kbps bit rate
Entry Queue Service	The default entry queue IVR Service shipped with the system and includes default voice messages and prompts in English.
Ad Hoc	Enabled
Cascade	None (Disabled)
Enable ISDN (audio/ video) Access	Disabled. You can modify the properties of this entry queue to enable ISDN (audio/ video) participants to dial in to a conference. You can assign up to two dial-in numbers.

Add an Entry Queue

You can add an entry queue in the RMX Manager.

Procedure

1. In RMX Manager, go to **RMX Management** > **Entry Queues**.
2. Click **New Entry Queue**.
3. Configure the following settings:

Option	Description
Display Name	The conferencing entity name in native language character sets to be displayed in the RMX Manager. The system automatically generates an ASCII name for the **Display Name** field. You can modify it using Unicode encoding. • The maximum field length in ASCII is 80 characters. • The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. If the name is already in use, the RealPresence Collaboration Server displays an error message requesting you to enter a different name.

Option	Description
Routing Name	Enter a name using ASCII text only. If the routing name is blank, the system automatically assigns a new name as follows: • If **Display Name** uses only ASCII text, then the **Routing Name** uses the display name as the routing name. • If **Display Name** is any combination of Unicode and ASCII text (or full Unicode text), the **Routing Name** uses the conference ID as the routing name.
Profile	The profile that the entry queue uses to determine the bit rate and the video properties with which participants connect to the entry queue and destination conference. Set the profile to **Video Switching** to connect to a video switching conference via entry queue. Poly recommends to use the same profile for both the destination conference and entry queue. In Ad Hoc conferencing, the profile is used to define the new conference properties.
ID	Enter a unique number identifying this conferencing entity for dial-in. Default string length is 4 digits. If you don't manually assign the ID, the MCU assigns one after you complete the definition. The `NUMERIC_CONF_ID_LEN` flag defines the ID string length in the **System Configuration**.
Entry Queue Mode	Select the mode for the entry queue. • **Standard Lobby** (default): When selected, uses the entry queue as a routing lobby to access conferences. Participants connect to a single-dial lobby. Their route to the destination conference is based on the conference ID they enter. • **Ad Hoc**: Select this option to enable the ad hoc option for this entry queue. In this mode, when the participant enters the target conference ID, the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. • **IVR Only Service Provider**: When selected, designates the current entry queue as a special entry queue. The special entry queue provides IVR Services to SIP calls on behalf of the Poly Clariti Core system. This results in the IVR Only Service Provider entry queue routing SIP calls to the Poly Clariti Core system. • **External IVR Control**: Controls the IVR Services externally from an application server (such as Poly Clariti Core) supporting the MCCF-IVR package. When selected, an external IVR service of an application server (for example, Poly Clariti Core) controls and manages the connection process of the participant to the conference via the virtual entry queue.
Entry Queue IVR Service	The default entry queue IVR service. If required, select an alternate entry queue IVR service, which includes the required voice prompts, to guide participants during their connection to the entry queue.

Option	Description
Cascade	Set this field to **None** for all entry queues other than cascading. Use this entry queue to connect dial-in cascaded links, then select **Primary** or **Secondary** depending on the primary/secondary relationship in the cascading topology. • Set this field to **Primary** if: ◦ The MCU on level 1 contains the entry queue and level 2 dials in to level 1. ◦ The MCU on level 2 contains the entry queue and level 3 dials in to level 2. • Set this field to **Secondary** if MCU on level 2 (secondary) contains the entry queue and MCU level 1 dials in to level 2.
Enable ISDN (audio/video) Access	Select this check box to allocate dial-in numbers for ISDN (audio/video) connections. To define the first dial-in number using the default **ISDN (audio/video) Network Service**, leave the default selection. Saving the entry queue on the MCU automatically assigns the dial-in number to the entry queue. This number is within the dial-in numbers range in the default **ISDN (audio/video) Network Service**.
ISDN (audio/video) Network Service	Automatically selects the default network service. To select a different **ISDN (audio/video) Network Service** in the service list, select the name of the network service.
Dial-in Number (1)	Leave this field blank to let the system automatically assign a number from the selected **ISDN (audio/video) Network Service**. To manually define a dial-in number, enter a required number from the dial-in number range defined for the selected network service.
Dial-in Number (2)	By default, the second dial-in number is blank. To define a second-dial-in number, enter a number from the dial-in number range of the selected network service.

4. Click **OK**.

Transit Entry Queues

A transit entry queue contains calls transferred with dial strings that have incomplete or incorrect conference routing information.

A RealPresence Collaboration Server without an transit entry queue rejects all calls containing incomplete or incorrect conference routing information.

In the transit entry queue, the entry queue IVR Service prompts the participant for a destination conference ID. Entering the correct information transfers the participant to the destination conference.

The RealPresence Collaboration Server routes IP calls to the transit entry queue in the following situations:

- Your deployment doesn’t use a gatekeeper.
- A participant dials a call directly to the RealPresence Collaboration Server’s signaling IP address without a conference ID or uses an incorrect conference ID.

- You deployment uses a gatekeeper, and a participant dials only the prefix of the RealPresence Collaboration Server (no conference ID).
- You deployment uses a gatekeeper, and a participant dials the correct prefix of the RealPresence Collaboration Server but uses an incorrect conference ID.

Set a Transit Entry Queue

You can only define one transit entry queue at a time for a RealPresence Collaboration Server. If you select another entry queue as the transit entry queue, it overrides your previous selection.

You must have an entry queue in the RealPresence Collaboration Server to set it as a transit entry queue.

Procedure

1. In RMX Manager, go to **RMX Management** > **Entry Queues**.
2. In the entry queues list, right-click the entry queue you want to set, then select **Set Transit Entry Queue**.

Remove a Transit Entry Queue

If you want to remove the transit entry queue from your conferencing deployment, you can cancel the setting.

Procedure

1. In RMX Manager, go to **RMX Management** > **Entry Queues**.
2. In the entry queues list, right-click the entry queue you want to set, then select **Cancel Transit Entry Queue**.

Entry Queues and ISDN (Audio/Video)

You can assign an ISDN (audio/video) dial-in number to the entry queue to enable ISDN (audio/video) participants to dial in to the entry queue. You can assign up to two dial-in numbers to each EQ.

Allocate the dial-in numbers only from the dial-in number range defined in the ISDN (audio/video) Network Service. You can allocate the two dial-in numbers from the same ISDN (audio/video) Network Service or from two different ISDN (audio/video) Network Services.

Once you've assigned the dial-in numbers, communicate the dial-in number to the ISDN-video or ISDN-voice dial-in participants.

IVR Provider Entry Queue (Shared Number Dialing)

With a Poly Clariti Core system, you can configure the RealPresence Collaboration Server entry queue to provide the IVR Services to SIP endpoints.

You must assign an entry queue IVR service to the entry queue. The IVR enables voice prompts and a video slide that guide the participants through the connection process.

The IVR service performs the following tasks:

- Displays the welcome slide
- Plays the welcome message
- Retrieves the destination conference ID using DTMF codes

Use the following guidelines when defining IVR provider entry queues:

- Defining an entry queue as **IVR Only Service Provider** doesn’t route the SIP call to a target conference.
- You can’t use the entry queue to route calls on the RealPresence Collaboration Server. In such a configuration, the Poly Clariti Core system handles the calls. You must define normal entry queues separately.
- You must disable **Operator Assistance** in the IVR service assigned to this entry queue.
- Only configure the conference ID prompts. **IVR Only Service Provider** configuration doesn't support any other prompts.
- The entry queue rejects ISDN-voice, ISDN-video, and H.323 calls.
- You must configure Poly Clariti Core to locate the **IVR Only Service Provider** entry queue on the RealPresence Collaboration Server. To locate the entry queue, Poly Clariti Core requires the entry queue’s ID number and the RealPresence Collaboration Server signaling IP address (xxx.xx.xxx.xx).

Define an IVR Provider Entry Queue

The IVR provider entry queue doesn’t forward calls to conferences running on the RealPresence Collaboration Server. Its main functionality is to provide IVR services.

Procedure

1. In RMX Manager, go to **RMX Management** > **Entry Queues**.
2. Click **New Entry Queue**.
3. In the **Entry Queue Mode** drop-down list, select **IVR Only Service Provider**.
4. Click **OK**.

Using External IVR Services via the MCCF-IVR Package

You can control IVR Services externally from an application server supporting the Media Control Channel Framework-Interactive Voice Response (MCCF-IVR) package.

Use the following guidelines when using external IVR services via the MCCF-IVR package.

- It only supports AVC SIP and TIP protocols.
- MCCF channels support both IPV4 and IPV6.
- Disconnection of the MCCF channel raises an alarm and deletes all external IVR files. When the MCCF channel reconnects, the MCU receives all the external IVR files.
- Restarting the RealPresence Collaboration Server (MCU), deletes all existing external IVR files. When the MCCF channel connects to the RealPresence Collaboration Server, the server receives all the external IVR files.
- It doesn't support H.323 and ISDN-video protocols.
- Video switching conferences don’t support the TIP protocol
- TIP-based conferencing doesn’t support the following features during conferences:
    - Gathering phase
    - Skin display
    - Text messaging using message overlay
    - Site name display
    - PCM
    - Click&View

- To play audio messages and display the welcome slide during the conference via the virtual entry queue, the media files must meet the following requirements (as defined in the entry queue IVR Service):
  - Audio messages: WAV files - PCM, 16 KHz, 16 bit, Mono
  - Video slides: JPG files - 1920 × 1088 resolution

Disable External IVR Services via the MCCF-IVR

You can configure the external IVR services via the MCCF-IVR settings.

RealPresence Collaboration Server supports external IVR Services via the MCCF-IVR package by default. However, in Ultra Secure Mode and in secure environments, you should disable this option.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. Click **New Flag**.
3. Configure the following options:
   - **New Flag**: Enter `ENABLE_MCCF`.
   - **Value**: Enter `NO`.
4. Click **OK**, then click **Close**.

Ad Hoc Conferencing

The RealPresence Collaboration Server ad hoc conferencing feature enables participants to start ongoing conferences at any time. Conferences don’t require prior definition when dialing in to an ad hoc-enabled entry queue

When the participant enters the target conference ID in the ad hoc-enabled queue, the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID.

The created conference parameters are the same as the profile parameters of the ad hoc-enabled entry queue.

System Settings for Ad Hoc Conferencing

Before a participant can initiate an ad hoc conference (with our without authentication), you must define the ad hoc conferencing components.

Verify that the following settings are configured:

- Profiles

  Defines the conference parameters for the conferences that start from the ad hoc-enabled entry queue.

- Entry queue IVR service with conference ID request enabled

  Use the entry queue service to route participants to their destination conferences. You can also create a new conference with this ID.

  In ad hoc conferencing, use the conference ID to check whether the destination conference is already running on the MCU. If not, use it to start a new conference using this ID.

- Ad hoc-enabled entry queue

Enable ad hoc conferencing in the entry queue and assign a profile to the entry queue. In addition, use an entry queue IVR service supporting conference ID request.

External Database Authentication Settings

Before you can use an external database for ad hoc conferencing, you must define the authentication settings.

Verify that the following settings are configured:

- MCU Configuration:

  System Configuration contains the configuration for the usage of an external database application for authentication for the MCU.

- Entry Queue IVR Service with Conference Initiation Authentication Enabled:

  Set the Entry Queue IVR Service to send authentication requests to the external database application. This verifies the participant's right to start a new conference according to the Conference ID.

- Conference IVR Service with Conference Access Authentication Enabled:

  Set the Conference IVR Service to send authentication requests to the external database application. This verifies the participant's right to connect to the conference as a standard participant or as a chairperson.

- External Database Application Settings

  The external database contains a list of participants (users), with their assigned parameters. These parameters are:

  - Conference Name
  - Conference Billing code
  - Conference Password
  - Chairperson Password
  - Conference Information, such as the contact person name. These fields correspond to Info 1, 2, and 3 fields in the **Conference Properties - Information** dialog box.
  - Maximum number of participants allowed for the conference
  - Conference Owner
  - Participant name (display name)
  - Participant Information, such as the participant email. These fields correspond to Info 1, 2, 3, and 4 fields in the **Participant Properties - Information** dialog box.

Configure External Database Application Communication

You can use an external database application for authentication with ad hoc conferences. The authentication can take place at the entry queue level and the conference level.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. Configure the following flags:

Flag	Description and Value
ENABLE_EXTERNAL_DB_ACCESS	The flag that enables the use of the external database application.
EXTERNAL_DB_IP	The IP address of the external database application server. Default IP: 0.0.0.0.
EXTERNAL_DB_PORT	The port number used by the MCU to access the external application server. Default Port: 80.
EXTERNAL_DB_LOGIN	The user name defined in the external database application for the MCU.
EXTERNAL_DB_PASSWORD	The password associated with the user name defined for the MCU in the external database application.
EXTERNAL_DB_DIRECTORY	The URL of the external database application.

3. Click **OK**.
4. Reset the MCU for the flag changes to take effect.

Enable External Database Validation to Start New Ongoing Conferences

You can validate the participant's right to start a new conference after configuring an external database application in the **Entry Queue IVR Service - Global** dialog.

Procedure

1. Go to **RMX Management** > **IVR Services**.
2. Right-click **Entry Queue IVR Service** and select **Properties**.
3. In the **Global** tab, set the **External Server Authentication** field to **Numeric ID**.
4. Click **OK**.

Enable External Database Validation for Conference Access

You can validate the participant's right to join an ongoing conference with an external database application.

You can set the system to validate all the participants joining the conference or just the chairperson.

Procedure

1. Go to **RMX Management** > **IVR Services**.
2. Right-click **Conference IVR Service** and select **Properties**.
3. In the **Global** tab, set the **External Server Authentication** field to one of the following options:
   - **Always**: Validate the participant's right to join an ongoing conference for all participants.
   - **Upon Request**: Validate the participant's right to join an ongoing conference as chairperson.
4. Click **OK**.

SIP Factories

A SIP factory is a conferencing entity that enables SIP endpoints to create ad hoc conferences.

The system contains a default SIP factory, named **DefaultFactory**.

Note: The default SIP factory uses the conferencing ID `7001`. When using a SIP factory, don't assign this ID to any conferencing entity, including conferences, reservations, and meeting rooms.

When a SIP endpoint calls the SIP factory URI, it creates a new conference with the profile parameters. Then the endpoint joins the conference.

Register the SIP factory URI with the SIP server to enable routing of calls to the SIP factory. To ensure registration of the SIP factory, select the option to register **Factories** in the Default IP Network Service.

Add a SIP Factory

Procedure

1. Go to **RMX Management** > **SIP Factories**.
2. Click **New SIP Factory**.
3. Configure the following settings:

Option	Description
Display Name	The SIP factory name in native language character sets to be displayed in the RMX Manager. The system automatically generates an ASCII name for the **Display Name** field. You can modify it using Unicode encoding. • The maximum field length in ASCII is 80 characters. • The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. If the name is already in use, the RealPresence Collaboration Server displays an error message requesting you to enter a different name.
Routing Name	Enter a name using ASCII text only. If the routing name is blank, the system automatically assigns a new name as follows: • If **Display Name** uses only ASCII text, then the **Routing Name** uses the display name as the routing name. • If **Display Name** is any combination of Unicode and ASCII text (or full Unicode text), the **Routing Name** uses the conference ID as the routing name.
Profile	Select the conference profile from the list of profiles present in the MCU. The MCU creates a new conference using the parameters of the profile.
Automatic Connection	Select this check box to immediately accept the conference creator endpoint to the conference. Clearing the check box redirects the endpoint to the conference and then connects to it.

SIP Registration and Presence for EQs and SIP Factories with SIP Servers

You can register the entry queues and SIP Factories with SIP servers.

This registration enables Office Communication Server or Lync server client users to see the conferencing entities availability status (**Available**, **Offline**, or **Busy**). It also enables the server to connect to them directly from the Buddy List.

Use the following guidelines when registering entry queues and SIP factories with SIP servers:

- Add the entry queue or SIP factory to the Active Directory as a user.
- Enable the SIP registration in the profile assigned to the entry queue or SIP factory.

Monitor Registration Status

You can view the SIP registration status in the **Entry Queue** or **SIP Factory** list sections.

Procedure

1. Do one of the following:
   - Go to **RMX Management** > **Entry Queues**.
   - Go to **RMX Management** > **SIP Factories**.
2. In the **SIP Registration** column, view the following status information:

Status	Description
Not Configured	Disables the registration with the SIP Server in the conference profile assigned to the entry queue or SIP factory. If you set the SIP registration to **Disable** in the conference profile, the RealPresence Collaboration Server registers to SIP servers with a URL derived from its own signaling address. In RealPresence Collaboration Server 2000/4000, this unique URL replaces the non-unique URL, `dummy_tester`, used in previous versions.
Failed	Registration with the SIP server failed. It can be due one of the following reasons: • Incorrect definition of the SIP server in the IP Network Service • The SIP server is down • Other reason that affects the connection between the RealPresence Collaboration Server or the SIP server to the network
Registered	Registers the conferencing entity with the SIP server.
Partially Registered	This status is available only in multiple networks configuration, when the conferencing entity fails to register to all the required network services.

Cascading Conferences

Topics:

Conferences are cascaded when a link is created between two conferences or several conferences (depending on the topology), creating one large conference. The conferences can run on the same MCU or different MCUs.

You can enable cascading only for AVC-based conferences (CP, VSW, or mixed CP/SVC). Cascading conferences don’t support the gathering phase.

Note: RealPresence Collaboration Server (RMX) 1800 with no DSP cards and RealPresence Collaboration Server 1800, Entry Level don’t support cascading conferences.

There are many reasons for cascading conferences. The most common reasons include:

- Connecting two conferences on different MCUs at different sites.
- Using the connection abilities of different MCUs as different communication protocols, such as serial connections or ISDN-video.

Note the following when configuring cascading conferences:

- To properly share content in cascaded conferences, you must predefine dial-in and dial-out link participants with primary/secondary settings in the conferences. (AVC dial-outs only.)
- When cascading between RealPresence Collaboration Server and third-party MCUs, you must define the RealPresence Collaboration Server participant as controller.
- For the best results, use the same software version and license on all MCUs participating the cascading topology.
- Configure the following conference parameters using the same settings on all MCUs participating the cascading topology:
  - Conference line rates
  - Content rate
  - Encryption settings

Cascading Link Properties

Cascading links are the method you use to connect multiple conferences or MCUs into one cascaded conference. You define the cascading link based on the topology of the cascaded conference.

CP conferences treat cascade links as endpoints. The system allocates resources to cascaded conferences as any other endpoint based on the following parameters:

- Default Minimum Threshold Line Rates per Resolution
- Resolution Configuration for CP Conferences

They transmit audio, video, and content between conferences as well as DTMF tones from other endpoints in the conference.

Note: Enabling the **Mute Participants Except Lecturer** option in the conference profile mutes all participants (including the cascading link participants) except the lecturer.

Configure the Cascading Link Video Layout

Set the video layout of the cascading link to 1×1 to ensure the best conferencing experience.

Note: Cascaded links in 1×1 video layout use SD resolution.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. Configure the following flags:

Flag	Description
FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION	Set this flag to `YES` (default) to automatically force the cascading link to full screen (1×1) in CP conferences. Set this flag to `NO` when cascading between a RealPresence Collaboration Server and an MCU/MGC functioning as a gateway, if you don't want to force the participant layouts on the MCU/MGC to 1×1.
AVOID_VIDEO_LOOP_BACK_IN_CASCADE	Set this flag to `YES` (default) to prevent the speaker's image from being sent back through the participant link from the cascaded conference. Video loopback can occur in cascaded conferences with conference layouts other than 1×1. It results in the speaker's own video image being displayed in the speaker's video layout. This option is supported in IP (H.323, SIP) and ISDN-video environments and with basic cascading in CP and VSW conferences. In a primary-secondary MCU conference with two subordinates, the secondary MCU participants don't receive video from each other. **Note:** The video resolution displays according to the resolution configuration or VSW profile.

3. Click **OK**, then click **Close**.

Play a Tone When Establishing a Cascading Link

You can configure the RealPresence Collaboration Server to play a tone in both conferences when a cascading link between the conferences is established.

Note the following:

- You can't customize the tone.
- The tone volume is controlled by the same flag as the IVR messages and tones in **IVR_MESSAGE_VOLUME**.
- The tone doesn't play when the cascading link disconnects from the conferences.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. Select **CASCADE_LINK_PLAY_TONE_ON_CONNECTION** and click **Edit Flag**.
3. Enter `YES` in the **New Value** field and click **OK**.
4. Click **Close**.

Basic Cascading

This topology creates a link between two conferences running on two different MCUs.

Basic cascading uses different locations (states/countries) to install the MCUs to save long-distance charges by connecting each participant to their local MCU. As a result, only the link between the two conferences is billed as long distance call.

- This is the only topology that enables both IP and ISDN-video cascading links.
- This topology supports cascading between RealPresence Collaboration Server, Virtual Edition and RealPresence Collaboration Server (RMX) 1800, 2000, and 4000.
- You can send content over IP and ISDN-video cascading links.
- When linking two conferences using an IP cascading link:
  - Indications for the destination MCU are the IP address and H.323 alias.
  - Both MCUs must be located in the same network.
  - You can use one MCU as a gateway.
- The configuration can include two RealPresence Collaboration Servers or one RealPresence Collaboration Server and one MGC.
- You can define multiple cascade links between MCUs hosting conferences that include ITP rooms.

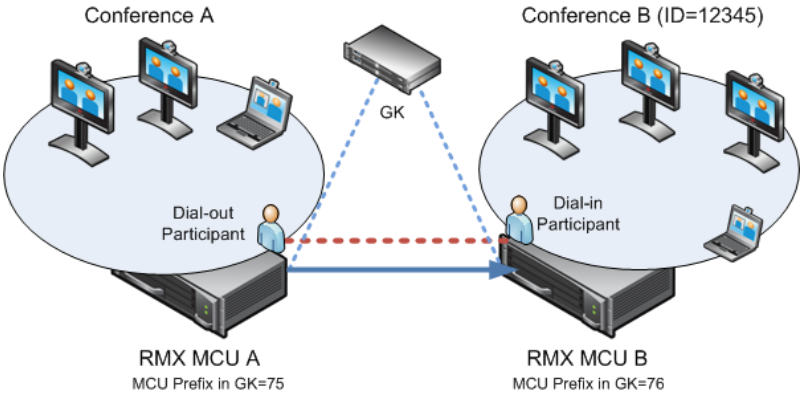
Related Links

Participant Properties on page 160

Basic Cascading Using an IP Cascaded Link

In this topology, you can register both MCUs with the same gatekeeper and use the IP addresses of both MCUs for the cascading link.

Figure 39: Basic Cascading Topology - IP Cascading Link



For example, MCU B is registered with the gatekeeper using 76 as the MCU prefix.

Defining (adding) a dial-out IP participant to conference A creates a connection between the two conferences. The dial-out number of conference A acts as the dial-in number of the conference or entry queue running on MCU B. (AVC dial-outs only.)

Dial In Directly to a Conference

To dial directly in to a conference, participants must enter the dialing string in the proper format.

Procedure

» In conference A, the dial out IP participant dials out to the conference running on MCU B in the following format:

`[MCU B Prefix/IP address][conference B ID]`

For example, if MCU B prefix is 76 and the conference ID is 12345, the dial number is `7612345`.

Dial In to an Entry Queue

To dial in to an entry queue, the participant must enter the dialing string in the proper format.

Procedure

1. The dial out participant dialing in to an entry queue dials the MCU B prefix or IP address of MCU B and the entry queue ID in the following format:

   `[MCU B Prefix/IP address][EQ B ID]`

   For example, if MCU B prefix is 76 and the entry queue ID is 22558, the dial number is `7622558`.
2. When the participant from conference A connects to the entry queue, the system plays to all the participants in Conference A, the IVR message requesting the participant to enter the destination conference ID.
3. Then the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes.

   For example, the meeting organizer enters the destination conference ID `12345`.

4. Any DTMF input from conference A is forwarded to the entry queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.
5. Once the DTMF codes are entered and forwarded to the entry queue on MCU B, the IVR session is completed, the participant moved to the destination conference and the connection between the two conferences is established.

Related Links

Entry Queues on page 210
Cascading via Entry Queue on page 234

Automatic Identification of the IP Cascading Link

When using basic cascading with an IP cascaded link, the system automatically identifies the dial-in participant as an MCU, creates a cascading link, and displays the **Link** icon  for the participant .

MCUs randomly define the primary-secondary relationship during the negotiation process of the connection phase.

DTMF Forwarding in IP Cascaded Calls

When two conferences connect over an IP link, DTMF codes from one conference generally don't forward to the second. An exception is that cascading conferences between a gateway and a conference can forward all DTMF codes from the gateway to the conference and vice versa.

Best practices for DTMF tones in cascaded conferences dictate that you suppress DTMF forwarding to avoid issues. However, if you don't suppress DTMF tones, you can use DTMF tones to execute the following operations throughout the conference. These tones are forwarded to both conferences in a cascaded conference.

- Terminate conference
- Mute all but me
- Unmute all but me
- Secure conference
- Unsecure conference

Note: If you choose to use DTMF tones in your conference, define identical DTMF tones in the IVR services assigned to the cascading conferences.

Basic Cascading Using an ISDN-Video Cascaded Link

To create a cascading conference using ISDN-video, use an ISDN-video connection to link two gateways, an MCU and gateway, or two MCUs.

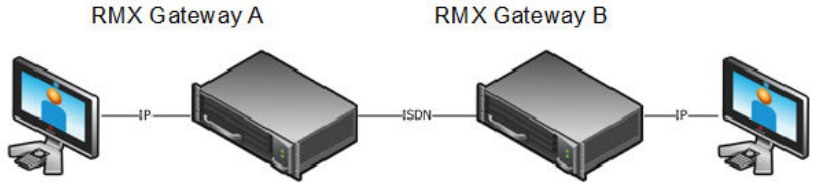
Use the following guidelines when setting up ISDN-video cascaded links.

- Content sharing:
  - The content sharing protocol is H.263 when sent over an ISDN-video cascading link.
  - Endpoints that don't support H.239 can receive content using the **Send Content to Legacy Endpoints** option.
  - The first endpoint must stop sending content before the second endpoint can initiate or send content.
  - Restart content sharing so that a participant joining a conference with active content is able to view it.

- Register cascaded MCUs/gateways with the same gatekeeper or neighboring gatekeepers.
- Register MCUs and endpoints with gatekeepers.
- Gateway/MCU calls require you to define IVR Services.

Gateway to Gateway

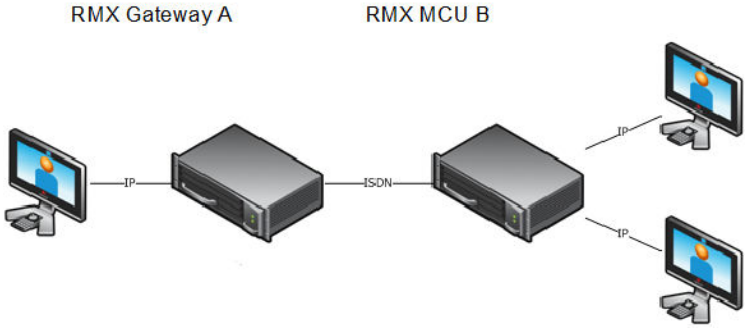
Figure 40: Gateway to Gateway Topology



In this topology, an IP participant calls another IP participant over an ISDN-video link between two gateways.

Gateway to MCU

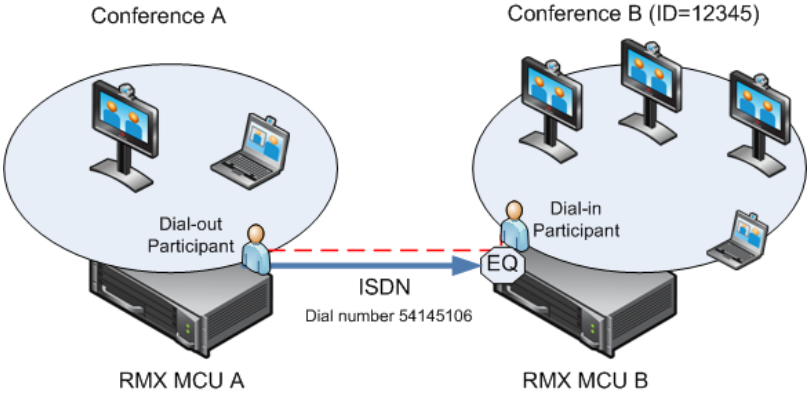
Figure 41: Gateway to MCU / MCU to Gateway Topology



In this topology, an IP participant calls a conference running on an MCU via a gateway.

MCU to MCU

Figure 42: Cascading Between Two MCUs Using an ISDN-Video Link



In this topology, an ISDN-video participant from conference running on MCU A calls a conference running on MCU B over an ISDN-video link.

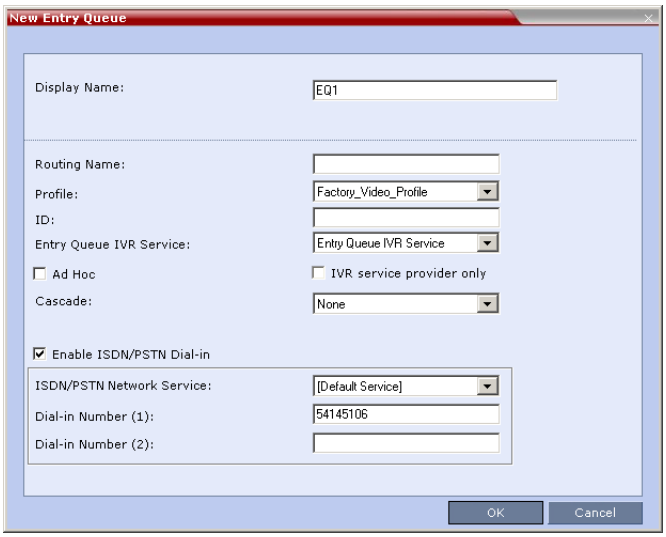
Enable ISDN-Video Cascading Links

ISDN-video connection links between two MCUs or MCU and gateway and creates a cascading conference. Content is sent across the ISDN-video Cascading Link.

To enable Gateway-to-Gateway, Gateway-to-MCU and MCU-to-MCU call over ISDN-video Cascading links, the following configurations are required:

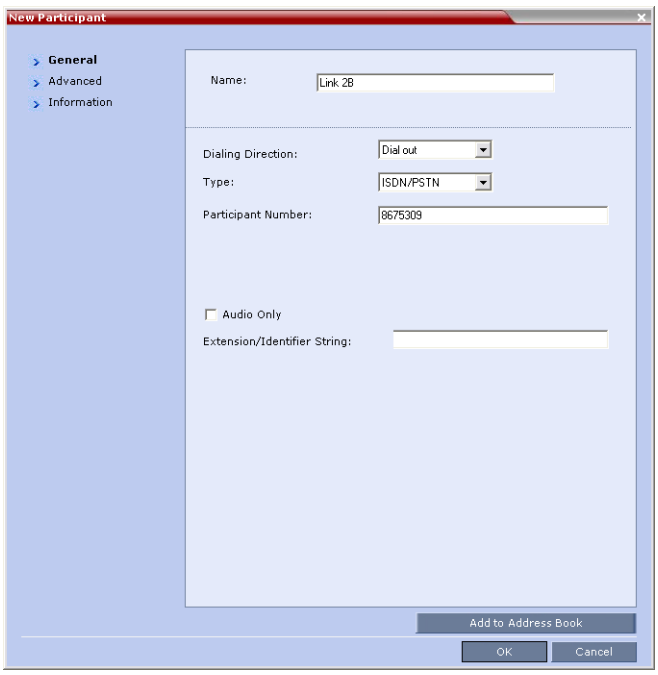
Procedure

1. Modify the IP Network Service to include the MCU Prefix in the Gatekeeper (in the Gatekeepers dialog box).
2. Configure the ISDN-video Network Service in both MCUs.
3. Configure a Gateway Profile and assign dial-in ISDN (audio/video) numbers.
4. Configure the Entry Queue or conference (for direct dial-in) as enabled for ISDN-video connection. This assigns a dial-in number (for example 54145106).



5. Define the dial-in ISDN-video participant in MCU B and Dial-out ISDN-video participant in MCU A (for MCU-to-MCU cascading conferences). (AVC dial-outs only.)

   A dial out ISDN-video participant is defined (added) to conference A. The participant's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).



MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

DTMF Forwarding in ISDN-Video Cascaded Calls

Forwarding of the DTMF codes from one conference to another over an ISDN-video cascading link isn't automatically suppressed.

DTMF tones are limited to basic operations while suppressing all other operations by the system flag **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS**.

Once the timer expires, instead of forwarding of most of the DTMF codes (excluding five operations as for IP links) in conference A to conference B, they're applied within the MCU receiving the DTMF code. This prevents application of an operation requested by a participant individually (for example, mute my line) to all the participants in conference B.

This flag is defined on MCU A (the calling MCU).

Note: If you choose to use DTMF tones in your conference, define identical DTMF tones in the IVR services assigned to the cascading conferences.

Recommended Conference Profile Options

The following table lists the recommended meeting room/conference profile parameters setting when routing ISDN-video cascaded calls.

Recommended Conference Profile Options Setting

Line Rate	Motion	Sharpness	Encryption	Polycom Lost Packet Recovery (LPR)
128	Yes			
128		Yes		
128	Yes			Yes
128	Yes		Yes	Yes
256	Yes			
256		Yes		
256	Yes			Yes
256	Yes		Yes	Yes
384	Yes			
384		Yes		
384	Yes			Yes
384	Yes		Yes	Yes
512	Yes			
512		Yes		
512	Yes			Yes
512	Yes		Yes	Yes
768	Yes			
768		Yes		
768	Yes			Yes
768	Yes		Yes	Yes

Note: Since the remote participant settings are unknown, configure the gateway or endpoint to support a higher line rate (for example, 768 Kbps). This allows flexibility during endpoint capability negotiations.

Star Cascading Topology

In the star cascading topology, the MCUs are usually present at different locations (states or countries). Participants connect to their local MCU, which helps save long distance call costs.

Star cascading requires that all cascaded MCUs reside on the same network.

Note: Although participants in star cascading conferences can connect to their local conference using IP (H.323, SIP, and ISDN-video), the cascading links between conferences must connect via H.323.

In this topology, use the following two modes to network the MCUs:

- primary-secondary cascading
- Cascading via entry queue

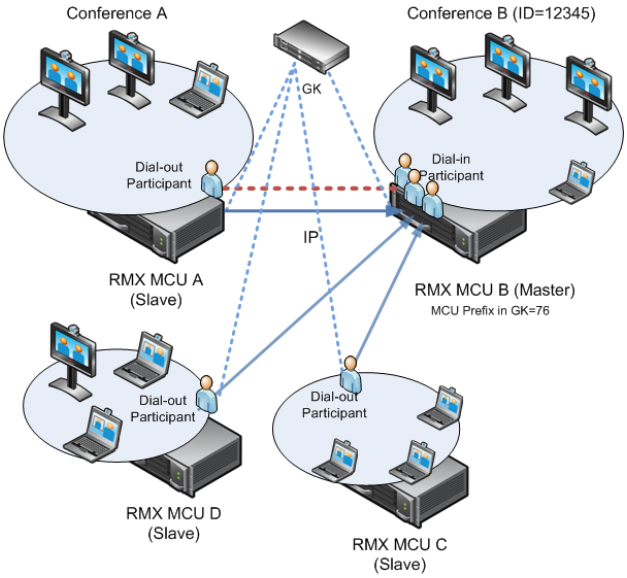
Primary-Secondary Cascading

Primary-secondary cascading contains only two levels: one primary MCU on level 1 and several secondary MCUs on level 2.

Use following guidelines to configure primary-secondary cascading:

- If level 1 contains a RealPresence Collaboration Server:
  - Use RealPresence Collaboration Server on level 2.
  - Use an MGC with version 9.0.4 on level 2 if level 1 contains RealPresence Collaboration Server version 7.0.2 and higher.
- If level 1 contains an MGC:
  - Use an MGC or RealPresence Collaboration Server on level 2.

Figure 43: Primary-Secondary Star Cascading Topology



- When creating a cascading link between two RealPresence Collaboration Servers, the RealPresence Collaboration Servers operate in CP mode.

- When creating a cascading link between MGCs and RealPresence Collaboration Servers, the MGCs can only operate in VSW mode.

Creating Star Cascading Conferences with Two RealPresence Collaboration Servers

You can create star cascading conferences with two RealPresence Collaboration Servers by making one a primary MCU and the other a secondary MCU.

To establish the links between two RealPresence Collaboration Servers, you must do the following:

- Establish the primary-secondary relationships between the cascaded conferences by defining the dialing direction.
- Create the primary and secondary conferences, defining the appropriate line rate.
- Create a cascade-enabled Dial-out Participant link in the primary conference. (AVC dial-outs only.)
- Create a cascade-enabled Dial-in Participant link in the secondary conference.

Video Session Mode and Line Rates

The following table summarizes video session mode line rate options available for each conference in the cascading hierarchy.

Video Session Mode and Line Rate

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	RealPresence Collaboration Server	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	HDX
Level 2	RealPresence Collaboration Server	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	
Level 1	RealPresence Collaboration Server	CP - CIF	768Kb/s, 2Mb/s	VSX
Level 2	RealPresence Collaboration Server	CP - CIF	768Kb/s, 2Mb/s	
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s	HDX, VSX
Level 2	RealPresence Collaboration Server	CP - CIF 264	768Kb/s, 2Mb/s	
Level 1	MGC	VSW - HD	1.5Mb/s	HDX
Level 2	RealPresence Collaboration Server	VSW - HD	1.5Mb/s	

Set RealPresence Collaboration Server as Controller in Codian MCU Cascading Conferences

You can set RealPresence Collaboration Server as controller at all times in cascading conferences between RealPresence Collaboration Server and a Codian MCU.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. Select **ENABLE_CODIAN_CASCADE** and click **Edit Flag**.
3. Enter `YES` in the **New Value** field and click **OK**.
4. Click **Close**.

Cascade-Enabled Participant Links

The connection between two cascaded conferences is established by a cascade enabled dial-out and dial-in participants, acting as a cascades link. (AVC dial-outs only.)

The dialing direction determines whether the dial-out participant is defined in the conference running on the controller MCU or the secondary MCU. For example, if the dialing direction is from the primary conference on level 1 to the secondary conference on level 2, the dial-out participant is defined in the primary conference on level 1 and a dial-in participant is defined in the secondary conference running on the MCU on level 2.

If the cascade-enabled dial-out participant always connects to the same destination conference on the other (second) MCU, the participant properties can be saved in the address book of the MCU for future repeated use of the cascaded link.

Related Links

Participant Properties on page 160

Define a Cascade-Enabled Dial-Out Participant Link

Create a dial-out cascade link to use for primary-secondary cascading.

Procedure

1. In RMX Manager, go to the **Conferences** pane and select the conference.
2. In the **Participants** pane, click **New Participant** .
3. In the **General** tab, configure the following settings:

Field	Description
Name	Enter the participant's name. Note the following: • You can't leave this field blank. • You can't use a duplicate participant name. • You can't use a comma or semicolon in this field.
Dialing Direction	Select **Dial-out**.
Type	Select **H.323**.

Field	Description
IP Address	Enter the IP address of the signaling host of the MCU running the other (second) conference, where the cascade-enabled entry queue is defined.
Alias Name	If you're using the target MCU IP address, enter the conference ID of the target conference. For example: `24006`. If you're using a gatekeeper, instead of the IP address you can enter the prefix of the target MCU (as registered with the gatekeeper) as part of the dialing string and the conference ID in the format `<Target MCU Prefix><Conference_ID>`. For example: `92524006`. If the conference has a password and you want to include the password in the dial string, append the password to in the dial string after the conference ID. For example: `92524006##1234`. If the conference has a password and you don't want to include the password in the dial string, set the `ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD` flag to `YES`.
Alias Type	Select **E.164** (digits 0–9, *, #).

4. In the **Advanced** tab, choose one of the following options for **Cascade**:
   - **Primary**: The defined participant is in a conference running on a subordinate MCU.
   - **Secondary**: The defined participant is in a conference running on the master MCU.
5. Click **OK**.

Define a Cascade-Enabled Dial-In Participant Link

Create a dial-in cascade link to use for primary-secondary cascading.

Procedure

1. In RMX Manager, go to the **Conferences** pane and select the conference.
2. In the **Participants** pane, click **New Participant** .
3. In the **General** tab, configure the following settings:

Field	Description
Name	Enter the participant's name. Note the following: • You can't leave this field blank. • You can't use a duplicate participant name. • You can't use a comma or semicolon in this field.
Dialing Direction	Select **Dial-in**.
Type	Select **H.323**.
IP Address	If you use a gatekeeper: Leave this field empty. If you don't use a gatekeeper: Enter the IP address of the signaling host of the MCU running the other conference.
Alias Name	If you use a gatekeeper: Enter the name of the other (second) conference. If you don't use a gatekeeper: Enter the ID of the MCU running the other (second) conference.
Alias Type	If you use a gatekeeper: Select **H.323 ID**. If you don't use a gatekeeper: Select **E.164** (digits 0–9, *, #).

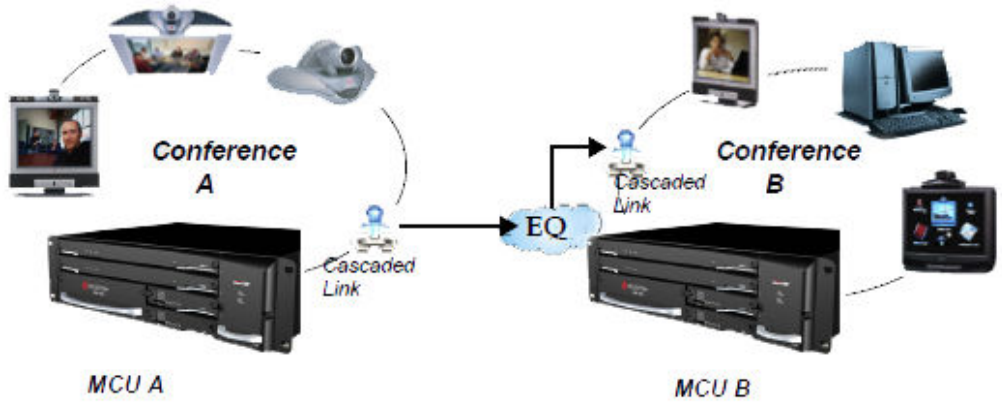
4. In the **Advanced** tab, choose one of the following options for **Cascade**:
   - **Primary**: The defined participant is in a conference running on a subordinate MCU.
   - **Secondary**: The defined participant is in a conference running on the master MCU.
5. Click **OK**.

Cascading via Entry Queue

Defining a participant as a dial-out cascaded link in one conference and connecting it to a second conference via a special cascaded entry queue (EQ) creates a link between them.

When MCU A dials out to the cascaded link to connect it to conference A, it actually dials out to the cascaded entry queue defined on MCU B.

Figure 44: Cascaded Conferences - Star Topology



The process of cascading conferences mentioned here refers to conferences running on two different RealPresence Collaboration Server units. But it's possible to cascade conferences running between RealPresence Collaboration Server units and other MCUs.

The cascaded link dosen't support the following features and therefore they aren't supported in the combined conference:

- DTMF codes are enabled in cascaded conference, but only in their local conference. The operations executed via DTMF codes aren't forwarded between linked conferences.
- FECC (Far End Camera Control) only applies to conferences running in their local MCU.

Related Links

Dial In to an Entry Queue on page 224
Create an Entry Queue IVR Service for Operator Conferences on page 198

Enable Entry Queue Cascading

Cascading enables administrators to connect one conference directly to one or several conferences, depending on the topology, creating one large conference.

Procedure

1. Create the cascade-enabled entry queue.

   This is a cascade-enabled entry queue in the MCU hosting the destination conference (Conference B). The cascade-enabled entry queue is used to establish the dial-in link between the destination conference and the linked conference and bypassing standard entry queue, IVR prompt, and video slide display.
2. Create a cascade-enabled dial-out link.

   This is a cascade-enabled dial-out link (participant) in the linked conference (Conference A). This dial-out participant functions as the link between the two conferences.
3. Optional: Enable the cascaded linked participant to connect to the linked conference (Conference A) without entering the conference password. You can do this by modifying the default settings of the relevant system flag.

Define the Entry Queue Dial-Out Cascaded Link

Create or add the dial-out link (to a participant) in the linked conference (Conference A).

To connect to a conference entry queue (Conference B), use a dial-out string. The MCU hosting the destination cascade conference contains this entry queue. (AVC dial-outs only.)

Once you add the participant to the Address Book, you can add the participant to the conference whenever you use the same cascade-enabled entry queue and a destination conference (with the same ID and password).

There are two options to define the dialing string: using the MCU's IP address and the alias string or using the alias string only.

Procedure

1. In RMX Manager, click **Address Book**.
2. Right-click the group to which to add the participant and select **New Participant**.
3. In the **General** tab, configure the following settings:

   In method A, no gatekeeper is used.

   Method A - MCU IP Address and Alias String

Field	Description
IP Address	Enter the IP address of the signaling host of the MCU hosting the destination conference (MCU B).
Alias Name/Type	Enter the ID of the cascade-enabled entry queue, the conference ID, and the password of the destination conference (MCU B) in the following format: `<EQ ID>#<Destination Conference ID>#<Password>` (password is optional). For example, `78485#24006#1234`, where • `78485` is the cascade-enabled EQ ID • `24006` is the destination conference ID • `1234` is the password (optional)

   In method B, a gatekeeper is used.

Method B - Alias String Only

Field	Description
Alias Name	Enter the prefix of MCU B, the ID of the cascade-enabled entry queue, the destination conference ID, and the password of the destination conference in the following format: `<MCU Prefix EQ ID>#<Conference ID>#<Password>` (password is optional). For example, `92578485#24006#1234`, where • `925` is the MCU prefix as registered in the gatekeeper • `78485` is the cascade-enabled EQ ID • `24006` is the destination conference ID • `1234` is the password (optional)

4. In the **Advanced** tab, choose one of the following options for **Cascade**:
   - **Primary**: The defined participant is in a conference running on a subordinate MCU.
   - **Secondary**: The defined participant is in a conference running on the master MCU.
5. Click **OK**.

Monitor Star Cascaded Conferences

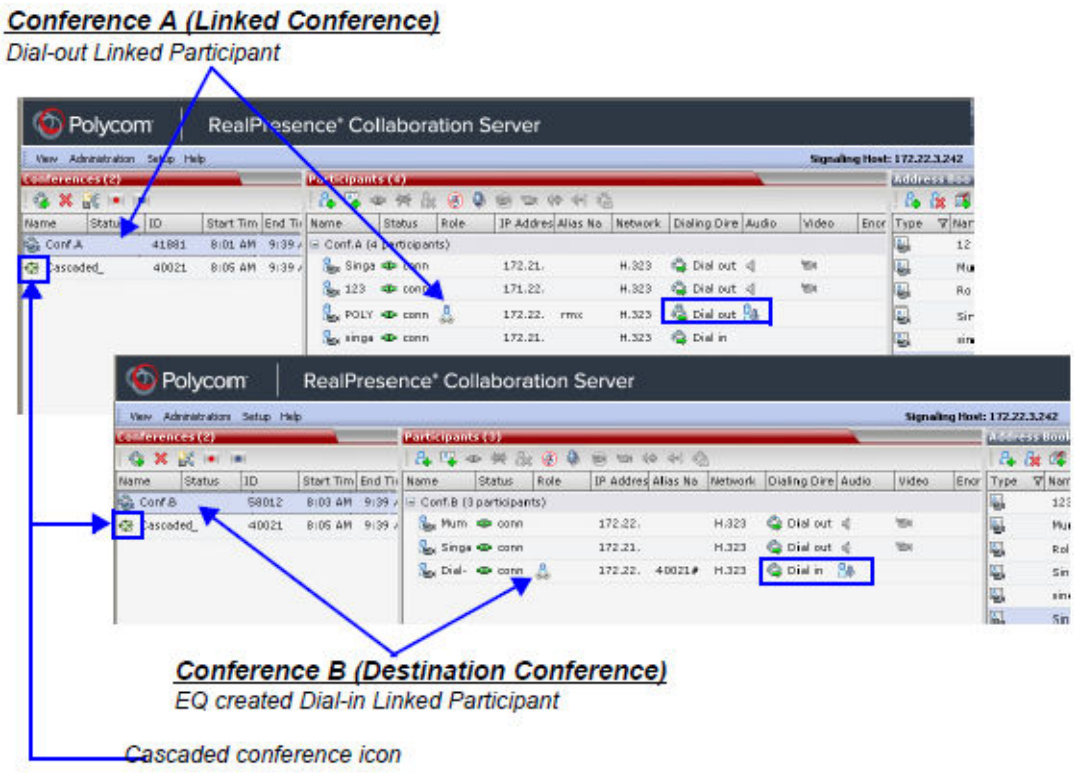
To monitor both conferences at the same time, you must open two instances of the RMX Web Client (one for each MCU) by entering the IP address of each MCU into a web browser.

If both conferences are running on the same MCU, you need to open only one RMX Web Client window.

Procedure

» When conferences are cascaded, the **Participant List** pane of each of the two conferences displays the **Link** icon  ; a dial-in linked icon in the destination conference (Conference B) and a dial-out linked icon in the linked conference (Conference A).

The **Conferences List** panes in each of the two conferences display a **Cascaded Conference** icon  , indicating that a conference running on the MCU is presently cascading with another conference running on the same or another MCU. The cascaded conference icon displays for a short time.



H.239-Enabled MIH Topology

Using a H.323 connection, H.239 Multi-Hierarchy (MIH) cascading enables the RealPresence Collaboration Server users to run very large conferences on different MCUs in multiple levels of primary-secondary relationships. The MCUs can reside on different networks.

Note: You can only deploy the MIH cascading topology RealPresence Collaboration Server appliance editions (1800, 2000, or 4000).

MIH cascading enables the following:

- Opening and using a content channel (H.239) during conferences
- Full management of extremely large, distributed conferences
- Connecting conferences on different MCUs at different sites
- Using the connection abilities of different MCUs, for example, using different communication protocols such as serial connections and ISDN-video
- Saving significant call costs by having participants call local MCUs which in turn call remote MCUs long distance

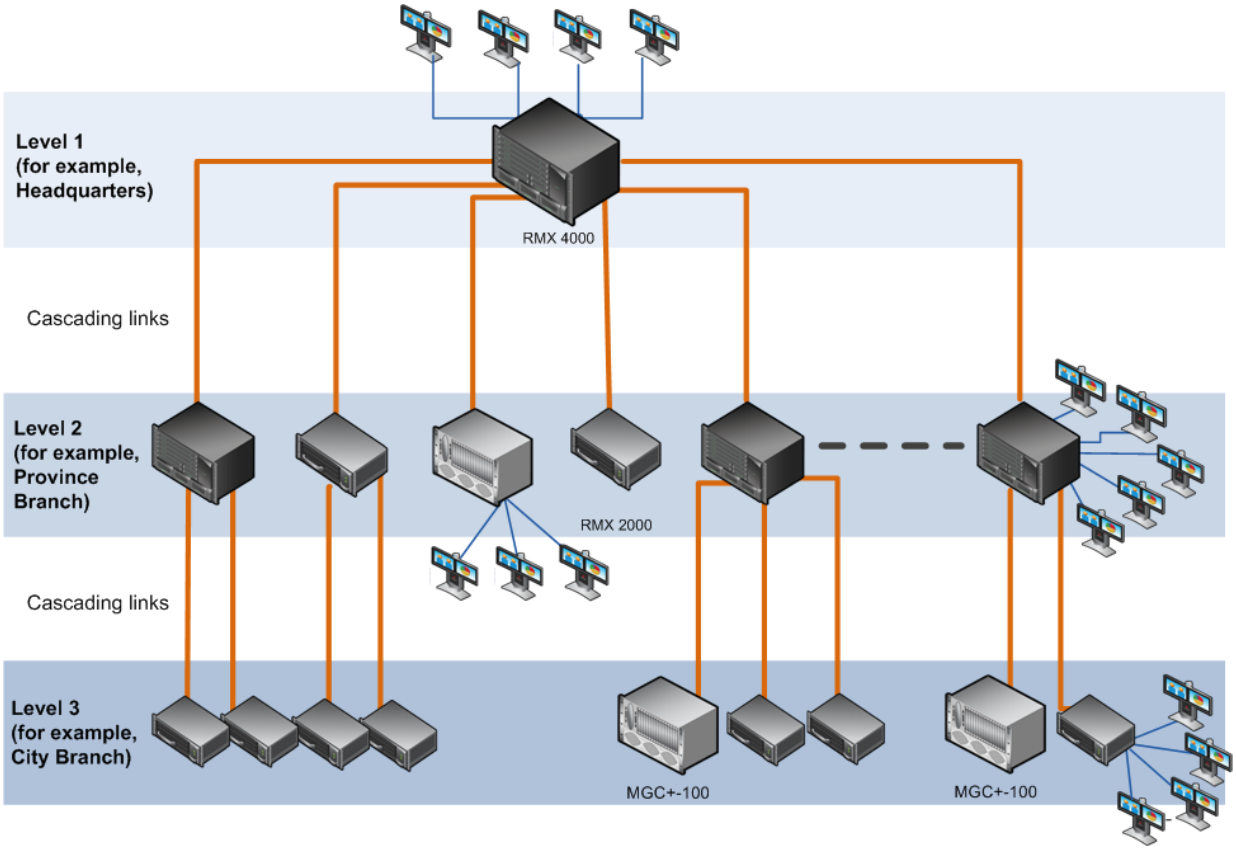
---

Note: Although participants in MIH cascading conferences can connect using IP (H.323, SIP) and ISDN-video, the MIH cascading links must connect via H.323.

MIH Cascading Levels

The cascading hierarchy topology can extend to up to four levels, where the most common configuration includes up to three levels.

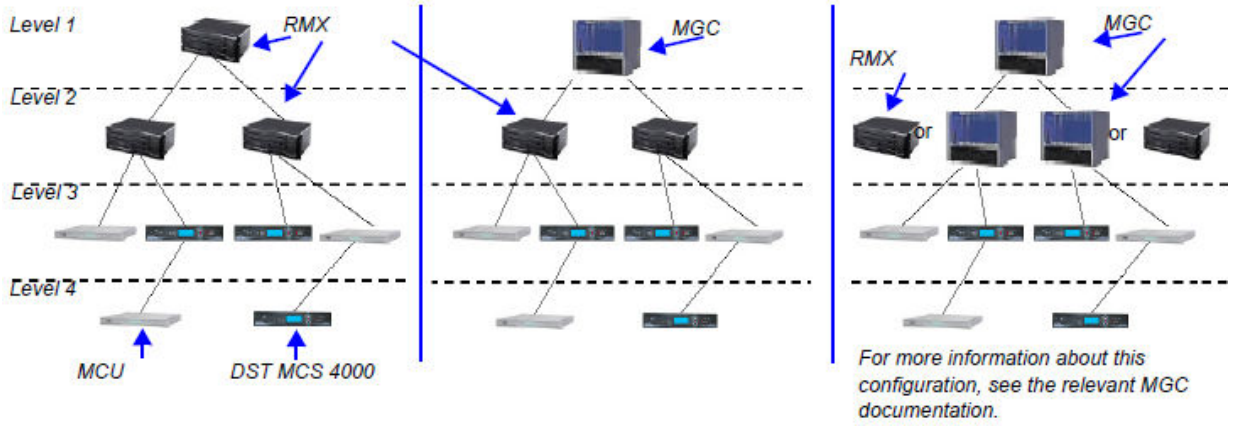
Figure 45: MIH Cascade - a Sample 3-Level Cascading Configuration



Deploy the cascading hierarchy topology according to the following guidelines:

- If level 1 contains an RealPresence Collaboration Server (RMX) (recommended deployment):
  - Level 2, level 3, and level 4 can contain any RealPresence Collaboration Server (RMX) (recommended deployment).
  - Level 2 and level 3 can contain MGC version 9.0.4.
  - Level 3 and level 4 can contain DST MCS 4000 and other MCUs.
- If level 1 contains an MGC:
  - Level 2 can contain MGC or RealPresence Collaboration Server (RMX).
  - Level 3 and level 4 can contain DST MCS 4000 and other MCUs.
- DST MCS 4000 MCUs connect as endpoints to the RealPresence Collaboration Server (RMXs) or MGCs on higher levels.

Figure 46: MIH Cascade Levels



Primary - Secondary Conferences

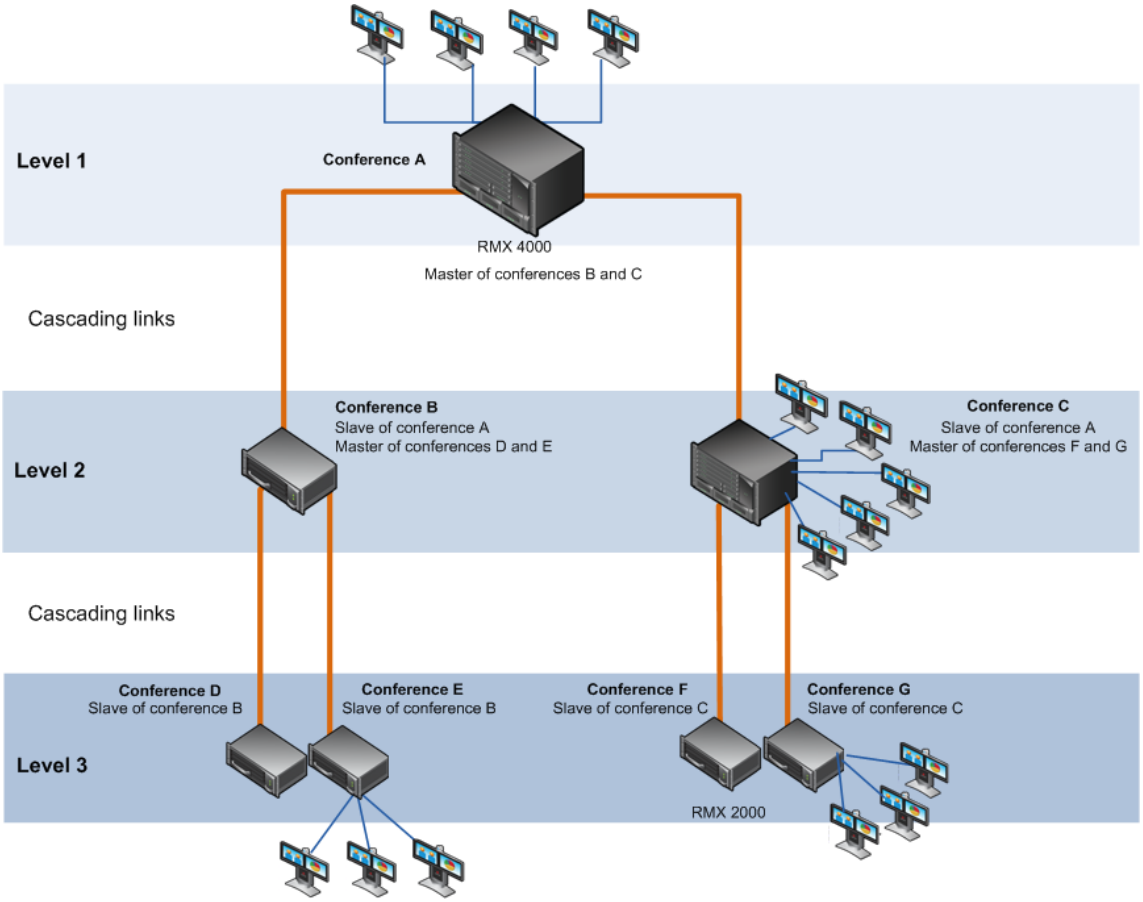
In MIH cascading conferences, there are multiple levels of primary and secondary relationships between conferences.

Note: Polycom recommends that you have RealPresence Collaboration Servers at all levels to use the high-quality video and content offered by the RealPresence Collaboration Server (RMX).

Use the following guidelines when configuring MIH cascading primary-secondary conferencing:

- The conference running on the MCU on level 1 of the hierarchy must be the primary for the entire cascading session. If you have an MGC running version 9.0.4, you can configure it for any level of the cascading topology. For an MGC running any other version, you must set the MGC as the level 1 MCU.
- Conferences running on MCUs on levels 2 and 3 and can be both primaries and secondaries to conferences running on MCUs on levels above and below them.
- All conferences running on MCUs on the lowest level in the configuration (for example, level 3 in a three-level hierarchy configuration) are secondary conferences.
- When the DST MCS 4000 is on level 3 and acting as secondary to level 2, the RealPresence Collaboration Server (RMX) on level 2 must dial out to it. This identifies the DST MCS 4000 as secondary. The link between the two MCUs (dial-out participant) is defined as a standard participant and not as a cascading link.

Figure 47: MIH Cascading - Primary-Secondary Relationship



Video Session Mode, Line Rate, and Video Settings

The types of MCUs, their position in the cascade topology, and the endpoint capabilities (HD/CIF and H.263/H.264) determine the video session type of the MIH cascading conference.

- When creating a cascading link between two RealPresence Collaboration Servers:
  - The RealPresence Collaboration Servers operate in CP mode.
  - Define the DTMF codes with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between MGCs and RealPresence Collaboration Servers:
  - If there are no MGCs on level 2, the MGCs can operate in either in CP or VSW mode.
  - If there are MGCs on level 2, the MGCs can only operate in VSW mode.
  - MGC doesn't support H.264 High Profile, therefore when MGC is part of the cascading topology, don’t select **High Profile** on the RealPresence Collaboration Server.
  - Define the DTMF codes with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between two MGCs, configure the MGCs to operate in VSW mode.
- To enable the connection of the links between cascaded conferences, use the same line rate for both.

- To enable content sharing between the RealPresence Collaboration Server and the MGC, the rate allocated to the content must be identical in both conferences. Correctly select the line rate for both conferences and the content settings (**Graphics**, **Hi-resolution Graphics** or **Live video**) to ensure the compatible rate allocation.

The following table summarizes the video session modes line rate options for each conference in the cascading hierarchy:

MIH Cascading - Video Session Mode and Line Rate

Topology	MCU Type	Video Session Type	Line Rate
Level 1	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 2	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 1	RMX	CP - CIF	768Kb/s, 2Mb/s
Level 2	RMX	CP - CIF	768Kb/s, 2Mb/s
Level 1	RMX	CP	768Kb/s, 2Mb/s
Level 2	MGC	CP or VSW	768Kb/s, 2Mb/s
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s
Level 2	RMX	CP - CIF 264	768Kb/s, 2Mb/s
Level 1	MGC	VSW - HD	1.5Mb/s
Level 2	RMX	VSW HD	1.5Mb/s
Level 2	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 2	MGC	VSW*	384 kbps, 768 kbps
Level 3	MGC	VSW*	384 kbps, 768 kbps
Level 2	RMX	CP/VSW - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	MCS 4000	CP/VSW - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 2	RMX	CP - CIF	768kb/s, 2Mb/s
Level 3	MCS 4000	CP - CIF	768kb/s, 2Mb/s

* When MGC is on Level 3, Content cannot be shared between Level 2 and Level 3.

MGC to RealPresence Collaboration Server Cascading

Use the following guidelines when setting up cascading conferences between MGC and RealPresence Collaboration Server.

If an MGC is running version 9.0.4, and RealPresence Collaboration Server is running version 7.0.2 and higher, set the RealPresence Collaboration Server as primary on level 1 and the MGC as secondary on level 2.

MGCs running versions other than 9.0.4 must always be on level 1 and set as the primary MCU.

If the cascading topology includes additional MGCs as well as RealPresence Collaboration Servers, define video switching conferences for all the cascading conferences running on the MGC in the topology.

You can use two methods to create the cascading links between conferences running on the RealPresence Collaboration Server and MGC:

- Method I - Establish the links by defining a dial-in and a dial-out participant in the secondary and primary conference, where the primary conference is created on the MCU on Level 1 and the secondary conference is created on the MCU on Level 2. (AVC dial-outs only.)
- Method II - Use a cascading entry queue on either the MGC or the RealPresence Collaboration Server, depending on the dialing direction and the MCU level. Polycom recommends this method when the RealPresence Collaboration Server is on Level 1.

Create Cascading Links Using Dial-In and Dial-Out - MGC to RealPresence Collaboration Server

Create cascading links by defining dial-in and dial-out participants from the MGC to the RealPresence Collaboration Server.

Procedure

1. Configure the following settings for the level 1 RealPresence Collaboration Server:
    a. Set the appropriate flags (done once only).
    b. Define the conference setting and its line rate to be the same as the one set on the RealPresence Collaboration Server.
    c. Define the dial-in participant (Cascaded Link) with the calling number from the MGC.

       The alias that is used to identify the dial-in participant can be the name of the calling secondary conference.
    d. Set the **Cascading** option to **Primary**.
2. Configure the following settings for the level 2 MCG:
    a. Set the appropriate flags (done once only).
    b. Define the conference setting and its line rate to be the same as the one set on the MCG.
    c. Define the dial-out participant (cascaded link) to the conference running on the RealPresence Collaboration Server. Set the dial-out alias to be the prefix of the MCU and the name of the primary conference running on the RealPresence Collaboration Server.

Create Cascading Links Using Dial-In and Dial-Out - RealPresence Collaboration Server to MCG

Create cascading links by defining dial-in and dial-out participants from the RealPresence Collaboration Server to the MCG.

Procedure

1. Configure the following settings for the level 1 RealPresence Collaboration Server:
   a. Set the appropriate flags (done once only).
   b. Define the conference setting and its line rate to be the same as the one set on the RealPresence Collaboration Server.
   c. Define the dial-out participant (cascaded link) with the calling number from the MGC. Set the dial-out alias to be the prefix of the MGC and the name of the secondary conference running on the MGC.
   d. Set the **Cascading** option to **Primary**.
2. Configure the following settings for the level 2 MCG:
   a. Set the appropriate flags (done once only).
   b. Define the conference setting and its line rate to be the same as the one set on the MCG.
   c. Define the dial-in participant (cascaded link) to the conference running on the RealPresence Collaboration Server.

      The alias that is used to identify the dial-in participant can be the name of the calling secondary conference.

Note: To enable content sharing between the RealPresence Collaboration Server and the MGC, the rate allocated to the content must be identical in both conferences. Correctly select the line rate for both conferences and the content settings (**Graphics**, **Hi-resolution Graphics** or **Live video**) to ensure the compatible rate allocation.

Create Cascading Links Using a Cascading EQ - MGC to RealPresence Collaboration Server

Create cascading links by defining a cascading entry queue from the MGC to the RealPresence Collaboration Server.

Procedure

1. Configure the following settings for the level 1 MCG:
   a. Set the appropriate flags (done once only).
   b. Define the conference setting and its line rate to be the same as the one set on the RealPresence Collaboration Server.
   c. Define the dial-out participant (cascaded link) to the conference running on the RealPresence Collaboration Server.
2. Configure the following settings for the level 2 RealPresence Collaboration Server:
   a. Set the appropriate flags (done once only).
   b. Define the cascade-enabled entry queue, setting it to **Slave**.

c. Define the conference setting and its line rate to be the same as the one set on the MGC.

Create Cascading Links Using a Cascading EQ - RealPresence Collaboration Server to MCG

Create cascading links by defining a cascading entry queue from the RealPresence Collaboration Server to the MCG.

Procedure

1. Configure the following settings for the level 1 MCG:
   a. Set the appropriate flags (done once only).
   b. Define the cascade-enabled entry queue.
   c. Define the conference setting and its line rate to be the same as the one set on the RealPresence Collaboration Server.
2. Configure the following settings for the level 2 RealPresence Collaboration Server:
   a. Set the appropriate flags (done once only).
   b. Define the conference setting and its line rate to be the same as the one set on the MCG.
   c. Define the dial-out participant (cascaded link) to the conference running on the MGC, setting the participant cascade parameter to **Slave**.

SVC Cascading with Poly Clariti Relay

Polycom RealPresence Collaboration Server (RMX) supports SVC cascading between RealPresence Collaboration Server and a Poly Clariti Relay server.

SVC cascading is only available for continuous presence (CP) mode.

Enable SVC Cascading with Poly Media Relay

Configure Poly Clariti Core to enable SVC cascading between RealPresence Collaboration Server (RMX) and a Poly Media Relay server using Poly Clariti Core.

For more details, refer to https://docs.poly.com/bundle/cce-ag-10-2/page/t-dma-ops-add-a-standalone-conference-template.html.

Procedure

» In Poly Clariti Core, set the conference mode to **AVC, SIP MRC and Poly SVC**.

Multistream for SVC Cascading with Poly Clariti Relay

Polycom RealPresence Collaboration Server (RMX) supports multiple SVC video streams over an SVC-cascaded link from the Poly Clariti server with one or more participants.

You can either enable or disable content transcoding for content sharing between the Poly Clariti Relay server and RealPresence Collaboration Server. When content transcoding is enabled, RealPresence Collaboration Server allocates two additional ports that remain occupied till the conference ends, even if content sharing stops earlier or the SVC cascading link disconnects. Disabling the content transcoding frees port resources on RealPresence Collaboration Server and allows more AVC endpoints for connection. However, in this case only AVC endpoints with H.264 High Profile can receive content.

Note the following limitations:

- The maximum number of video streams from Poly Clarity Relay server is predefined to 5.
- SVC-cascaded primary party can't mute/unmute audio or video from EMA.
- SVC-cascaded secondary parties are decoder-only and don't support EMA controls.

Port Utilization by Bandwidth Speed for SVC-Cascaded Links with Multiple Content Resolutions

System	1920 Kbps or Higher	Between 1920 Kbps and 768 Kbps	Below 768 Kbps
RealPresence Collaboration Server, Virtual Edition	6 *6.5 with 1080p content	5 *5.5 with 1080p content	4.5
RMX 1800	5 *6.5 with 1080p content	4 *5.5 with 1080p content	3.5
RMX 2000/4000	5 *6.5 with 1080p content	4 *5.5 with 1080p content	3.5

*1080p content is only available with bandwidth higher than 1024 Kbps.

Port Utilization by Bandwidth Speed for SVC-Cascaded Links without Multiple Content Resolutions

System	1920 Kbps or Higher	Between 1920 Kbps and 768 Kbps	Below 768 Kbps
RealPresence Collaboration Server, Virtual Edition	3.5	2.5	2
RMX 1800	3.5	2.5	2
RMX 2000/4000	3.5	2.5	2

Gateway Calls

Topics:

The RealPresence Collaboration Server allows sites with different frame rates, connection speeds, audio algorithms, video resolutions, and network protocols to transparently connect with one another. It also enables multi-point conference creation from an endpoint.

A special conference acting as a Gateway Session is created on the RealPresence Collaboration Server. It includes one dial-in connection of the endpoint initiating the Gateway Session and one or several dial-out connections to endpoints. It provides connectivity between the various protocols: H.323, SIP, ISDN-video, and ISDN-voice.

Note:
- Gateways are not supported by Polycom RealPresence Collaboration Servers Virtual Edition or 1800 with no DSP cards.
- Gateway calls are supported with AVC conferencing only.

Gateway Functionality

A special Gateway Profile is defined on the RealPresence Collaboration Server to enable the gateway functionality.

The following features and capabilities are supported in gateway calls:

- Gateway Sessions are in CP Mode only.

  If Video Switching is selected in the Profile assigned to the Gateway Session, the system ignores this setting and runs the Gateway Session in CP mode.

  Gathering phase is not supported in gateway calls, even if it is defined in the Profile assigned to the Gateway Profile.
- Sharing Content using H.239 protocol
- FECC.

  Note: Only IP participants can use FECC as it is not supported by the ISDN-video protocol.
- Recording.

Note: The Recording Link is not considered as a participant and therefore, the gateway session automatically ends when only one of the participants remains connected in addition to the recording link. The video of the Recording Link is not included in the display of the video of the gateway call.

- Forwarding of DTMF codes from the Gateway Session to a conference running on another gateway, MCU or Poly Clariti Edge. This enables the participant to enter the required conference or chairperson password when connecting to another conference.

  DTMF forwarding is enabled when there are only two participants connected to the Gateway Session.
- Forwarding of all DTMF codes sent by participants in the Gateway Session to all ISDN-voice and ISDN-video participants. This is enabled by adding the **ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN** System Flag to `system.cfg` and setting its value to `YES`.
- Up to 80 gateway calls may be run on a fully configured MCU.
- Gateway Profiles are included in the **Backup** and **Restore Configuration** operations.
- CDR files are generated for Gateway Sessions in the same way as for conferences.
- **Cascading** - To support cascading, the gateway indicates a lower number than the MCU for primary-secondary relation (directly or through Poly Clariti Core).

  A participant, wishing to join the conference as a chairperson, is required to connect using the chairperson password.
- Gateway calls are supported in Microsoft and Avaya environments.
- If the **ENABLE_AUTO_EXTENSION** system flag is set to:
  - **YES** (default), Gateway Calls are not limited in duration while endpoints are connected.
  - **NO**, Gateway Calls are limited to 60 minutes.

Configuring the Gateway Components on the RealPresence Collaboration Server

Configuring the components to enable Gateway Calls in the RealPresence Collaboration Server.

- Conference IVR Service to be used with the Conference Profile assigned to the Gateway Profile. The IVR Services are used for Gateway IVR connections.
- Conference Profile that includes the IVR Service for the Gateway Session and the settings to automatically terminate the Gateway Session when one participant is still connected or when no participants are connected.
- Gateway Profile for call routing.

Define Conference IVR Service for Gateway Calls

The system is shipped with a default Conference IVR Services for gateway calls named GW IVR Service that enables you to run gateway calls without defining a new Conference IVR Service.

This IVR Service includes the following settings:

- **Welcome slide** and **message** - disabled
- **Conference** and **Chairperson Passwords** - disabled

- **General Messages** - all messages including the gateway messages and dial tones are selected
- **Roll Call** - disabled
- **Video Services** - Click&View - enabled
- **Video Services** - Video Welcome Slide - Default_GW_Welcom_Slide
- **Operator Assistance** - disabled

Note: For gateway redial, ensure that the audio files for the gateway redial messages have been assigned.

Procedure

1. Select  to display the Conference IVR Services list in the **RMX Management - Rarely Used** pane.
2. Click  on the IVR Services toolbar to create a new Conference IVR Service.

   The **New Conference IVR Service - Global** dialog opens.
3. Enter a name identifying the service as a gateway IVR service in the **Conference IVR Service Name** field.
4. Define the IVR Service Global parameters (it is recommended to use the system defaults).
5. Ensure that the following options are disabled while defining a Gateway IVR Service:
   - Welcome Messages (in the **Conference IVR Service - Welcome** dialog).
   - Chairperson Messages (in the **Conference IVR Service - Conference Chairperson** dialog).
   - Password Messages (in the **Conference IVR Service - Conference Password** dialog).
6. Select the **General** tab.

   The **General** tab lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.
7. Click the appropriate table entry in the **Message File** column to assign the appropriate audio file to the message type. A drop-down list is enabled. Select the audio file to assign to the event or indication from the list.
8. Repeat Step 6 on page 249 and Step 7 on page 249 to select the audio files for the required messages.
9. For a gateway IVR Service, select the audio file for the following message types:

Message Type	Description
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again.
Dial Tone	The tone that will be played to indicate a dialing tone, to let the calling participant enter the destination number.

Message Type	Description
Ringing Tone	The tone that will be played to indicate that the system is calling the destination number.
Redial on Wrong Number	The message played when the wrong destination is entered, allowing you to enter a new number.
Disconnect on Wrong Number	The message played when the wrong destination is entered, followed by a disconnection tone.
Disconnect on Busy	The tone (or message) played when the dialed destination number is busy.
Disconnect on No Answer	The tone (or message) played when the dialed destination number does not answer.

10. When defining a gateway IVR Service, it is recommended that the **Roll Call** option remains disabled.
11. Open the **Video Services** tab.
12. Define the following conference service parameters:

Video Services	Description
Click&View	Select this option to enable endpoints to run the Click&View application that enables participants to select a video layout from their endpoint.
Video Welcome Slide	Select the video slide file to be displayed when participants connect to the conference. Click **Preview Slide** to view a slide. If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click **Add Slide**. The **Install File** dialog opens. The uploading process is similar to the uploading of audio files. For more information, see step 7. **Note:** • When using one of the default Polycom slides, the slide is displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. • When defining a gateway IVR Service, the recommended default slide is: **Default_GW_Welcome_Slide**.

13. Open the **DTMF Codes** tab.
14. If required, modify the DTMF codes or permissions.
15. Click the **Operator Assistance** tab.
16. If no Operator Assistance is available to participants, clear the **Enable Operator Assistance** option to disable it.
17. Click **OK** to complete the IVR Service definition.

    The new Conference IVR Service is added to the IVR Services list.

Define the Conference Profile for Gateway Calls

The Conference Profile that will be later assigned to the Gateway Profile determine the parameters of the gateway call, such as the line rate and video resolution and if to automatically terminate the gateway session when one participant or no participants are connected to the Gateway Session.

Note: Gathering phase is not supported in gateway calls, even if it is defined in the Profile assigned to the Gateway Profile.

Procedure

1. In the **RMX Management - Rarely Used** pane, select **Conference Profiles**.
2. In the **Conference Profiles** pane, click **New Profile**.

   The **New Profile – General** dialog opens.
3. Define the Profile name and select the line rate for the gateway session.
4. Open the **Advanced** tab.
5. Define the required settings for **Encryption** and **LPR**.
6. Set the **Auto Terminate - At the End** option to **When Last Participant Remains** ensuring that the gateway call will end when only one participant is connected.
7. Define the remaining AVC CP Conferencing Profile parameters and click **OK**.

   The Conference profile for Gateway Sessions is added.

Define the Gateway Profile

A Gateway Profile is a conferencing entity based on the Conference Profile assigned to it that enables endpoints to dial-in and initiate Gateway Sessions.

The system is shipped with a default Gateway Profile, named **Default_GW_Session**.

When an endpoint calls the Gateway Profile, a new Gateway Session is automatically created based on the Profile parameters, and the endpoint joins the gateway call, which can also be a multipoint conference if more than two participants are connected to the conference.

The Gateway Profile defines the parameters of the gateway call that are taken from the Conference Profile assigned to it, such as line rate, resolution, the IVR Service to be used and the dial-in numbers.

Note: Do not enable ISDN (audio or video) access without defining the dial-in numbers range and the use of **Dial-In Numbers as Prefix Range**. If you enable the ISDN (audio or video) access without defining the dialing parameters, people can dial in to the gateway from outside the organization and make long distance calls at the 'host' expense.

Procedure

1. Select  in the **RMX Management - Rarely Used** pane.
2. In the Gateway Profiles pane, click **New Gateway Profile**  .
3. Enter all the details in the New Gateway Profiles pane and click **OK**.

   The Gateway Profile is added to the list.

Gateway Connection to Poly Clariti Edge

You can configure a gateway to Poly Clariti Edge in a combination configuration that enables audio-only ISDN-voice, ISDN-video (video endpoints using only their audio channels), SIP, and H.323 calls. The gateway sessions running on the RealPresence Collaboration Server connect these calls to the Poly Clariti Edge system in a combination configuration.

Each RealPresence Collaboration Server conference acting as a gateway session includes one connection to the Poly Clariti Edge system and another connection to the endpoint. The Poly Clariti Edge system enables load balancing and distribution of multipoint calls on up to 10 RealPresence Collaboration Servers.

The RealPresence Collaboration Server acts as a gateway for the Poly Clariti Edge system that supports H.323 calls. ISDN-voice, ISDN-video, or SIP endpoints dial the virtual meeting room (VMR) on the Poly Clariti Edge system via a special entry queue on the RealPresence Collaboration Server.

Note: Gateway functionality is not supported by RealPresence Collaboration Server (RMX) 1800 with no DSP cards.

For more information on using gateways with Poly Clariti Edge in a combination configuration, see the *Polycom RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Technical Reference* and the *Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay Administrator Guide*.

System Configuration

A Gateway Profile is a conferencing entity based on the Conference Profile assigned to it that enables endpoints to dial-in and initiate Gateway Sessions.

The system is shipped with a default Gateway Profile, named **Default_GW_Session**.

When an endpoint calls the Gateway Profile, a new Gateway Session is automatically created based on the Profile parameters, and the endpoint joins the gateway call, which can also be a multipoint conference if more than two participants are connected to the conference.

The Gateway Profile defines the parameters of the gateway call that are taken from the Conference Profile assigned to it, such as line rate, resolution, the IVR Service to be used and the dial-in numbers.

Note: Do not enable ISDN (audio or video) access without defining the dial-in numbers range and the use of **Dial-In Numbers as Prefix Range**. If you enable the ISDN (audio or video) access without defining the dialing parameters, people can dial in to the gateway from outside the organization and make long distance calls at the 'host' expense.

Hide the Connection Information

You can hide the connection indications on the participant's screen during the connection phase by change the system configuration and system flag.

By default, this flag is set to **NO** and all connection indications are displayed.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.

2. In the **MCMS_PARAMETERS_USER** tab, set the value of the **DISABLE_GW_OVERLAY_INDICATION** to **YES**.

Enable ISDN-voice Dial-in Using GK Prefix

You can enable the ISDN-voice dial-in using GK prefix.

The following table summarizes the ISDN-voice participant's DTMF input depending on the flag value.

ISDN-voice Participant input via DTMF

Configuration	FLAG: USE_GK_PREFIX_FOR_PSTN_CALLS=NO	FLAG: USE_GK_PREFIX_FOR_PSTN_CALLS=YES
Standalone Collaboration Server Conference ID = 1234	ISDN-voice participant enters: 1234#.	ISDN-voice participant enters: 761234# (The Gatekeeper Prefix "76" is automatically removed from the DTMF input string for a standalone Collaboration Server.)
Collaboration Server with Poly Clariti Core Virtual Meeting Room ID in Poly Clariti Core = 1234 Poly Clariti Edge gatekeeper prefix = 76	ISDN-voice participant enters: 761234#	

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, set the value of the **USE_GK_PREFIX_FOR_PSTN_CALLS** to **YES**.

Redial Gateway Calls

The gateway can redial to numbers that are wrong, or busy, or there is no answer.

Procedure

- Redial the call with IVR is supported in the following scenarios:
  - In CP environments only.
  - For H.323, SIP and ISDN-video calls.
  - When using the Collaboration Server's Inviting Participants using DTMF functionality.
- Redial the call with IVR is not supportedin the following scenarios:
  - When using PCM's Invite Participant functionality.
  - Dialing multiple destination numbers.

Direct Dialing Using IP Addresses

You can configure RealPresence Collaboration Servers registered to a gatekeeper to dial and receive calls to and from H.323 endpoints using the IP address.

This option is available to place calls if the gatekeeper is not functioning.

Configure Direct IP Dialing for Dial-Out Calls

Direct IP dialing for dial-out calls enables you to dial to an endpoint using the endpoint's IP address if the gatekeeper isn't functioning.

Make sure you have defined an **IP address** for the endpoint's Participant Properties in the **Address Book**. If you haven't defined the endpoint's IP address and try use the direct IP dial option, the call fails.

Direct IP dialing is enabled by default.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration** > **MCMS_PARAMETERS_USER**.
2. Configure the following system flag:

   GK_MANDATORY_FOR_CALLS_OUT

   No (default) - Enable direct IP dialing

   Yes - Disable direct IP dialing (require the gatekeeper for dial-out calls)
3. Select **OK**, then select **Close**.
4. Reset the RealPresence Collaboration Server for the flag changes to take effect.

Configure Direct IP Dialing for Dial-In Calls

Direct IP dialing for dial-in calls enables you to connect directly to the entry queue, conference, or meeting room if the gatekeeper isn't functioning.

Direct IP dialing is enabled by default.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration** > **MCMS_PARAMETERS_USER**.
2. Configure the following system flag:

   GK_MANDATORY_FOR_CALLS_IN

   No (default) - Enable direct IP dialing

   Yes - Disable direct IP dialing (require the gatekeeper for dial-in calls)
3. Select **OK**, then select **Close**.
4. Reset the RealPresence Collaboration Server for the flag changes to take effect.

Direct Dialing from ISDN (audio or video) Endpoint to IP Endpoint Using a Meeting Room

Dialing from an ISDN-video endpoint to a specific IP endpoint using the Gateway Profile is a two-step process (dialing to the Gateway and then entering the number of the destination IP endpoint).

When dialing to specific IP endpoints, you can simplify the dialing process by creating the appropriate Meeting Room.

Procedure

1. Set the conference parameters in the Conference Profile and make sure that the conference will automatically end when there is only one participant connected to the meeting.
2. Define the Meeting Room with the following:
    - Conference Profile in which the **Auto Terminate - At the end - When Last Participant Remains** option is selected.
    - ISDN (audio/video) access is enabled and a dial-in number is assigned to the Meeting Room.
    - The dial-out IP endpoint is added to the Meeting Room's Participants list.

Deploying a Polycom RMX Serial Gateway S4GW

UC APL Public Key Infrastructure (PKI) requires that the Serial Gateway S4GW be connected directly to the RealPresence Collaboration Server and not to the H.323 network.

The Serial Gateway effectively becomes an additional module of the RealPresence Collaboration Server, with all web and H.323 traffic passing through the RealPresence Collaboration Server. For more information see *RealPresence Collaboration Server (RMX) 2000/4000 Deployment Guide for Maximum Security Environments*, Deploying a Polycom RMX Serial Gateway S4GW.

System Configuration

Topics:

This section includes information on managing system user accounts, security information, and modular MCU configuration. You can also find descriptions and values for system flags.

- User Management
- System Flags
- Secure Communication Mode
- Security Certificates
- Modular MCU

User Management

Topics:

This section provides an introduction to user management options, functionality, and operations associated with the RealPresence Collaboration Server.

It includes the following topics:

- User roles and permissions
- Managing users

Related Links

Move Participants Between Conferences on page 181

User Roles (Authorization Levels) and Permissions

The RealPresence Collaboration Server (also called the MCU) includes a default set of user roles or authorization levels.

Each role is associated with a unique set of permissions that allow a user with that role to perform a set of tasks.

The following table identifies the default system user roles or authorization levels.

Role	Description
Administrator	A full administrator can define and delete other users and perform all configuration and maintenance tasks. The RealPresence Collaboration Server ships with a default Administrator user called `POLYCOM`, whose password is `POLYCOM`. However, once you have defined other authorized Administrator users, it is recommended to remove the default user. Administrators can verify which users are defined in the system. Administrators can't view user passwords, but administrators can change user passwords.
Administrator read-only	An administrator with read-only permissions has the same viewing and monitoring permissions as a full administrator and a read-only administrator can create system backups. However, a read-only administrator cannot perform any other configuration- or conference-related operation.
Operator	An operator can manage meeting rooms, profiles, entry queues, and SIP factories. An operator can also view the system configuration, but cannot change it. Operators can verify which users are defined in the system. However, operators can't view user passwords.

Role	Description
Chairperson	A chairperson can manage active conferences and participants in both single and cascading MCU scenarios. The chairperson does not have any access to the system configurations and utilities.
Auditor	An Auditor can only view auditor and CDR files and audit the system. The Auditor can connect to the RealPresence Collaboration Server only via the RMX Web Client.

Related Links

Event Auditor on page 478

Available Tasks by User Type

The following tables identify which user interface panes, features, and functions are available to which type of RealPresence Collaboration Server (RMX) system user based on conferencing mode.

Admin Tasks by Conferencing Mode

Task	CP	SVC	Mixed	VSW
General	Yes	Yes	Yes	Yes
Advanced	Yes	Yes	Yes	Yes
Gathering Settings	Yes	No	No	Yes
Video Quality	Yes	Yes	Yes	Yes
Video Settings	Yes	Yes	Yes	Yes
Audio Settings	Yes	Yes	Yes	Yes
Customized Polling	Yes	No	No	Yes
Skins	Yes	No	Yes	No
IVR	Yes	Yes	Yes	Yes
Information	Yes	Yes	Yes	Yes
Recording	Yes	No	Yes	Yes
Site Names	Yes	No	Yes	No
Message Overlay	Yes	No	No	No
Network Services	Yes	Yes	Yes	Yes

Chairperson Tasks by Conferencing Mode

Task	CP	SVC	Mixed	VSW
General	Yes	Yes	Yes	Yes
Advanced	Yes	Yes	Yes	Yes
Gathering Settings	Yes	No	No	Yes
Video Quality	Yes	Yes	Yes	Yes
Video Settings	Yes	Yes	Yes	Yes
Audio Settings	Yes	Yes	Yes	Yes
Customized Polling	No	No	No	No
Skins	Yes	No	Yes	No
IVR	No	No	No	No
Information	Yes	Yes	Yes	Yes
Recording	Yes	No	Yes	Yes
Site Names	Yes	No	Yes	No
Message Overlay	Yes	No	No	No
Network Services	Yes	Yes	Yes	Yes

Operator Tasks by Conferencing Mode

Setting	CP	SVC	Mixed	VSW
General	Yes	Yes	Yes	Yes
Advanced	Yes	Yes	Yes	Yes
Gathering Settings	Yes	No	No	Yes
Video Quality	Yes	Yes	Yes	Yes
Video Settings	Yes	Yes	Yes	Yes
Audio Settings	Yes	Yes	Yes	Yes
Customized Polling	Yes	No	No	Yes
Skins	Yes	No	Yes	No
IVR	Yes	Yes	Yes	Yes
Information	Yes	Yes	Yes	Yes
Recording	Yes	No	Yes	Yes

Setting	CP	SVC	Mixed	VSW
Site Names	Yes	No	Yes	No
Message Overlay	Yes	No	No	No
Network Services	Yes	Yes	Yes	Yes

Managing Users

Only users assigned the administrator role can manage RealPresence Collaboration Server users.

View the List of Current Users

The **Users** pane lists the currently defined users in the system.

Procedure

» In the **RMX Management** pane, click **Users** .

The displayed **User** list includes the following columns:

Field	Description
User Name	The login name used by the user to connect to the MCU.
Authorization	The role assigned to the user.
Disabled	Indicates whether the user is enabled or disabled. Disabled users cannot access the system. This setting is controlled by the system administrator.
Locked	Indicates whether or not the user has been locked out system. In Ultra Secure Mode (ULTRA_SECURE_MODE=YES), the system can automatically lock users when: • They have not logged into the system for a predefined period • Their login session does not meet Enhanced Security requirements Only administrators can reset this lock.

Add a User

Administrators can add a new user to the system.

Procedure

1. In the **RMX Management** pane, click **Users** .
2. Click **New User** .
3. In the User Properties dialog box, enter the following information.

Column	Description
User Name	Enter the user's unique login name.
Password	Assign the user a password. This password must be a minimum of eight ASCII characters in length.
Authorization Level	Assign the user the correct role: Administrator, Administrator Read-Only, Operator, Chairperson, or Auditor

4. Click **OK**.

Edit a User

Administrators can edit a user's account information.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. In the **Users** list, select the user, right-click, and select User Properties.
3. In the **User Properties** dialog box, edit the account information and click **OK**.

Delete a User

Administrators can delete a user’s account.

Note: You can’t delete the last remaining administrator in the **Users** list.

Procedure

1. Go to **RMX Management** > **Users**  .
2. In the **Users** list, select the user and select **Delete**  .
3. Select **Yes**.

Change a User's Password

Administrators can change their own passwords and other users' passwords.

Operators can change their own passwords.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. In the **Users** list, select the user, right-click, and select **Change User Password**.
3. Enter the **Old Password** (current), **New Password** and **Confirm the New Password**. This password must be a minimum of eight ASCII characters in length.
4. Click **OK**.

Disable a User

When necessary, an administrator can disable a user rather than deleting the user.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. In the **Users** list, select the user, right-click, and select **Disable User**.
3. Click **Yes** to confirm.

Enable a User

An administrator can re-enable a disabled user.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. In the **Users** list, select the user, right-click, and select **Enable User**.
3. Click **Yes** to confirm.

Rename a User

You may occasionally be required to change or correct a user's name.

In this case, you can rename the user.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. Right-click the user to be renamed and select **Rename User**.
3. Enter the user's correct name and click **OK**.

Add a Machine Account

Servers or systems may need to periodically connect with the RealPresence Collaboration Server to enable some features and functions.

Assign these servers or systems (application user) machine accounts to ensure that all connections are secured using the same connection standards as user accounts.

Machine accounts are only supported when TLS security is enabled and Request peer certificate is selected.

Administrators add machine accounts to the system as a special class of user known as application users.

Procedure

1. In the **RMX Management** pane, click **Users**  .
2. Click **New User**  .
3. In the **User Properties** dialog box, enter the following information.

Column	Description
User Name	Enter a unique application user name--for example, DMA1.
Password	Assign the application user a password. This password must be a minimum of eight ASCII characters in length.
Authorization Level	Assign the application user the required role: Administrator, Administrator Read-Only, Operator, Chairperson, or Auditor
Associate with a machine	Check this option for machine accounts only
Common Name (CN)	Enter the FQDN of the server/machine hosting the application for which the added application user is defined--for example, dma1.polycom.com

4. Click **OK**.

View MCU Connections

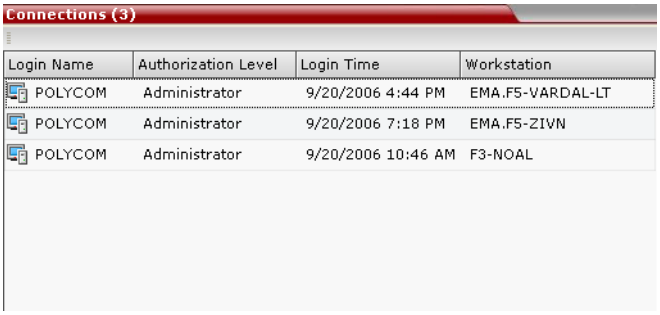
The RealPresence Collaboration Server allows you to list all connections that are currently logged into the MCU including users, servers or API users.

The MCU issues an ID number for each login. The ID numbers are reset whenever the MCU is reset.

An MCU supports a maximum of 50 concurrent connections.

Procedure

» In the **RMX Management** pane, click **Connections** ( ).



The information includes:

- The user's login name.
- The user's authorization level (Chairperson, Operator, Administrator or Auditor).
- The time the user logged in.
- The name/identification of the computer used for the user's connection.

System Flags

Topics:

In general, configure the RealPresence Collaboration Server using the Web Client user interface.

However, if necessary, you can also configure the MCU for specific application and operational needs by adding RealPresence Collaboration Server system flags and setting them to the required values. While many of the predefined system flags have corresponding user interface settings, some don't.

Related Links

Integrate with the Poly Clariti Manager System on page 30
Participant Properties on page 160
Schedule a Conference on page 169
Conference Profile Parameters on page 138
Restrict Content Sharing in Lecture Mode on page 192
System Flags Controlling Secure Communication on page 341
Enable Multi-Part CDRs on page 399
Discussion Mode Layout System Flags on page 450
Motion Slide Blocking for TIP Endpoints System Flags on page 457

Add a System Flag

Add system flags to the RealPresence Collaboration Server through the RMX Manager.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, click **New Flag**.
3. Enter the flag name in the **New Flag** field and the flag setting in the **Value** field.
4. Click **OK**.
5. Click **Close**.

Edit a System Flag

You can modify the value of system flags from their default settings.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, select the flag to modify and click **Edit Flag**.

3. Enter the value in the **New Value** field and click **OK**.
4. Repeat steps 2 and 3 to modify any additional flags.
5. Click **Close**.

Delete a System Flag

You can delete a system flag from the RealPresence Collaboration Server.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, select a flag to be deleted and click **Delete Flag**.
3. Click **Yes** to confirm and then click **OK**.

Predefined System Flags

The following tables list the predefined RealPresence Collaboration Server's system flags that are responsible for general system logic.

In this case, predefined means that the RealPresence Collaboration Server can interpret and integrate the value of these system flags into its configuration and logic.

- General System Flags
- CS System Flags
- Password Generation Flags
- Global Address Book Integration Flags
- Auto Layout - Default Layouts in CP Conferences Flags
- Available Layout Flags

General System Flags

Flag Name	Description	Platform	Add?
`ACCEPT_VOIP_DTMF_TYPE`	Defines the type of DTMF tones (inband) or digits (outband) that the RealPresence Collaboration Server accepts in VoIP calls depending on the endpoint's current setting. Range: • 0 - Auto (default) Changing the endpoint, causes the value of the `SET_DTMF_SOURCE_DIFF_IN_SEC` flag to determine the time interval after which the server accepts both the inband and outband tones/digits. • 1 - Outband (H.245) only • 2 - Inband only	HW/VE	Yes

Flag Name	Description	Platform	Add?
ALLOW_SIREN7_CODEC	Prevents disconnection of Lync clients using audio rates smaller than 42 Kbps, when the Lync server configuration is to allow 33 Kbps audio rate. SIP/Lync calls prefer Siren 7 audio codec, depending on the value of this flag. Default value: NO Possible values: YES/NO	HW/VE	Yes
ALWAYS_APPLY_CONTENT_THRESHOLD	Setting this flag to YES, applies the content rate thresholds configured through the following: • H264_HD_GRAPHICS_MIN_CONTENT_RATE • H264_HD_HIGHRES_MIN_CONTENT_RATE • H264_HD_LIVEVIDEO_MIN_CONTENT_RATE Default value: YES Possible values: YES/NO **Note:** Requires MCU reset for the settings to take effect.	HW/VE	Yes
ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN	Setting the flag to YES, causes the gateway session to forward the DTMF codes to all ISDN-voice and video participants. Default Value: NO Possible values: YES/NO	HW	Yes
AVC_WITH_SVC_CASCADE	When set to YES this flag puts the RealPresence Collaboration Server in AVC+SVC(SIP)-Cascade-only mode. When set to NO, the RealPresence Collaboration Server is in its default state rather than AVC+SVC (SIP) Cascade mode or SVC-only mode.		
AV_MCU_PANORAMIC_LAYOUT_ENABLED	Enables panoramic layout on the MCU. Default value: NO Possible values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
BLOCK_CONTENT_LEGACY_FOR_LYNC	When set to YES, Lync clients don't receive content over the video channel. Also includes those with the Polycom CCS plug-in installed, and enabling Send Content to Legacy Endpoints. This has no effect on other non-Lync legacy endpoints and they receive content according to the Send Content to Legacy Endpoints settings in the conference profile. When set to NO, Lync clients receive content over the video channel, including those with the plug-in, with disabling the Send Content to Legacy Endpoints. Other non-Lync legacy endpoints receive content according to the Send Content to Legacy Endpoints settings in the conference Profile. Default value: NO Possible values: YES/NO	HW/VE	Yes
BLOCK_NEW_LYNC2013_FUNCTIONALITY	Setting this flag to YES, disables all Microsoft Lync 2013 functionality. All Lync 2013 clients, whether connected directly or through cascading, connect using the RTV codec. Default value: NO Possible values: YES/NO		Yes
BONDING_CHANNEL_DELAY (ISDN-video)	When connecting a bonding group, this is the delay (number of 1/100 seconds) between dialing attempts to connect sequential channels. The channel per second connection of ISDN-video switches can vary and cause timing issues resulting in bonding channel disconnection. Default value: 50	HW/VE	No
BONDING_DIALING_METHOD	Setting this flag to SEQUENTIAL, the MCU initiates channel connections until it reaches the number of channels defined by the BONDING_NUM_CHANNELS_IN_GROUP flag. After connecting a channel, dialing begins for the next channel in the group. Setting this flag to BY_TIMERS, the MCU initiates channel connections using values of the BONDING_CHANNEL_DELAY and BONDING_GROUP_DELAY flags. Dial the first group of channels using the BONDING_CHANNEL_DELAY flag for dialing between each channel in the group. Default value: SEQUENTIAL	HW	Yes

Flag Name	Description	Platform	Add?
BONDING_GROUP_DELAY (ISDN-video)	When connecting several bonding groups, this is the delay (number of 1/100 seconds) preceding the first dialing attempt to connect the next bonding group. Default value: 500	HW	Yes
BONDING_NUM_CHANNELS_IN_GROUP (ISDN-video)	The number of channels to connect in the bonding group before dialing the next sequential channel. Default value: 50	HW	Yes
BURN_BIOS	Although not recommended, setting this flag's value to NO prevents BIOS upgrade. Default value: YES Possible values: YES/NO	HW/VE	Yes
CAC_ENABLE	Setting this flag to YES, enables Call Admission Control (CAC) implementation in the RealPresence Collaboration Server. Default value: NO (CAC is inactive). Possible values: YES/NO	HW/VE	Yes
CASCADE_LINK_PLAY_TONE_ON_CONNECTION	Setting this flag to YES, the RealPresence Collaboration Server plays a tone on creation of a cascading link between conferences. The tone plays in both conferences. There's no tone for the disconnection of the cascading link from the conferences. Use the IVR_MESSAGE_VOLUME flag to control the tone volume. Default value: NO Possible values: YES/NO	HW/VE	Yes
CFG_KEY_ENABLE_FLOW_CONTROL_REINVITE	Enables or disables sending a re-INVITE to endpoints to adjust data rate. When set to YES, use re-INVITE for endpoints not supporting flow control in SIP using either the information or RTCP feedback mechanisms. Default value: NO Possible values: YES/NO	HW/VE	Yes
CHANGE_AD_HOC_CONF_DURATION	To configure the duration of an ad hoc conference, set the flag to one of the following values:* Default value: 60 minutes Possible values: 90 minutes, 180 minutes, and 270 minutes.	HW/VE	No

Flag Name	Description	Platform	Add?
CONTENT_SLAVE_LINKS_INTRA_SUPPRESSION_IN_SECONDS	Defines the interval for RealPresence Collaboration Server to forward an Intra Request received from any of the Secondary Cascading Links. The Secondary Cascading Link connects to the local RealPresence Collaboration Server, to an MCU on a higher cascade level, or to the content sharer. On receiving the first Intra request from the secondary MCUs, the interval counter starts. It forwards the request to the next level MC, or to the content sharer. It registers other Intra requests within this interval. Then the system checks for any additional registration of intra requests during the last interval. If there's at least one Intra request, it forwards it, else it waits for the next cycle. It repeats this filtering process every <flag value> second. Default value: 30 seconds	HW/VE	No
CP_REGARD_TO_INCOMING_SETUP_RATE	For use in the Avaya environment. When set to YES, the server calculates the line rate according to the line rate of the endpoint in the H. 225 setup message. When set to NO, the server calculates the rate according to the conference line rate. Default value: YES Possible values: YES/NO	HW/VE	Yes
CPU_BONDING_LINK_MONITORING_FREQUENCY	Used when using the MII Monitor for troubleshooting networks. This flag sets the MII Polling Interval in milliseconds. A value of zero disables the MII monitoring. Default value: 100	HW/VE	Yes

* When the participant dials into an Ad hoc Entry Queue and enters a unique conference ID, it automatically creates an Ad hoc conference. Conference Profile assigned to the EQ determines the type of the conference. <does ad hoc conference need to be defined>.

Flag Name	Description	Platform	Add?
CPU_BONDING_MODE	Sets the Bonding Mode of the Signaling and Management network interface controllers. Mode=6, balance-alb, (Adaptive Load Balancing) includes balance-tlb, (Transmit Load Balancing) and balance-rlb (Receive Load Balancing) for IPv4 traffic. Requires no special switch support. ARP negotiation achieves Receive Load Balancing. This replaces the ARP Replies and their source hardware address. It uses the unique hardware address of one of the secondary in the bond. In this way, different peers use different hardware addresses for the server. **Note:** balance-alb is the only supported value. All other possible values are for troubleshooting purposes only. Default value: balance-alb Possible values: • balance-alb • balance-rr • active-backup • balance-xor • broadcast • 802.3ad • balance-tlb	HW/VE	Yes
CPU_TCP_KEEP_ALIVE_TIME_SECONDS	Indicates when to send the first KeepAlive indication to check the TCP connection. Default value: 7200 seconds Range: 600-18000 seconds **Note:** When there are NAT problems and this default is too long, it causes the loss of the TCP connection. In such a case, change the default value to 3600 seconds (60 minutes) or less.	HW/VE	No
CPU_TCP_KEEP_INTERVAL_SECONDS	Indicates the interval in seconds between the KeepAlive requests. Default value: 75 seconds Range: 10-720 seconds	HW/VE	No

Flag Name	Description	Platform	Add?
DELAY_BETWEEN_H320_DIAL_OUT_PARTY	The delay in milliseconds that the MCU waits when connecting dial out ISDN-video and voice participants. Default value: 1000	HW	Yes
DISABLE_DUMMY_REGISTRATION	Enables or disables SIP dummy registration on the domain. Default value: NO Possible Values: • NO (Default) - Disables SIP dummy registration. • YES - Enables SIP dummy registration. **Note:** Set the flag to YES for homologation and certification testing.	HW/VE	Yes
DISABLE_GW_OVERLAY_INDICATION	When set to NO, this flag displays the progress indication during the connection phase of a gateway call. When set to YES, it hides the connection indications on the participant's screen during the connection phase of a gateway call. Default value: NO Possible values: YES/NO	HW/VE	Yes
DISABLE_WIDE_RES_TO_SIP_DIAL_OUT	When set to NO, the RealPresence Collaboration Server sends a widescreen resolution to dial-out SIP endpoints. The server automatically identifies the endpoint types not supporting wide screen resolutions according to their product type and version. When set to YES, the RealPresence Collaboration Server doesn't send wide screen. Default value: NO Possible values: YES/NO	HW/VE	Yes
DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS	Used for DTMF code suppression in cascading conferences. Determines the time period during which MCU A forwards all DTMF inputs from conference A participants to MCU B. This has no effect to conferences running on itself. Default value: 60 seconds Range: 0 - 360000 seconds	HW/VE	Yes

Flag Name	Description	Platform	Add?
ENABLE_AGC	When set to YES, this flag implements Auto Gain Control (AGC) for the participant audio. This mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. Default value: NO Possible values: YES/NO **Note:** Enabling AGC might result in amplification of background noise.	HW/VE	No
ENABLE_AUTO_EXTENSION	When set to YES, this flag allows conferences running on the RealPresence Collaboration Server to automatically extend as long as it has participants in it and the system has free resources. When set to NO, this flag prevents the conference duration from automatically extending. Default value: YES Possible values: YES/NO **Note:** Setting this flag to: • YES, there's no limit in duration for gateway calls if there are endpoints in it. • NO, the time duration for gateway calls is 60 minutes.	HW/VE	No
ENABLE_AQUA_FEATURE_SYSTEM_FLAG	Use this system flag for enabling the RealPresence Collaboration Server, Virtual Edition to support Polycom RealConnect specific functionality in a Microsoft Online Office365 environment. Default value: NO Possible values: YES/NO	VE	

Flag Name	Description	Platform	Add?
ENABLE_AQUA_DOUGH_BOY_FLAG	Set the ENABLE_AQUA_FEATURE_SYSTEM_FLAG flag and then use this system flag to enable the Doughboy feature. This feature displays a Doughboy image in the place of the normal image when a Skype for Business or Lync user disables its video output. This is applicable only for a Skype or Lync user in a Polycom RealConnect conference. If the Skype or Lync user enables its video output once again, the server stops displaying the Doughboy image and reverts to the normal image. Default value: NO Possible values: YES/NO		
ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD	Enables a cascaded link to enter the conference without a password. Default value: NO, for security reasons. Possible values: YES/NO	HW/VE	No
ENABLE_CISCO_GK	When set to YES, this flag enables the use of an identical prefix for different RealPresence Collaboration Servers when registering with a Cisco MCM gatekeeper. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_CLOSED_CAPTION	When set to NO, disables the Closed Captions option that allows endpoints to provide real-time text transcriptions or language translations of the video conference. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_CODIAN_CASCADE	When set to YES, it defines the MCU as primary at all times when cascading between the RealPresence Collaboration Server and a Codian MCU. Possible values: YES/NO		

Flag Name	Description	Platform	Add?
ENABLE_CONTENT_OF_768_FOR_1024_LV	Generally, the content rate used for 1024 Kbps conferences with a Live Video setting is 512 Kbps. Set this flag to YES, to increase the content rate in this scenario to 768 Kbps. This flag is applicable for protocols supporting H.264 media protocol usage: • H.263 and H.264 auto selection • H.264 HD • H.264 Cascade Optimized Default value: NO Possible values: YES/NO Modifying the flag values requires manual addition with no system reset.	HW/VE	Yes
ENABLE_CONTENT_SNATCH_OVER_CASCADE	When set to YES it enables content snatching in all the MCUs within the H.323 cascaded topology, and also MCUs using RealPresence Collaboration Server version 8.6 and up. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_DTMF_NUMBER_WO_DELIMITER	Using this flag, the administrator can configure the system to change the previous system behavior. When the MCU collects the Conference ID in the local entry queue or the conference password, use time-out as a stop indicator for the string input.		
ENABLE_EPC	When set to YES, enables the Polycom proprietary People+Content. When set to NO, disables this feature for all conferences and participants. Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_EXTERNAL_DB_ACCESS	When set to YES, the RealPresence Collaboration Server connects to an external database application, to validate the participant's right to start a new conference or access a conference. Default value: NO Possible values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
ENABLE_FLOW_CONTROL_RE INVITE	Use this flag to enable or disable sending a re-INVITE to endpoints to adjust their data rate. When set to YES, it uses re-INVITE for endpoints that don't support flow control in SIP using either the Information or RTCP feedback mechanisms. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_G729	Enabled using the G.729 audio codec. When set to NO, ensures disabling of the G.729 codec, and using of G.711 instead. This is useful in calls where the audio quality affects lower line rates. Default value: YES Possible values: YES/NO **Note:** The modified flag setting affects new calls.	HW/VE	Yes
ENABLE_H239	When set to YES, it sends the content through a separate Content channel. Endpoints not supporting H.239, don't receive content. Sending content as a separate stream enables this flag. When set to NO, it closes the Content channel. In such a case, it uses video channel to send H.239 Content. This enables endpoints not supporting H. 239 Content sharing to receive the content in their video channel. Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_H239_ANNEX_T	In H.239-enabled MIH cascading, when MGC is on Level 1, this flag enables sending Content using Annex T. Set this flag to the same value (YES/NO) as the settings of the RealPresence Collaboration Server flag H263_ANNEX_T. Possible values: YES/NO	HW/VE	Yes
ENABLE_HD_SD_IN_FIXED_ MODE	When set to YES, enables H.264 Standard Definition (SD), High Definition (HD), and VSX 8000 (Version 8.0) support in Video Switching conferences. Possible values: YES/NO		
ENABLE_LOBBY_FOR_LOCKE D_CONFERENCE	When set to YES, enables secure meeting lobby to hold new callers who want to join active locked conferences. Possible values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
ENABLE_LYNC_RTCP_INTRA	When set to YES, it uses RTCP FIR for sending Intra Requests. When set to NO, it sends Intra Requests using SIP INFO Messages. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_MCCF	Enables or disables the support of External IVR Services through the MCCF-IVR package. In Ultra Secure Mode and secure environments, set this flag to NO if: • There's no requirement of the External IVR Service • You want to close the ports not in use. Default value: YES (in Standard security Mode) or NO (in Ultra Secure Mode) Possible values: YES/NO	HW/VE	Yes
ENABLE_MULTI_PART_CDR	Enables saving more than 1MB of Call Detail Record (CDR) data on the MCU. By default, the MCU limits the CDR file size to 1MB. When a CDR file reaches that size, the MCU saves the CDR, stops further call data recording, and loses the additional data. This flag adds a Part Index to the CDR List. It displays the CDR file sequence in the CDR file set. The files in a set have the same unique Display Name. Default value: NO (disabled) Possible values: YES/NO		
ENABLE_MODULAR_MCU	Indicates whether the system is in MMCU mode. Possible values: Default value: NO - System isn't in MMCU mode. Possible values: • MIX - System is in partial MMCU mode. • YES - System is in full MMCU mode. **Note:** It requires MCU reset for changes to take effect.	HW/VE	No

Flag Name	Description	Platform	Add?
ENABLE_MS_FEC	Enables the Microsoft FEC (Forward Error Correction) support for RTV. When set to AUTO, it enables FEC support. FEC uses the DV00 option (DV=00 - one FEC per frame using XOR). When set to No, it disables FEC support. Default value: AUTO Possible values: AUTO/No	HW/VE	Yes
ENABLE_NO_VIDEO_RESOURCES_AUDIO_ONLY_MESSAGE	Enables playing a voice message informing the participant of the lack of video resources. They connect as audio only. Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_POLYCOM_EPS_IN_LYNC_ROSTER	Enables all Polycom endpoints connected to the RealPresence Platform in Lync roster. Default value: DISABLED Possible values: DISABLED, ENABLE_IGNORE_ORGANIZER, ENABLE_CONSIDER_ORGANIZER	HW/VE	Yes
ENABLE_RECORDING_OPERATION_VIA_SIPINFO	Allows performing the recording control operations using either DTMF tones or a SIP INFO request. When set to NO, the server sends Recording Control Operation commands to the Polycom® RealPresence® Media Suite using DTMF. When set to YES, the server sends Recording Control Operation commands to the RealPresence® Media Suite system using a SIP INFO request. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_SELECTIVE_MIXING	Manually add this flag and enable or disable the function by changing the value to YES/NO. It doesn't require MCU reset when changing the system flag value. Possible values: YES/NO		Yes

Flag Name	Description	Platform	Add?
ENABLE_SIP_PEOPLE_PLUS_CONTENT	If security is of a higher priority than SIP Content sharing, disable SIP People+Content™ technology by setting this system flag to NO. (The content management control (BFCP) uses an unsecured channel (port 60005 and 60006 for IPv4 and IPv6 respectively) even after enabling SIP TLS). Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_SIP_PPC_FOR_ALL_USER_AGENT	When set to YES, it declares SIP People+Content and BFCP capabilities with all vendors' endpoints. Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_SIRENLPR	Enables or disables the Polycom® Siren™ Lost Packet Recovery Audio Algorithm for use in IP (H. 323, SIP) calls in both CP and VSW conferences. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_SIRENLPR_SIP_ENCRYPTION	Enables the Polycom® Siren™ Lost Packet Recovery audio algorithm when using encryption with the SIP protocol. Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_SVC_ONLY	Enables Exclusive SVC Mode. In this mode, the system supports only SVC Meeting Room conferences and rejects all other types of conferences, including calls made to Virtual Meeting Rooms on Poly Clariti Core systems. Changing this flag requires an RMX reboot. Default value: NO Possible values: YES/NO		
ENABLE_TC_PACKAGE	Enables or disables the Network Traffic Control. Default value: NO Possible values: YES/NO	HW/VE	Yes
ENABLE_TEXTUAL_CONFERENCE_STATUS	Set the flag value to NO to disable Text Indication. Use this setting for MCUs running Telepresence conferences. Default value: YES Possible values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
ENABLE_TOGGLE_SVC_ONLY	When set to YES this flag puts the RealPresence Collaboration Server in SVC-only mode. When set to NO, the RealPresence Collaboration Server is in its default state rather than AVC+SVC (SIP) Cascade mode or SVC-only mode.		
ENFORCE_SAFE_UPGRADE	When set to YES this flag enables the RealPresence Collaboration Server to notify users on selection of an incorrect version upgrade/downgrade or upgrade/downgrade path. When set to NO, the server activates a fault alert in the Faults List after initiating an upgrade or downgrade software installation. **Note:** Upgrade started and SAFE Upgrade protection is turned OFF and the upgrade/downgrade process continues. Default value: YES Possible values: YES/NO	HW	No
EXT_DB_IVR_PROV_TIME_SECONDS	Sets an Entry Queue as IVR Service Provider for the Poly Clariti Core system. The value here indicates the time interval in seconds in which the database is accessible for the ID. Default value: 300	HW/VE	No
EXTERNAL_CONTENT_DIRECTORY	The Web Server folder name. Change this name if it's different than the default value of the Poly Clariti Manager application. Default value: /PlcmWebServices	HW/VE	Yes
EXTERNAL_CONTENT_IP	Enter the IP address of the Poly Clariti Manager server in the format: For example, http://172.22.185.89 This flag is also a trigger for replacing the internal RealPresence Collaboration Server address book with Poly Clariti Manager global Address Book. When empty, it disables the integration of Poly Clariti Manager address book with RealPresence Collaboration Server.	HW/VE	Yes
EXTERNAL_CONTENT_PASSWORD	The password of the user name for RealPresence Collaboration Server in Poly Clariti Manager server.	HW/VE	Yes

Flag Name	Description	Platform	Add?
EXTERNAL_CONTENT_PORT	The Poly Clariti Manager port that the server uses to send and receive XML requests/responses. Default value: 80	HW/VE	Yes
EXTERNAL_CONTENT_USER	The login name for the RealPresence Collaboration Server in the Poly Clariti Manager server in the format: domain name/user name	HW/VE	Yes
EXTERNAL_DB_DIRECTORY	The URL of the external database application. For the sample script application, the URL is: <virtual directory>/SubmitQuery.asp **Note:** Applicable to RealPresence Collaboration Server 2000 or 4000 only.	HW/VE	Yes
EXTERNAL_DB_IP	The IP address of the external database server, if one is in use. Default value: 0.0.0.0 **Note:** Applicable to RealPresence Collaboration Server 2000 or 4000 only.	HW/VE	Yes
EXTERNAL_DB_LOGIN	The login name for the RealPresence Collaboration Server in the external database server. Default value: POLYCOM **Note:** Applicable to RealPresence Collaboration Server 2000 or 4000 only.	HW/VE	Yes
EXTERNAL_DB_PASSWORD	The password for the user name for the server on the external database server. Default value: POLYCOM **Note:** Applicable to RealPresence Collaboration Server 2000 or 4000 only.	HW/VE	Yes
FADE_IN_FADE_OUT	Add this flag to disable the Fade-In/Fade-Out feature, and set its value to NO. Possible values: YES/ NO		

Flag Name	Description	Platform	Add?
FORCE_APACHE_REBOOT_UPON_CRL_UPLOAD	Allows the administrator to choose the method of propagating a new, automatically downloaded CRL to various Apache Server clients. Default value: NO Possible values: YES/NO When set to NO, no Apache Server reboot upon a new CRL upload. When set to YES, the Apache Server is reboots upon a new CRL upload. **Note:** Applicable to automatically upload of CRLs only. Manual CRL upload includes the option of updating the Certification Repository by rebooting the Apache Server. Applies to the Default Management Network Service CRL only.		
FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE	Hosting a Microsoft Office Communicator R2 or Lync client is on a workstation with a single core processor, forces the use of a specific audio algorithm. The flag value overrides the default audio algorithm selection (G.722.1) that might cause audio quality problems when Microsoft clients running on single processor workstations use G.722.1. You can set this flag to: • AUTO - No forcing occurs and the RealPresence Collaboration Server negotiates a full set of Audio algorithm during capabilities exchange. • G711A/U or G722 - Set this flag value according to the hosting workstation capabilities. If the RealPresence Collaboration Server detects single core host during capabilities exchange, it assigns a G.711 or G.722 Audio algorithm according to the flag value. Default value: G.711A Possible values: AUTO, G.711A, G.711U, G.722	HW/VE	Yes

Flag Name	Description	Platform	Add?
FORCE_CIF_PORT_ALLOCATION	Sets the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution of the Conference Profile parameters. You can specify the endpoint types for which you want to force resource allocation to CIF resource. This enables other types of endpoints to use higher resolutions in the same conference. Enter the product type to which you want to allocate the CIF resource. Possible values are VSX nnnn - where nnnn represents the model number. For example, VSX 8000.	HW/VE	No
FORCE_G711A	Forces the use of the G.711A audio codec. Default value: NO Possible values: YES/NO	HW/VE	Yes
FORCE_LEGACY_EP_CONTENT_LAYOUT_ON_TELEPRESENCE	To ignore personal layouts during Telepresence conferences (while working with MLA), set the value of the flag FORCE_LEGACY_EP_CONTENT_LAYOUT_ON_TELEPRESENCE to YES. If the layout for displaying content in Legacy endpoints includes multiples cells, the MCU might populate Telepresence room streams sources in remote cells. NO (Default) - The MCU doesn't manage the layouts while sending Content. Personal layout changes, for example, by MLA, override the default MCU layout. Legacy endpoints might not display Content in Telepresence conferences due to layout changes. YES - The MCU manages the layouts while sending Content. It ignores personal layout changes, for example, by MLA. MCU manages the layouts for legacy endpoints.		
FORCE_RESOLUTION	This flag specifies IP (H.323 and SIP) endpoint types that don't receive wide screen resolution. Also the server can't identify them automatically. Possible values are endpoint types, each type followed by a semicolon. For example, when disabling wide screen resolution in an HDX endpoint, enter the following string: HDX. **Note:** Use this flag when the flag value of SEND_WIDE_RES_TO_IP is YES.	HW/VE	Yes

Flag Name	Description	Platform	Add?
FORCE_STATIC_MB_ENCODING	This flag supports Tandberg MXP mode of sending and receiving video when IP endpoints: • Have HD 720p resolution. • Have Video Quality as Motion. ISDN-video endpoints don't support this mode. Default value: Tandberg MXP. To disable this flag, enter NONE.	HW/VE	Yes
FORCE_SYSTEM_BROADCAST_VOLUME	When set to YES, the level of broadcasting volume of the connected participant is value taken from the system flag SYSTEM_BROADCAST_VOLUME. If set to NO (default), the broadcasting volume level is 5. Default value: NO Possible values: YES/NO	HW/VE	No
FORCE_SYSTEM_LISTENING_VOLUME	When set to YES, the level of listening volume of the connected participant is value taken from the system flag SYSTEM_LISTENING_VOLUME. If set to NO (default), the listening volume level is 5. Default value: NO Possible values: YES/NO	HW/VE	No
G728_IP	Enables or disables the declaration of G.728 Audio Algorithm capabilities in IP calls. Default value: NO Possible values: YES/NO	HW/VE	Yes
G728_ISDN	Enables or disables the declaration of G.728 Audio Algorithm capabilities in ISDN-video calls. Default value: NO Possible values: YES/NO	HW	Yes
GK_MANDATORY_FOR_CALLS_IN	When set to YES, it requires a gatekeeper to receive incoming H.323 calls. Not configuring a gatekeeper in the RealPresence Collaboration Server causes the calls to fail. When set to NO (default), it doesn't require a gatekeeper to process H.323 incoming calls, and H. 323 participants can dial in with or without a gatekeeper. Default value: NO Possible values: YES/NO	HW/VE	No

Flag Name	Description	Platform	Add?
GK_MANDATORY_FOR_CALLS_OUT	When set to YES, it requires a gatekeeper to perform H.323 outgoing calls. Not configuring a gatekeeper on the RealPresence Collaboration Server causes the calls to fail. When set to NO (default), it doesn't require a gatekeeper to dial out to H.323 participants and participants can dial out with or without a gatekeeper. Default: NO Possible values: YES/NO	HW/VE	No
H239_FORCE_CAPABILITIES	When set to NO, the RealPresence Collaboration Server only verifies that the endpoint supports the Content protocols: Up to H.264 or H.263. When set to YES, the RealPresence Collaboration Server checks the frame rate, resolution, and all other parameters of the Content mode as set by an endpoint before receiving or transmitting Content. Default value: NO Possible value: YES/NO	HW/VE	Yes
H263_ANNEX_T	When set to NO, this flag sends the content stream without Annex T and enables Aethra and Tandberg endpoints, that don't support Annex T to process the content. Default value: YES Possible values: YES/NO	HW/VE	No
H264_HD_GRAPHICS_MIN_CONTENT_RATE	Determines the minimum content rate required for endpoints to share H.264 high-quality content through the Content channel when Content Setting is **Graphics**. Default value: 128 Kbps Range: 0-1536 Kbps	HW/VE	Yes
H264_HD_HIGHRES_MIN_CONTENT_RATE	Determines the minimum content rate required for endpoints to share H.264 high-quality content through the Content channel when Content Setting is **Hi Resolution Graphics**. Default value: 256 Kbps Range: 0-1536 Kbps	HW/VE	Yes

Flag Name	Description	Platform	Add?
H264_HD_LIVEVIDEO_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high-quality content through the Content channel when Content Setting is **Live Video**. Default value: 384 Kbps Range: 0-1536 Kbps	HW/VE	Yes
H264_VSW_AUTO	Setting the flag to NO, causes it to disable the highest common mechanism in H.264. It also enables selection of H.264 Video Protocol in Dual Stream Video Switching cascading conferences. Possible values: YES/NO		
H323_FREE_VIDEO_RESOURCES	For use in the Avaya Environment. In the Avaya Environment, there are features that involve converting undefined dial-in participants' connections from video to audio (or vice versa). Setting this flag to NO, causes the participants' video resources to remain available for them. If set to YES, the RealPresence Collaboration Server releases video resources for audio only calls. Default value: YES Possible value: YES/NO	HW/VE	Yes
HD_THRESHOLD_BITRATE	The value of this flag is the minimum threshold bit rate for HD resolutions. The conference profile line rate must be the same or higher than the value of this flag. Default value: 768 Kbps Range: 384 Kbps - 4 Mbps	HW/VE	No
HW_FOLLOW_SPEAKER_RESOLUTION_ON_1X1_LAYOUT	Enables endpoints that are capable of higher resolution in a conference to receive the indication icons. Possible values: • AUTO (default) - Configuring any of the indication icons for display, causes them to not follow the speaker. Not configuring the indication icons for display, they follow the speaker. • YES - Always follow the speaker in 1x1 layout. • NO - Never follow the speaker in 1x1 layout.	HW	No

Flag Name	Description	Platform	Add?
IGNORE_AIM	Audio Indicate Muted (AIM) is relevant to H.323 endpoints. When an endpoint mutes its microphone, it doesn't mute its entire audio stream. This allows sharing of content that includes audio while microphones are on mute. Default value: NO Possible values: NO - Receiving the AIM signal, mutes the participant and displays a mute icon in the RMX Web Client or RMX Manager. YES - Receiving the AIM signal, the participant isn't on mute and it doesn't display a mute icon in the RMX Web Client or RMX Manager. Range: YES/NO	HW	Yes
RPCSVE_ENHANCE_CAPACITY	Setting this flag to YES it only supports AVC-only and SVC-only conference modes. It enables hardware and virtual machine configuration to achieve a higher capacity. Default value: NO Possible values: YES/NO **Note:** This flag is applicable only to MCU ports. You can't use it to enhance the capacity of Soft Blade.	VE	
INTERNAL_SCHEDULER	Setting this flag to NO (default) prevents potential scheduling conflicts that result due to system calls from external scheduling applications. These applications include Polycom ReadiManager®, and others through the API. Set to YES to schedule conference reservations using an external scheduling application. Default value: NO Possible values: YES/NO	HW/VE	No

Flag Name	Description	Platform	Add?
IP_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES adjusts the line rate of HD video switching conferences run on the server. Modify the value from 1920 Kbps to 18432, 100 bps to match the actual rate of the IP Only HD video switching conference running on the MGC. **Note:** If the value of the flag MIX_LINK_ENVIRONMENT is NO, set the IP_ENVIRONMENT_LINK flag to YES. Possible values: YES/NO	HW/VE	Yes
IP_RESPONSE_ECHO	When set to YES, the RealPresence Collaboration Server responds to ping (IPv4 and IPv6) commands. When set to NO, the server doesn't respond to ping commands. Possible values: YES/NO	HW/VE	Yes
IPV6_AUTO_ADDRESS_CONFIGURATION_METHOD	The value of this flag determines the SLAAC (Stateless Address Auto Configuration) and DHCPv6 related system behavior. Default value: AUTO Range: AUTO/SLAAC AUTO (default) - Use DHCPv6 first in case of failure use SLAAC. SLAAC - Use SLAAC only.	HW/VE	Yes
ISDN_COUNTRY_CODE	The name of the country, which contains the MCU. Default value: COUNTRY_NIL	HW	No
ISDN_IDLE_CODE_E1	The Idle code (silent), transmitted on the ISDN-video E1 B channels, when there's no transmission on the channels. Default value: 0x54	HW	No
ISDN_IDLE_CODE_T1	The Idle code (silent), transmitted on the ISDN-video T1 B channels, when there's no transmission on the channels. Default value: 0x13	HW	No
ISDN_NUM_OF_DIGITS	When using ISDN-video overlap sending dialing mode, this field holds the number of digits the MCU receives. Default value: 9	HW	No

Flag Name	Description	Platform	Add?
ISDN_RESOURCE_POLICY	Determines the allocation of the ISDN-video B-channels within spans. You can improve the robustness of the ISDN-video network by allocating channels evenly (load balancing) among the spans. This minimizes the effect of channel loss resulting from the malfunction of a single span. Default value: LOAD_BALANCE Set the flag value to: • LOAD_BALANCE - To allocate channels evenly among all configured spans. • FILL_FROM_FIRST_CONFIGURED_SPAN - To allocate all channels on the first configured span before allocating channels on other spans. • FILL_FROM_LAST_CONFIGURED_SPAN - To allocate all channels on the last configured span before allocating channels on other spans.	HW	No
ITP_CERTIFICATION	When set to NO (default), this flag disables the telepresence features in the Conference Profile. Set the flag to YES to enable the telepresence features in the Conference Profile (provided it has the appropriate license). Default value: NO Possible values: YES/NO	HW/VE	Yes
ITP_CROPPING	Setting the conference to telepresence mode, crops the image according to this flag value: Default value: ITP Possible values: • ITP (default) - No cropping of left-right, symmetric cropping of top-bottom. • CP - Symmetric cropping of both left-right and top-bottom areas (separately calculated). • MIXED - Symmetric cropping of left-right areas and asymmetric cropping of top-bottom areas (16% from top, 84% of bottom). **Note:** Adding the flag with NO in the telepresence conference, doesn't crop the left-right areas. But it crops the top-bottom areas asymmetrically (16% from top, 84% from bottom).	HW/VE	No

Flag Name	Description	Platform	Add?
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Default values: 6 Possible values: 0 - disables playing the IVR messages. 1 - lowest volume 10 - highest volume **Note:** • Don't disable IVR messages by setting the flag value to 0. • It doesn't require system reset for flag changes to take effect.	HW/VE	No
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant connects to the conference varies according to the value of this flag. Default value: 5 Possible values: 0 - disables playing the music. 1 - lowest volume. 10 - highest volume. **Note:** It doesn't require system reset for flag changes to take effect.	HW/VE	No
IVR_ROLL_CALL_SUPPRESS_OPERATOR	When set to YES, the MCU suppresses the entry/exit tone when the operator participant joins or leaves the conference. Default value: NO Possible values: YES/NO	HW/VE	No
IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE	When set to YES, the system doesn't play the Roll Call names when participants enter the conference. Possible values: YES/NO		

Flag Name	Description	Platform	Add?
IVR_ROLL_CALL_VOLUME	The volume of the Roll Call varies according to the value of this flag. Default value: 6 Possible values: 0 - disables playing the Roll Call. 1 - lowest volume. 10 - highest volume. **Note:** • Don't disable the Roll Call by setting the flag value to 0. • It doesn't require system reset for flag changes to take effect.	HW/VE	No
LEGACY_EP_CONTENT_DEFAULT_LAYOUT	Defines the video layout for the screen of the legacy endpoints when switching to Content mode. Default value: CP_LAYOUT_1P7 (1+7)	HW/VE	No

Flag Name	Description	Platform	Add?
LPR_CONTENT_RATE_ADJUST_WEAK_LPR	Initiating the Polycom Lost Packet Recovery (LPR) in an AVC-CP conference due to packet loss, causes the MCU to reduce video rate and avoid exceeding bandwidth. At times, it requires further reduction to preserve the bandwidth, which this system flag regulates. When set to YES, enables H.323 endpoints to reduce their content rate or Polycom Lost Packet Recovery (LPR) strength as follows: • For single MCU conferences: ◦ VSW content - Drop content rate upon packet loss condition. ◦ Transcoding - Drop content rate upon packet loss condition for the endpoint protocol experiencing the packet loss. • For cascaded conferences: ◦ VSW content - Decrease Polycom Lost Packet Recovery (LPR) strength (from 5% to 2%). ◦ Transcoding: If packet loss occurs at one of the local endpoints, drop content rate upon packet loss condition for the endpoint protocol experiencing the packet loss. If packet loss occurs at the cascaded link, Decrease Polycom Lost Packet Recovery (LPR) strength (from 5% to 2%). When set to NO, it doesn't reduce the content rate but guarantees MCU packet loss protection for 5%. Default value: NO Possible values: YES/NO **Note:** • It doesn't require system restart for the new flag value to take effect. • Don't set this flag to YES in systems using TIP conferencing.	HW/VE	Yes

Flag Name	Description	Platform	Add?
LYNC_AVMCU_1080p30_ENCODE_RESOLUTION	Microsoft AVMCU cascade deployment supports HD1080p30 video resolution according to the settings of this flag only in video optimized mode. Default values: NO Possible values: YES/NO • NO - Video streams sent to and received from the MS AVMCU are HD720p30, SD, and CIF. • YES - Video streams sent to the Microsoft AVMCU are HD1080p30, SD, CIF. Video streams received from the Microsoft AVMCU are 720p30, SD, and CIF.	HW/VE	Yes
MANAGE_TELEPRESENCE_ROOM_SWITCH_LAYOUTS	Determines whether the MLA or RealPresence Collaboration Server controls the Room Switch Telepresence Layouts. • When set to NO, the MLA manages Telepresence Room Switch Layouts. • When set to YES, the RealPresence Collaboration Server manages Telepresence Room Switch Layouts. Default value: NO Possible values: YES/NO	HW/VE	Yes
MAX_ALLOWED_RTV_HD_FRAME_RATE	Defines the threshold frame rate in which RTV Video Protocol initiates HD resolutions. Flag values are as follows: Default value: 0 fps Implements any Frame Rate based on Lync RTV Client capabilities. Range: 0-30 fps	HW/VE	Yes
MAX_COUNT_LYNC_PARTIES	Gets the count of Skype and non-Skype for Business audio and video participants in the cascaded conference. Flag values are as follows: Default value: 20 Range: 0-99	HW/VE	Yes

Flag Name	Description	Platform	Add?
MAX_TRACE_LEVEL	Indicates the debugging level for system support. Default value: n Possible values: • TRACE = t • DEBUG = d • INFO_NORMAL = n • INFO_HIGH = i • WARN = w • ERROR = e • FATAL = f • OFF = o	HW/VE	Yes
MAXIMUM_RECORDING_LINKS	The maximum number of links available in the Recording Links list. Default value: 20 Range: 1 - 100	HW/VE	Yes
MCU_DISPLAY_NAME	The MCU name on the endpoint's screen when connecting to the conference. Default value: Polycom RealPresence Collaboration Server 1800, 2000, or 4000 (the last depends on the product type).	HW/VE	No
MEDIA_NIC_MTU_SIZE	The maximum data payload size (bytes) transmitted in a single packet over the network, and should be minimally the MTU_SIZE (see below) to avoid fragmenting of data packets. The RealPresence Collaboration Server sends large amount of data over the network. This helps adjust its MTU size according to its network environment. Default value: 1,500 Range: 500-20,000. It treats values outside that range as 1,500.	HW/VE	Yes
MIN_H239_HD1080_RATE	Use this to set the threshold line rate for HD Resolution Content: the line rate at which the RealPresence Collaboration Server sends Content at HD1080 Resolution. Setting the flag to 0 disables HD Resolution Content. Default value: 768 Kbps	HW/VE	Yes

Flag Name	Description	Platform	Add?
MIN_SYSTEM_DISK_SPACE_TO_ALERT	This flag defines s a minimum remaining disk capacity in megabytes. It also raises an alarm if it falls below this level. Default value: 2048	HW/VE	No
MIN_TIP_COMPATIBILITY_LINE_RATE	The minimum line rate at which you can TIP-enable the conferencing entities to connect endpoints. CTS version 7 requires a minimum line rate of 1024 Kbps and rejects calls at lower line rates. Set to 0 to not enforce minimum line rate on the conference for TIP connectivity. Default value: 1024	HW/VE	No
MIX_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES adjusts the line rate of HD Video Switching conferences from 1920 Kbps to 17897, 100bits/sec. This matches the actual rate of the HD Video Switching conference running on the MGC. **Note:** If the flag value is YES, the IP_ENVIRONMENT_LINK flag value must be NO. Possible values: YES/NO	HW/VE	Yes
MMCU_BLOCK_TR_ABORTED	When set to NO, enables the MMCU recovery mechanism, otherwise disables the MMCU recovery. Default value: NO (recommended) Possible values: YES/NO	HW/VE	Yes
MS_AV_MCU_MONITORING	You can control the system behavior by adding this flag and setting its value accordingly.		
MS_CAC_AUDIO_MIN_BR	Provides the minimum audio bit rate using the Microsoft CAC (Call Admission Control) protocol. When the bit rate is lower than the flag value, the call fails to connect. Default value: 30 Possible values: 0 - 384	HW/VE	Yes

Flag Name	Description	Platform	Add?
MS_CAC_VIDEO_MIN_BR	The minimum bit rate for video using the Microsoft CAC protocol. When the bit rate is lower than the MS_CAC_VIDEO_MIN_BR, the call fails to connect as a video call. Default value: 40 Range: 0 - 384	HW/VE	Yes
MS_ENVIRONMENT	When set to YES, the RealPresence Collaboration Server SIP environment integrates with Microsoft OCS solution. Default value: NO Possible values: YES/NO	HW/VE	No
MS_KEEP_ALIVE_ENABLE	Enables the Microsoft Keep Alive flag. Set this flag to YES to ensure the connection of the endpoints to the conference until the configuration of RealPresence Collaboration Server with FQDN address and Microsoft Lync server works with load balancing and holds more than one address. Default value: NO Possible values: YES/NO **Note:** Now use the following system flags to get the functionality of this flag: • SIP_TCP_KEEP_ALIVE_TYPE • SIP_TCP_KEEP_ALIVE_BEHAVIOR	VE	Yes
MS_PROXY_REPLACE	Enables the proxy=replace parameter in the SIP Header. Set this flag to YES so that the outbound proxy replaces the contact information in the header. It also enables other clients and servers to reach the client using the proxy's IP address, irrespective of their firewall settings. Default value: YES Possible Values: YES/NO	HW/VE	Yes
MSFT_AVMCU_MUTE_AUDIENCE_TRIGGERS_MUTE_ALL_BUT_ME_IN_RMX_CONFERENCE	In an AVMCU call, the originator can selectively mute all participants or only mute the Skype for Business participants. Default value: YES Possible Values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
MTU_SIZE	Determines the maximum packet size created by the encoder. Default value: 1120 Range: 400 - 1440	HW/VE	Yes
NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT	Indicates the number of times an endpoint receives a Hello message from the server. This occurs in an environment that includes a Session Border Controller (SBC) with a 3-second interval between messages. Default value: 3 Range: 1 -10	HW/VE	Yes
NUMBER_OF_REDIAL	Enter the number of redialing attempts. Dialing might continue until the conference ends. Default value: 3	HW/VE	Yes
NUMERIC_CONF_ID_LEN	Defines the number of digits in the Conference ID that the MCU assigns. Enter 0 to disable the automatic assignment of IDs by the MCU and let the RealPresence Collaboration Server user manually assign them. Default value: 4 Range: 2-16	HW/VE	No
NUMERIC_CONF_ID_MAX_LEN	The maximum number of digits that a user can enter when manually assigning an ID to a conference. Default value: 8 Range: 2-16 **Note:** Selecting 2, limits the number of simultaneous ongoing conferences to 99.	HW/VE	No
NUMERIC_CONF_ID_MIN_LEN	The minimum number of digits that a user must enter when manually assigning an ID to a conference. Default value: 4 Range: 2-16 **Note:** Selecting 2, limits the number of simultaneous ongoing conferences to 99.	HW/VE	No

Flag Name	Description	Platform	Add?
OCSP_RESPONDER_TIMEOUT	Determines the number of seconds the server waits for an OCSP response from the OCSP Responder before the timeout. Network latency or slow WAN links can cause login problems when logging in to the management network of the RealPresence Collaboration Server. Default value: 3 seconds Range: 1-20 seconds **Note:** Not supported in RealPresence Collaboration Server 1800.	HW/VE	Yes
OVERRIDE_MUTE_ALL	When set to YES, the participants can unmute themselves by entering the DTMF code 123 regardless of who mutes them. Default value: NO Possible Values: YES/NO If the chairperson dials *5 and any endpoint dials the configured override mute all DTMF, the override DTMF continues to function without the need of this flag.	HW/VE	Yes
PAL_NTSC_VIDEO_OUTPUT	When set to AUTO, the video output sent by the RealPresence Collaboration Server is either PAL/ NTSC format, depending on the current speaker in the layout. This ensures full synchronization between the frame rate of the speaker and the video encoder, ensuring smoother video. Default value: AUTO Possible values: AUTO, PAL, NTSC	HW/VE	No
PARTY_GATHERING_DURATION_SECONDS	This flag determines the duration of the Gathering slide for participants connecting to the conference after its Start Time. Default values: 15 seconds Range: 0 - 3600 seconds	HW/VE	Yes
PCM_LANGUAGE	Determines the language of the PCM interface. Range: ENGLISH, CHINESE_SIMPLIFIED, CHINESE_TRADITIONAL, JAPANESE, GERMAN, FRENCH, SPANISH, KOREAN, PORTUGUESE, ITALIAN, RUSSIAN, NORWEGIAN Default value: The current RMX Web Client language.	HW/VE	Yes

Flag Name	Description	Platform	Add?
POLYCOM_EPS_DISPLAY_NAME_PREFIX_IN_LYNC_ROSTER	Determines the prefix of the RealPresence Collaboration Server participant names in Microsoft Lync conference roster. Default: Polycom/	HW/VE	Yes
PORT_GAUGE_ALARM	Setting the flag YES, if the system resource usage reaches the defined High Port Usage Threshold for the Port Gauges, it generates System Alerts in the form of an Active Alarm and an SNMP trap. Possible values: YES/NO	HW/VE	Yes
PRESENTATION_INDICATOR_ENABLED	This flag enables the Presentation Indicator feature. The Presentation Indicator feature displays a notification using the Message Overlay functionality to the participants in a Polycom RealConnect conference. This indicates certain restrictions pertaining to the presentation and viewing of content. Default value: NO Possible values: YES/NO	HW/VE	
PRESENTATION_INDICATOR_NUM_OF_REPETITIONS	This flag controls the number of times the Presentation Indicator text message overlay repeats on the Polycom RealConnect conference participants' video display. Default value: 20 Possible values: 1-90	HW/VE	
PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE	Setting the flag to NO (default), closes the ICE channel after applying CAC bandwidth management if CAC is active in the local network. When set to YES, the ICE channel remains open throughout the call. Default value: NO Possible values: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
PRESERVE_PARTY_CELL_ON_FORCE_LAYOUT	Use this flag to prevent reassignment of cells in a forced layout for endpoints that: • Disconnect from the conference. • Pause their video. • Are removed from a conference.. The cell remains black until: • The endpoints reconnect. • The endpoints use a new layout. • The conference ends. Range: YES/NO Default: NO • NO - Reassign the cells of dropped endpoints. The conference treats endpoints that reconnect as new endpoints. • YES - No reassignment of cells of dropped endpoints, but are on reserve until the endpoints reconnect. Forced Layout Guidelines: • If you want to use the RealPresence Collaboration Server primarily for ITP conferences with MLA, set the value of this flag to YES. • Sending a new forced layout to the MCU, the MCU no longer preserves the cells for disconnected participants. The layout is redrawn using the currently connected participants only. • If the dropped endpoint was forced to use a particular cell, and that cell switches from the forced layout to automatically assigned, the MCU no longer preserves the cell. Any other endpoint can be assigned to that particular cell. • This feature works the same way in Telepresence conferences, even where the MLA controls the layouts.	HW/VE	Yes
PSTN_RINGING_DURATION_SECONDS	If there's a slow response from the ISDN-video switch, the RealPresence Collaboration Server uses the ISDN-voice dial-out ringing duration (in seconds) to disconnect the call. Default value: 45	HW	Yes

Flag Name	Description	Platform	Add?
QOS_IP_AUDIO	Used to select the Diffserv priority of audio packets when DiffServ is the selected method for packet priority encoding. For any given DSCP level, set the flag to the full 8-bit hexadecimal value of the DS/TOS byte, which contains the DSCP level as its upper six bits. For example, assuming that it requires a DSCP level of 34 decimal: the binary representation of 34 is 0b100010, and placing it into the upper six bits of the DS/TOS byte, becomes 0b[100010]00, or 0b1000 1000 = 0x88 hex. Thus, set the flag value equal to 0x88. Default value: 0x30	HW/VE	Yes
QOS_IP_VIDEO	Used to select the Diffserv priority of video packets when DiffServ is the selected method for packet priority encoding. For any given DSCP level, set the flag to the full 8-bit hexadecimal value of the DS/TOS byte, which contains the DSCP level as its upper six bits. For example, assuming that it requires a DSCP level of 34 decimal: the binary representation of 34 is 0b100010 and placing it into the upper six bits of the DS/TOS byte, becomes 0b[100010]00, or 0b1000 1000 = 0x88 hex. Thus, set the flag value to 0x88. Default value: 0x30	HW/VE	Yes
QOS_MANAGEMENT_NETWORK	Enter the DSCP value for RealPresence Collaboration Server Management Network. Default value: 0x10 Range: 0x00 - 0x3F	HW/VE	Yes
REALLOC_UPDATE_SCM	Set the system flag to YES in case that RealPresence Collaboration Server increasing video resource consumption during the reallocation. For example, after hold and resume, increasing video resource consumption can lead to lose the video connection. Default value: NO Possible Value: YES/NO **Note:** Requires MCU reset.	HW/VE	Yes

Flag Name	Description	Platform	Add?
REDIAL_INTERVAL_IN_SECONDS	Enter the number of seconds that the RealPresence Collaboration Server should wait before successive redialing attempts. Default value: 10 Range: 0-30	HW/VE	Yes
REDUCE_CAPS_FOR_REDCOM_SIP	When the flag value is YES, the SDP size is less than 2 Kb and includes one audio and one video media line. This accommodates Redcom's SDP size limit. Default value: NO Possible values: YES/NO	HW/VE	Yes
REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME	When set to YES, the server rejects the call if the precedence domain of a SIP dial-in call doesn't match the precedence domain of the server. Default value: No Possible values: YES/NO	HW/VE	Yes
REMOVE_EP_FROM_LAYOUT_ON_NO_VIDEO_TIMER	Enables the removal of empty video cells from a video layout. Default value: 20 Range: • 0 - 19 (seconds): Disables the feature. • 20 - 300 (seconds): Enables the feature.	HW/VE	Yes
REMOVE_H323_EPC_CAP_TO_NON_POLYCOM_VENDOR	Used to disable EPC protocol. Use of Polycom's proprietary protocol, High Profile, EPC, might result in interoperability issues when used with other vendors' endpoints. Default value: NO Possible values: YES/NO	HW/VE	Yes
REMOVE_H323_HIGH_PROFILE_CAP_TO_NON_POLYCOM_VENDOR	Used to disable a high profile protocol. Use of Polycom's proprietary protocol, High Profile, might result in interoperability issues when used with other vendors' endpoints. Default value: NO Possible values: YES/NO	HW/VE	Yes
REMOVE_H323_HIGH_QUALITY_AUDIO_CAP_TO_NON_POLYCOM_VENDOR	Used to disable audio codecs G231, G7221C, G7221, G719, Siren 22, and Polycom® Siren™ 14. Default value: NO Possible values:YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
REMOVE_H323_LPR_CAP_TO_NON_POLYCOM_VENDOR	Used to disable H.323 Polycom Lost Packet Recovery (LPR) protocol. Use of Polycom's proprietary protocol, H.323 Polycom Lost Packet Recovery (LPR), might result in interoperability issues when used with other vendors' endpoints. Default value:NO Possible values:YES/NO	HW/VE	Yes
REMOVE_IP_IF_NUMBER_EXISTS	Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. This flag determines whether to substitute the E.164 number for the IP address in the dial string. Default value: YES - E.164 substitutes the IP address. Possible values: YES/NO	HW/VE	Yes
RESTRICT_CONTENT_BROADCAST_TO_LECTURER	When set to YES, only the conference lecturer may send content to the conference. When set to NO, any conference participant can send content. Default value: YES Possible value: YES/NO	HW/VE	No
RFC2833_DTMF	Controls the receipt of in-band and out-of-band DTMF Codes. When set to: • YES: RealPresence Collaboration Server receives DTMF Codes sent in-band. • NO: RealPresence Collaboration Server receives DTMF Codes sent out-of-band. The RealPresence Collaboration Server always sends DTMF codes in-band (as part of the audio media stream, but not as RTP events). Default value: YES Possible values: YES/NO	HW/VE	Yes
RMX2000_RTM_LAN	Used after installation on and RTM-LAN card to activate the card. Set the flag to YES (RealPresence Collaboration Server 2000). Possible values: YES/NO	HW	No

Flag Name	Description	Platform	Add?
RRQ_WITHOUT_GRQ	To enable registration, some gatekeepers require sending first RRQ and not GRQ. Set the flag to YES, if the gatekeeper requires this behavior in your environment. Gatekeeper Request (GRQ) - Gatekeeper discovery is the process an endpoint uses to determine which gatekeeper to register with. Registration Request (RRQ) - Registration request sent to the gatekeeper. Default: NO Possible values: YES/NO	HW/VE	No
RTCP_FIR_ENABLE	When set to YES, it sends the Full Intra Request (FIR) as INFO (and not RTCP). Default = YES Possible values: YES/NO	HW/VE	Yes
RTCP_FLOW_CONTROL_TMMBR_ENABLE	Enables or disables the SIP RTCP flow control parameter. Default: YES Possible values: YES/NO	HW/VE	Yes
RTCP_FLOW_CONTROL_TMMBR_INTERVAL	Modifies the interval (in seconds) of the TMMBR (Temporary Maximum Media Stream Bit Rate) parameter for SIP RTCP flow control. Default value: 180 Range: 5 - 999 (seconds)	HW/VE	Yes
RTCP_PLI_ENABLE	When set to YES, it sends the Picture Loss Indication (PLI) as INFO (and not RTCP). Default value= YES Possible values: YES/NO	HW/VE	Yes
RTCP_QOS_IS_EQUAL_TO_RTP	Default value: YES Range: YES/NO	HW/VE	Yes
RTV_MAX_BIT_RATE_FOR_FORCE_CIF_PARTICIPANT	Enables the removal of empty video cells from a Video Layout.	HW/VE	Yes

Flag Name	Description	Platform	Add?
SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD	Setting the flag to YES, causes the server to send a busy notification to a SIP audio endpoint or a device which is dialing in to the server and whose audio resource usage exceeds the Port Usage threshold. Setting this flag to NO, causes the system to limit the SIP audio endpoint connections to a certain capacity and not send a busy notification when the resource capacity threshold exceeds. Default value: NO Possible value: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
SEND_SRTP_MKI	Enables or disables the inclusion of the MKI field in SRTP packets sent by RealPresence Collaboration Server. Set the value to NO to disable the inclusion of the MKI field in SRTP packets sent by the RealPresence Collaboration Server. Set this flag to: • NO ◦ When all conferences on the server don't have Microsoft Lync clients participating and have third party endpoints participating. ◦ When using endpoints that can't decrypt SRTP-based audio and video streams if the these packets include MKI (Master Key Identifier) field. We recommend this setting for Maximum Security Environments. • YES ◦ When any conferences on the RealPresence Collaboration Server have both Microsoft Lync clients and Polycom endpoints participating. ◦ Some third-party endpoints are unsuccessful in participating in conferences with this setting. **Note:** • Add this system flag with value YES (default) when using Microsoft Office Communicator and Lync clients as they all support SRTP with MKI. • Add this system flag with value NO when using Siemens phones (Openstage and ODC WE) in the environment as they don't support SRTP with MKI. • Polycom endpoints function normally regardless of the setting of this flag. Default value: YES Possible value: YES/NO	HW/VE	Yes

Flag Name	Description	Platform	Add?
SEND_WIDE_RES_TO_IP	When set to YES (default), the RealPresence Collaboration Server sends widescreen resolution to IP endpoints. The server identifies endpoint types that don't support widescreen resolutions according to their product type and version and won't receive the wide resolution even when the flag value is YES. When manually added with value NO, the RealPresence Collaboration Server doesn't send widescreen resolution to all IP endpoints. Default value: YES	HW/VE	Yes
SEND_WIDE_RES_TO_ISDN	When set to YES, the RealPresence Collaboration Server sends widescreen resolution to ISDN-video endpoints. When set to NO (default), the RealPresence Collaboration Server doesn't send widescreen resolution to ISDN-video endpoints. Default value: NO Possible value: YES/NO	HW	Yes
SET_AUDIO_CLARITY	Polycom Audio Clarity technology improves received audio from participants connected through low audio bandwidth connections, by stretching the fidelity of the narrow-band telephone connection to improve call clarity. The enhancement is applied to the following low bandwidth (4 kHz) audio algorithms: • G.729a • G.711 **Note:** This flag sets the initial value for Polycom Audio Clarity during First-time Power-up. Thereafter, control the feature through the **Profile Properties** > **Audio Settings** dialog box. Default value: OFF Possible Values: ON/OFF	HW/VE	Yes

Flag Name	Description	Platform	Add?
SET_AUDIO_PLC	Packet Loss Concealment (PLC) for Siren audio algorithms improves received audio when packet loss occurs in the network. Supports the following audio algorithms: • Siren 7 (mono) • Siren 14 (mono/stereo) • Siren 22 (mono/stereo) Possible Values: ON/OFF Default value: ON **Note:** The speaker's endpoint must use a Siren algorithm for audio compression.	HW/VE	Yes
SET_AUTO_BRIGHTNESS	Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. Auto Brightness only increases brightness and doesn't darken video windows. **Note:** This flag sets the initial value for Auto Brightness during First-time Power-up. Thereafter the feature is controlled through the **New Profile - Video Quality** dialog box. Default value: NO Possible Values: YES/NO	HW/VE	Yes
SET_DTMF_SOURCE_DIFF_IN_SEC	If the ACCEPT_VOIP_DTMF_TYPE flag value is 0 (Auto) this flag determines the interval, in seconds after which the RealPresence Collaboration Server accepts both DTMF tones (inband) and digits (outband). Default value: 120	HW/VE	Yes

Flag Name	Description	Platform	Add?
SIP_AUTO_SUFFIX_EXTENSION	Used to automatically add a suffix to a SIP address (To Address) instead of adding it manually in the RMX Web Client (SIP address) when the SIP call is direct-dial and not through a Proxy. Example: Participant Name = john.smith Company Domain = maincorp.com SIP_AUTO_SUFFIX_EXTENSION flag value = @maincorp.com Entering john.smith generates a SIP URI = john.smith@maincorp.com	HW/VE	No
SIP_ENABLE_FECC	By default, enable FECC support for SIP endpoints at the MCU level. You can disable it by manually adding this flag and setting it to NO. Possible values: YES/NO.	HW/VE	Yes
SIP_FAST_UPDATE_INTERVAL_ENV	The default setting is 0 to prevent the RealPresence Collaboration Server from automatically sending an Intra request to all SIP endpoints. Enter n (where n is any number of seconds other than 0) to let the RealPresence Collaboration Server automatically send an Intra request to all SIP endpoints every n seconds. We recommend to set the flag to 0 and modify the frequency in which it sends the request at the endpoint level (as defined in the next flag).	HW/VE	Yes
SIP_FAST_UPDATE_INTERVAL_EP	The default setting is 6 to let the RealPresence Collaboration Server automatically send an Intra request to Microsoft OC endpoints only, every 6 seconds. Enter any other number of seconds to change the frequency in which the RealPresence Collaboration Server sends the Intra request to Microsoft OC endpoints only. Default value: 6 seconds	HW/VE	Yes

Flag Name	Description	Platform	Add?
SIP_FORMAT_GW_HEADERS_FOR_REDCOM	Controls whether the RealPresence Collaboration Server adds a special gateway prefix and postfix characters to your portion of the SIP URI expressed in the From and Contact headers of SIP messages sent during calls involving Gateway Services. The addition of these characters can result in call failures with some SIP call servers. We recommend to set this flag to YES whenever the RealPresence Collaboration Server is deployed such that it registers its conferences to a SIP call server. Default value: NO Possible value: YES/NO	HW/VE	Yes
SIP_FREE_VIDEO_RESOURCES	For use in Avaya and Microsoft Environments. When set to NO, it maintains allocation of video resources to participants as long as they're connected to the conference, even if the call was changed to audio only. The system allocates the resources according to the participant's endpoint capabilities, with a minimum of 1 CIF video resource. Enter YES to enable the system to free the video resources for allocation to other conference participants. The call becomes an audio only call and video resources aren't guaranteed to participants if they want to add video again. Default value in Microsoft environment: NO Possible values: YES/NO	HW/VE	Yes
SIP_OMIT_DOMAIN_FROM_PARTY_NAME	Removes domain names from SIP dial-in participants' site names. This prevents long domain names from being appended to SIP participant names. Default value: YES (Omits the domain name from SIP dial-in participant names) Possible values: YES/NO (NO - The domain name remains as part of SIP dial-in participant names)	HW/VE	Yes

Flag Name	Description	Platform	Add?
SIP_TCP_PORT_ADDR_STRATEGY	Setting the flag to 1, prevents the use of two sockets for one SIP call - one for inbound traffic, one for outbound traffic. This is done by inserting port 5060/5061 into the Route[0] header. Default value: 0 Possible values: • 0 - Inbound traffic on port 5060/5061 outbound traffic on port 60000 • 1 - Both inbound and outbound traffic on port 5060/5061	HW/VE	Yes
SOCKET_ACTIVITY_TIMEOUT	For use in Microsoft environments. When the MS_KEEP_ALIVE System Flag value is YES, the MS Keep-Alive Timer value uses the value of this flag.	HW/VE	Yes
STAR_DELIMITER_ALLOWED	When set to YES, an asterisk "*" can be used as a delimiter in the conference and meeting room dial strings. The dial string is first searched for "#" first followed by "*". Default value: NO Possible value: YES/NO	HW/VE	No
SUPPORT_HIGH_PROFILE	Enables or disables the support of High Profile video protocol in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Default value: YES Possible value: YES/NO	HW/VE	Yes
SUPPORT_HIGH_PROFILE_WITH_ISDN	Enables or disables the support of High Profile video protocol for ISDN-video participants in CP Only conferences. Default value: NO Possible value: YES/NO	HW	Yes
SUPPORT_MULTIPLE_ICE_USERS	Enables the configuration of multiple Microsoft Lync registrations.	HW	Yes

Flag Name	Description	Platform	Add?
SYSTEM_BROADCAST_VOLUME	If the system flag FORCE_SYSTEM_BROADCAST_VOLUME value is YES, use this value. Determines the default audio level with which the participants connect and send audio to the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Range: 1-10 Default value: 5	HW/VE	No
SYSTEM_LISTENING_VOLUME	If the system flag FORCE_SYSTEM_LISTENING_VOLUME value is YES, use this value. Determines the default audio level with which the participants connect and receive audio from the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Default value: 5 Range: 1-10	HW/VE	No
TC_BURST_SIZE	Regulates the traffic control buffer or max burst size as a percentage of the participant line rate. Range: 1-30	HW/VE	Yes
TC_LATENCY_SIZE	Limits the latency or the number of bytes that can be present in a queue. Range: 1-1000 (in milliseconds)	HW/VE	Yes
TCP_RETRANSMISSION_TIMEOUT	The number of seconds the server waits for a TCP client to answer a call before closing the connection. Default value: 5 seconds	HW/VE	Yes
TERMINATE_CONF_AFTER_CHAIR_DROPPED	Indicates that the chairperson has left the conference. **Note:** Enable the flag to play this message.		

Flag Name	Description	Platform	Add?
TIMEOUT_BETWEEN_IVR_AND_FIRST_DIGIT	The timeout between IVR message and DTMF input. Default value: 99 (seconds) Range: 0, 1-10, 99 **Note:** Configuring it to 99, the timeout is identical to the existing timeout value set through Timeout for User Input parameter.	HW/VE	Yes
USE_GK_PREFIX_FOR_PSTN_CALLS	When set to YES, the gatekeeper prefix is included in the DTMF input string enabling ISDN-voice participants to use the same when connecting to RealPresence Collaboration Server. Applicable for RealPresence Collaboration Server as a standalone MCU or as part of a Poly Clariti solution deployment. Default value: NO Possible Values: YES/NO	HW/VE	No
V35_MULTIPLE_SERVICES	Set this flag to YES if it requires the connection of multiple Serial Gateways to RTM-LAN cards. The default value of this system flag is NO, enabling only one Serial Gateway to be supported per RTM-LAN card. Possible values: YES/NO **Note:** Not Supported in RMX 1800.	HW/VE	Yes
V35_ULTRA_SECURED_SUPPORT	When deploying a Serial Gateway S4GW, set this flag to YES. This flag is applicable regardless of the security mode. Possible values: YES/NO	HW	Yes
VIDEO_BIT_RATE_REDUCTION_PERCENT	Indicates the percentage of actual reduction in bit rate sent from the RealPresence Collaboration Server to the endpoint (negotiated bit rate isn't reduced). This flag is applicable only when traffic shaping is active. Default value: 15 Range: 0-60	HW/VE	Yes

Flag Name	Description	Platform	Add?
VIDEO_ENCODER_CHANGE_LAYOUT_REQ	This flag contains a new parameter IsLyncVideoMuted and can take the following values: • 0 - To not display any doughboy image for the Microsoft Lync participants. • 1 - To display doughboy image for the Microsoft Lync participants.		
VSW_RATE_TOLERANCE_PERECENT	Determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference. For example, a value of 20 allows a participant to connect to the conference if the line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). Default value: 0 Range: 0 - 75	HW	Yes
WAITING_IN_LOBBY_DURATION	Defines the number of seconds users wait in the secure meeting lobby before RealPresence Collaboration Server disconnects them. Range: 60-300	HW/VE	Yes
WAITING_IN_LOBBY_MESSAGE_OVERLAY_REPETITIONS	Defines the number of times the secure meeting lobby notification displays to chairpersons in a locked conference. Range: 1-10	HW/VE	Yes
WRONG_NUMBER_DIAL_RETRIES	The number of redial attempts for a wrong destination number or a wrong destination number time-out. Default value: 3 Range: 0 - 5 A flag value of 0 means that no redials are attempted.	HW/VE	Yes

802.1x Authentication System Flags

Flag Name	Description
802_1X_CERTIFICATE_MODE	Determines whether one TLS certificate is retrieved from the Certificate Repository for all IP services or if it retrieves multiple certificates, one for each IP service. Default value: ONE_CERTIFICATE Possible values: ONE_CERTIFICATE, MULTIPLE_CERTIFICATE

Flag Name	Description
802_1X_CRL_MODE	If the flag value is: • ENABLED - Forces CRL checking. The system fails the connection request if the certificate has been revoked or if there's no CRL. • OPTIONAL - The system fails the connection request if the certificate is revoked but doesn't fail the connection request if there's no CRL. • DISABLED - Doesn't check the CRL and doesn't fail the connection request based on the CRL content. Default value: DISABLED Possible values: ENABLED, OPTIONAL, DISABLED
802_1X_SKIP_CERTIFICATE_VALIDATION	If the flag value is: • YES - The retrieved certificate isn't validated against the CA certificate. • NO - The retrieved certificate is validated against the CA certificate. Validation failure raises an Active Alarm and is reported in the Ethernet Monitoring dialog box. Default value: YES Possible values: YES/NO
802_FIPS_MODE	When set to YES, the availability of the MD5 Authentication Protocol is not displayed as a selectable option or supported. Default value: NO Default value Ultra Secure Mode: YES Possible values: YES/NO

Alternative Network Address Translation System Flag

Flag Name	Description
ANAT_IP_PROTOCOL	When set to YES enables Alternative Network Address Types (ANAT). Default value: • ULTRA SECURE MODE: NO • STANDARD SECURITY MODE: YES Range: DISABLED, AUTO, PREFER_IPv4, PREFER_IPv6

AS-SIP Content System Flag

Flag Name	Description
AS_SIP_CONTENT_TIMER	Controls the time that the RealPresence Collaboration Server waits for endpoints to respond to its SDP Reinvite that is determined by a timer. Default value: 10 seconds Range: 1-60 seconds (it rejects values outside this range and displays an error message).

CS System Flags

Flag Name	Description
CS_ENABLE_EPC	When set to YES enables endpoints that support People+Content and require a different signaling (for example, FX endpoints) to receive Content. Default value: NO Possible value: YES/NO
H245_TUNNELING	For use in the Avaya Environment. In the Avaya Environment, set the flag to YES to ensure that H.245 is tunneled through H.225. Both H.245 and H.225 use the same signaling port. Default value: NO Possible value: YES/NO
H323_RAS_IPV6	Configuring the RealPresence Collaboration Server for IPv4 & IPv6 addressing, RAS (Registration, Admission, and Status) sends the messages in both IPv4 and IPv6 format. If the gatekeeper can't operate in IPv6 addressing mode, registration fails and endpoints can't connect using the RealPresence Collaboration Server prefix. In such cases, set this system flag to NO. Default value: YES Possible value: YES/NO
H323_TIMERS_SET_INDEX	Enables or disables H.323 index timer according to standard or proprietary H.323 protocol. Default value: 0 Possible values: • 0 (Default) - Sets the H.323 index timer to Polycom proprietary. • 1 - Sets the H.323 index timer based on the H.323 Standard recommendation. **Note:** For homologation and certification testing, set this flag to 1.

Flag Name	Description
MS_UPDATE_CONTACT_REMOVE	When the flag value is: • YES - It removes the Contact Header from the UPDATE message that the endpoints receive periodically. Use this when the SIP Server Type field of the IP Network Service value is Microsoft. OCS R2 requires the removal of the Contact Header from the UPDATE message. • NO - The Contact Header is included in the UPDATE message. This is the system behavior when the SIP Server Type value is Generic. Use this after configuring the RealPresence Collaboration Server to accept calls from both Microsoft Lync and Cisco CUCM as CUCM requires the Contact Header. Possible values: YES/NO
QOS_IP_SIGNALING	Use this flag to select the Diffserv priority of signaling packets when packet priority encoding uses the DiffServ method. For any given DSCP level, set the flag to the full 8-bit hexadecimal value of the DS/TOS byte, which contains the DSCP level as its upper six bits. For example, assuming that a DSCP level of 34 decimal is required: the binary representation of 34 is 0b100010, which, when placed into the upper six bits of the DS/TOS byte, becomes 0b[100010]00, or 0b1000 1000 = 0x88 hex. Thus, set the flag value to 0x88. Default value: 0xA0
SIP_DUAL_DIRECTION_TCP_CON	For use in Microsoft environments. When set to YES, sends a new request on the same TCP connection instead of opening a new connection. Default value: NO
SIP_ST_ENFORCE_VAL	For use in Microsoft environments. Session timer interval in seconds. Default value= YES
SIP_TCP_TLS_TIMERS	Determines the timeout characteristics of SIP TCP TLS connections. Format: SIP_TCP_TLS_TIMERS = <string> The string contains the following parameters: Ct - Timeout of TCP CONNECT operation (seconds) Cs - Timeout of TLS CONNECT operation (seconds) A - Timeout of accept operation (seconds) D - Timeout of disconnect operation (nanoseconds) H - Timeout of handshake operation (seconds) Default value: <1,5, 4,500000,5>

Flag Name	Description
SIP_TIMERS_SET_INDEX	SIP Timer type timeout settings according to standard or proprietary protocol. Default value: 0 Possible values: 0, 1 (SIP Standard recommendation) **Note:** For homologation and certification testing, set this flag to 1.
SIP_TO_TAG_CONFLICT	For use in Microsoft environments. In case of forking, it resolves a tag conflict when it receives a Status 200 OK from an answering UA. Default value: YES Possible: YES/NO

Content Related System Flags

Flag Name	Description
CS_ENABLE_EPC	Endpoints supporting People+Content (for example, FX endpoints) might require a different signaling when in content mode. For these endpoints, manually add this flag with the value YES (default value is NO) to the CS_MODULE_PARAMETERS tab. Default value: NO Possible values: YES/NO
LEGACY_EP_CONTENT_DEFAULT_LAYOUT	Defines the video layout used in legacy endpoint when switching to Content mode.

Password Generation Flags

Flag Name	Description
FORCE_STRONG_PASSWORD_POLICY	When set to YES, this flag implements Strong Password rules. Default value: NO Default value in ULTRA_SECURE_MODE=YES Possible values: YES/NO

Flag Name	Description
HIDE_CONFERENCE_PASSWORD	NO (default) - Conference and chairperson passwords are displayed when viewing the Conference/Meeting Room/ Reservation properties. It also enables the automatic generation of passwords in general. YES - Conference and chairperson Passwords are hidden (they are replaced by asterisks). It also disables the automatic generation of passwords. Default value: NO Possible values: YES/NO
HIDE_CONFERENCE_PASSWORD	When set to YES (default in Ultra Secure Mode): • It hides conference and chairperson passwords present in the RMX Web Client or RMX Manager when viewing the properties of the conference. • It disables automatic generation of passwords (both conference and chairperson passwords), regardless of the settings of the flags: ◦ NUMERIC_CONF_PASS_DEFAULT_LEN ◦ NUMERIC_CHAIR_PASS_DEFAULT_LEN Default value: NO
MAX_CONF_PASSWORD_REPEATED_DIGITS	Allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password. Default value: 2 Range: 1 - 4
MAX_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a user password. Default value: 2 Range: 1 - 4
MIN_PASSWORD_LENGTH	The length of passwords. Possible values: between 0 and 20. 0 means that this rule isn't enforced.
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	Defines the frequency with which a user can change a password. Default value: 0 - users don't have to change their passwords. Range: Values: 0 -7
NUM_OF_LOWER_CASE_ALPHABETIC	The minimum number of lowercase alphabetic characters required in a login password in Ultra Secure Mode. Default value: 0

Flag Name	Description
NUM_OF_NUMERIC	The minimum number of numeric characters required in a login password in Ultra Secure Mode. Default value: 0
NUM_OF_SPECIAL_CHAR	The minimum number of special characters (asterisks, brackets, periods, etc.) required in a login password in Ultra Secure Mode. Default value: 0
NUM_OF_UPPER_CASE_ALPHABETIC	The minimum number of uppercase alphabetic characters required in a login password in Ultra Secure Mode. Default value: 0
NUMERIC_CHAIR_PASS_DEFAULT_LEN	Enables or disables the automatic generation of chairperson passwords and determines the number of digits in the chairperson passwords assigned by the MCU. Possible values are: • 0 disables the automatic password generation in both Standard Security Mode or Ultra Secure Mode. Any value other than 0 enables the automatic generation of chairperson passwords if the flag HIDE_CONFERENCE_PASSWORD value is NO. • 1 - 16, default: 6 (Standard Security Mode) • 9 - 16, default: 9 (Ultra Secure Mode). Using the default, in nonsecure mode the system automatically generates chairperson passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	The maximum number of digits that you can enter when manually assigning a password to the chairperson. Default value: 16 Range: 0 - 16
NUMERIC_CHAIR_PASS_MIN_LEN	Defines the minimum length required for the chairperson password. Default: 0 - This rule isn't enforced. Range: 0-16

Flag Name	Description
NUMERIC_CONF_PASS_DEFAULT_LEN	Enables or disables automatic generation of conference passwords. The flag value determines the length of the automatically generated passwords. Possible values: 0 - 16, where 0 disables automatic generation of passwords. Default: • 6 - In nonsecured mode • 9 - In Ultra Secure Mode Any value other than 0 enables automatic generation of conference passwords provided the flag HIDE_CONFERENCE_PASSWORD value is NO. Using the default, in nonsecure mode the system automatically generates conference passwords that contain 6 characters.
NUMERIC_CONF_PASS_MAX_LEN	Enter the maximum number of characters permitted for conference passwords. Possible values: 0 - 16 Default: 16
NUMERIC_CONF_PASS_MIN_LEN	Enter the minimum number of characters required for conference passwords. Possible values: 0 - 16 0 (default in nonsecured mode) means no minimum length. However when the RealPresence Collaboration Server is in Ultra Secure Mode, this setting cannot be applied. 9 (default in Ultra Secure Mode) Conference password must be at least 9 characters in length.
PASSWORD_EXPIRATION_DAYS	Determines the duration of password validity. Value: between 0 and 90 days. 0 - user passwords don't expire. In Ultra Secure Mode: default - 60 days, the minimum duration is 7 days.
PASSWORD_EXPIRATION_DAYS_MACHINE	Enables the administrator to change the password expiration period of Application-user's independently of regular users. Default: 365 (days)
PASSWORD_EXPIRATION_WARNING_DAYS	Determines the display of a warning of the number of days until password expiration. Value: between 0 and 14 days. 0 - password expiry warnings aren't displayed. In Ultra Secure Mode, the earliest display - 14 days, the latest 7 days (default).

Flag Name	Description
PASSWORD_FAILURE_LIMIT	The number of unsuccessful Logins permitted in Ultra Secure Mode. Default value: 3
PASSWORD_HISTORY_SIZE	The number of passwords that are recorded to prevent users from reusing their previous passwords. Values are between 0 and 16.

.

Ultra Secure Mode System Flags

Flag Name	Description
ULTRA_SECURE_MODE	When set to YES, this flag enables the Ultra Secure Mode. When enabled, affects the ranges and defaults of the System Flags that control: • Network Security • User Management • Strong Passwords • Login and Session Management • Cyclic File Systems alarms Default value: NO Possible values: YES/NO

Internet Control Message Protocol (ICMP) System Flags

Flag Name	Description
ENABLE_ACCEPTING_ICMP_REDIRECT	Enables the administrator to control the ICMP Redirect messages. This is typically used to instruct routers to redirect network traffic through alternate network element (ICMP message type #5). Default value: NO Possible values: YES/NO

Flag Name	Description
ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE	Enables the administrator to control the ICMP Destination Unreachable messages (ICMP message type #3). Default value: • Ultra Secure Mode: NO - Destination Unreachable Message is never sent. • Default Security Mode: YES - It sends Destination Unreachable Message when needed. Possible values: YES/NO

Minimum Threshold Line Rates

Flag Name	Description
VSW_CIF_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for CIF resolution for High Profile-enabled VSW conferences. Default value: 64 Kbps
VSW_HD_1080p_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for HD1080p resolution for High Profile-enabled VSW conferences. Default value: 1024 Kbps
VSW_HD_1080p60_BL_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for HD1080p60 resolution for Base Profile-enabled VSW conferences. Default value: 1728 Kbps
VSW_HD_1080p60_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for HD1080p60 resolution for High Profile-enabled VSW conferences. Default value: 1024 Kbps
VSW_HD_720p30_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for HD720p30 resolution for High Profile-enabled VSW conferences. Default value: 512 Kbps
VSW_HD_720p50-60_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for HD720p50 and HD720p60 resolutions for High Profile-enabled VSW conferences. Default value: 832 Kbps
VSW_SD_HP_THRESHOLD_BITRATE	Controls the Minimum Threshold Line Rate for SD resolution for High Profile-enabled VSW conferences. Default value: 128 Kbps

Encryption Flags

Flag	Description
ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	When set to NO (default), the Recording Link inherits the encryption settings of the conference. Encrypting the conference, also encrypts the recording link. When set to YES, it disables the encryption of the recording link, regardless of the encryption settings of the conference and the Polycom® RealPresence® Media Suite recorder. Default value: NO Possible values: YES/NO
FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE	When set to YES, undefined participants must connect encrypted, otherwise they're disconnected. When set to NO (default) and the conference Encryption Profile value is Encrypt When Possible, both the encrypted and nonencrypted participants can connect to the same conferences. Default value: NO Possible value: YES/NO

Recording Link Encryption Flags

Flag Name	Description
ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	When set to NO (default), the Recording Link inherits the encryption settings of the conference. Encrypting the conference, also encrypts the recording link. When set to YES, this flag disables the encryption of the recording link, regardless of the encryption settings of the conference and the Polycom® RealPresence® Media Suite recorder. Default value: NO Possible value: YES/NO

Modify Resolution Flags

Flag Name	Description
MAX_CP_RESOLUTION	Determines the maximum CP Resolution of the system. Apply the flag value to the system during First Time Power-on and after a system upgrade. Default value: HD1080 Possible values: • HD1080 - High Definition at 60 fps • HD1080 - High Definition at 30 fps • HD720 - High Definition at 60 fps • HD - High Definition at 30 fps • SD30 - Standard Definition at 30 fps • SD15 - Standard Definition at 15 fps • CIF - CIF resolution
MAX_MS_SVC_RESOLUTION	Minimizes the resource usage by overriding the default resolution selection and limiting it to a lower resolution. Operates independently from the MAX_RTV_RESOLUTION system flag allowing differing selection of maximum resolutions for the MS SVC and RTV protocols. Default value: AUTO Possible values: AUTO, CIF, VGA, HD720, HD1080
MAX_RTV_RESOLUTION	Enables you to override the RealPresence Collaboration Server resolution selection and limit it to a lower resolution. This minimizes the resource usage to 1 or 1.5 video resources per call instead of 3 resources. Default value: AUTO Possible values: AUTO, QCIF, CIF, VGA, or HD720
MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD	Prevents low quality and low frame rate video from being sent to endpoints by ensuring that an SD channel isn't opened at frame rates below the specified value. Default value: 15 Range: 0 -30

Cropping Control Flags

Flag Name	Description
CROPPING_PERCENTAGE_THRESHOLD_GENERAL	For nonpanoramic layouts, control cropping, and striping by adding this flag and setting its value accordingly. Default value: -1 Range: 1-100

Flag Name	Description
CROPPING_PERCENTAGE_THRESHOLD_PANORAMIC	For panoramic layouts, control cropping and striping by adding this flag and setting its value accordingly. Default value: -1 Range: 1-100

Controlling Secure Communication System Flags

Flag Name	Description
EXTERNAL_DB_PORT	Applicable to the RealPresence Collaboration Server 2000 or 4000 only. The external database server port used by the RealPresence Collaboration Server to send and receive XML requests/responses. For secure communications set the value to 443. Default value: 5005
RMX_MANAGEMENT_SECURITY_PROTOCOL	Enter the protocol to be used for secure communication. Default value: TLSV1_SSLV3 (both) Default value for U.S. Federal licenses: TLSV1

Controlling Cascade Layout Flags

Flag Name	Description
AVOID_VIDEO_LOOP_BACK_IN_CASCADE	When set to YES, the current speaker's image isn't sent back through the participant link in cascaded conferences with conference layouts other than 1x1. Default value: YES Possible values: YES/NO
FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION	When set to YES, the cascaded link is automatically set to Full Screen (1x1) in CP conferences. This forces the speaker in one cascaded conference to display in full window in the video layout of other conference. Set this flag to NO when connecting to an MGC using cascaded link, if the MGC is functioning as a gateway and participant layouts on the other network aren't to be forced to 1x1. Default value: YES Possible value: YES/NO

Network Quality Icon - Display Customization Flags

Flag Name	Description
CELL_IND_LOCATION	This flag changes the display location of the network quality indicators displayed in the cells of the conference video layout. Default value: TOP_RIGHT Possible values: • BOTTOM_LEFT • BOTTOM_RIGHT • TOP_LEFT • TOP_RIGHT
DISABLE_CELLS_NETWORK_IND	This flag disables the display of network quality indicators displayed in the cells of the conference video layout. Default value: YES Possible values: YES/NO
DISABLE_SELF_NETWORK_IND	This flag disables the display of the network quality indicator of the participant's own endpoint. Default value: NO Possible values: YES/NO **Note:** The **Network Quality** check box in the **Layout Indications** tab of the **New Profile/Profile Properties** dialog box replaces this flag's function.
SELF_IND_LOCATION	Changes the display location of the network quality indicators displayed in participant's endpoint. Default value: BOTTOM_RIGHT Possible values: • TOP_LEFT • TOP • TOP_RIGHT • BOTTOM_LEFT • BOTTOM • BOTTOM_RIGHT **Note:** The **Network Quality** check box in the **Layout Indications** tab of the **New Profile/Profile Properties** dialog box replaces this flag's function.

Traffic Shaping System Flags

Flag Name	Description
ENABLE_RTP_TRAFFIC_SHAPING	Indicates whether traffic shaping, which is responsible for flattening packet bursts within 100 msec time intervals, is active. When set to YES, traffic shaping is applied to all ports, resulting in some port capacity reduction in MCUs with MPMRx cards. Setting the value to NO, disables traffic shaping. Default value: NO Possible values: YES/NO
TRAFFIC_SHAPING_MTU_FACTOR	Used for the MTU (Maximum transmitting Unit - the size of transmitted packets) dynamic calculation: New MTU = video bit rate/ TRAFFIC_SHAPING_MTU_FACTOR Where the new MTU value is guaranteed to be a minimum of 410, and a maximum of 1460 (MAX_MTU). The purpose of this calculation is to match video rate in outgoing video to call rate, yet force lower encoder bit rates to avoid overflow. This flag is applicable only when traffic shaping is active. Default value: 800 Range: 0-5000, where 0 signifies no change in MTU
VIDEO_BIT_RATE_REDUCTION_PERCENT	Indicates the percentage of actual reduction in bit rate sent from the RealPresence Collaboration Server to the endpoint (negotiated bit rate isn't reduced). This flag is applicable only when traffic shaping is active. Default value: 15 Range: 0-60

PCM_FECC System Flag

Flag Name	Description
PCM_FECC	Determines whether the DTMF Code, ##, the Arrow Keys (FECC), or both activate the PCM interface. In addition, use this flag to disable the PCM. Default value: YES Possible Values: YES/NO

Network Quality Icon - Indication Threshold Flags

Flag Name	Description
NETWORK_IND_CRITICAL_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from Major to Critical. Default value: 5
NETWORK_IND_MAJOR_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from Normal to Major. Default value: 1

Gathering Phase Duration System Flag

Flag Name	Description
CONF_GATHERING_DURATION_SECONDS	Sets the Gathering Phase duration of the conference and is measured from the scheduled start time of the conference. For participants who connect before start time, it displays the Gathering slide from the time of connection until the end of the Gathering duration. Default value: 180 seconds Range: 0 - 3600 seconds

Content Connection Flags

Flag Name	Description
CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS	Controls the other participants request to refresh (intra) the content from the RealPresence Collaboration Server to the content sender. Enter the interval in seconds between the Intra requests sent from RealPresence Collaboration Server to the endpoint sending the content to refresh the content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval. Default value: 5
MAX_INTRA_REQUESTS_PER_INTERVAL_CONTENT	Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the RealPresence Collaboration Server. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended. Default value: 3

Flag Name	Description
MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_CONTENT	Enter the duration in seconds to ignore the participant's requests to refresh the Content display. Default value: 10

H.323 Endpoint Disconnection Detection Flag

Flag Name	Description
DETECT_H323_EP_DISCONNECT_TIMER	This flag controls the timeout used for H.323 endpoint disconnection detection. This flag must be added to the system configuration to view of modify its value. Default value: 20 Range: 16 - 300 (4-second units). Values indivisible by 4 will be rounded upward. Flag values between 0 and 15 disable the flag functionality.

SIP Endpoint Disconnection Detection Flag

Flag Name	Description
DETECT_SIP_EP_DISCONNECT_TIMER	This flag controls the time out used for SIP endpoint disconnection detection, which must be added to the System Configuration to view or modify its value. Default value: 20 Range: 16-300 (4-second units). Values indivisible by 4 will be rounded upward. Flag values between 0 and 15 disable the flag functionality.

User Management Flags

Flag Name	Description
DEFAULT_USER_ALERT	This flag alerts the administrator that the default user (Polycom) exists. Default value: NO Default value (Ultra Secure Mode): YES Possible values: YES/NO
DISABLE_INACTIVE_USER	The system automatically disables the users when not logged on to the RealPresence Collaboration Server application for a predefined period. Default value: 0 (disables this option) Default value (ULTRA_SECURE_MODE=YES): 30 Possible Values: 0 - 90 days

Cyclic File System Flag

Flag Name	Description
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	Enables or disables the display of Active Alarms before overwriting the older CDR/Auditor/Log files, enabling users to backup the older files before they're deleted. Default value: NO Default value (ULTRA_SECURE_MODE=YES): YES

Content Sharing System Flags

Flag Name	Description
SIP_BFCP_DIAL_OUT_MODE	Controls the BFCP's use of UDP and TCP protocols for dial-out SIP client connections according to its value: Default value: AUTO Possible values: • AUTO (Default) If SIP Client supports UDP, TCP, or UDP and TCP: - Select BFCP/UDP as the content sharing protocol. • UDP If SIP Client supports UDP or UDP and TCP: - BFCP/UDP selected as Content sharing protocol. If SIP client supports TCP - Content cannot be shared. • TCP If SIP client supports TCP, or UDP and TCP - BFCP/TCP selected as Content sharing protocol. If SIP client supports UDP, content cannot be shared.

Video Preview System Flag

Flag Name	Description
ENABLE_VIDEO_PREVIEW	Enables the video preview feature. Default value: YES

Network Security System Flags

Flag Name	Description
ICMP_ECHO	

Flag Name	Description
SEPARATE_MANAGEMENT_NETWORK	Enables or disables Network Separation. Can only be disabled in the Ultra Secure Mode. (ULTRA_SECURE_MODE=YES). Default value: NO Possible values: YES/NO
SIP_FIPS_MODE	This flag controls availability of the PFX/PEM Certificate Method. Range: • YES - PFX/PEM isn't available for selection. • NO - PFX/PEM is available for selection. Default value: • Standard Security Mode - NO • Ultra Secure Mode - YES
SNMP_FIPS_MODE	Controls the availability of DES and MD5 Authentication methods. Possible values: • YES - DES and MD5 aren't available for selection. • NO - DES and MD5 are available for selection. Default value: • Standard Security Mode - NO • Ultra Secure Mode - YES

Login and Session Management System Flags

Flag Name	Description
APACHE_KEEP_ALIVE_TIMEOUT	If the connection is idle for longer than the number of seconds specified by this flag, the connection to RealPresence Collaboration Server gets terminated. Default value: 15 Default value (ULTRA_SECURE_MODE=YES): 15 Range: 1 - 999
LAST_LOGIN_ATTEMPTS	When set to YES, the system displays a record of your last login. Default value: NO Possible values: YES/NO

Flag Name	Description
MAX_KEEP_ALIVE_REQUESTS	The number of KeepAliveTimeout request intervals for the Apache server. In a Maximum Security Environment, set this value to 1814400 to ensure that RMX Manager will remain connected for several hours, but not indefinitely. The exact time period depends on the type of client and the number of requests. Default: 0 (Don't use this value **ever** as the connection time is unlimited.) (Configuring the SESSION_TIMEOUT_IN_MINUTES system flag, disconnects the RMX Manager after the specific time, if there's no keyboard or mouse activity.)
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	Defines the maximum number of concurrent management sessions (http and https connections) per system. Default value: 80 Range: 4 - 80
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	Defines the maximum number of concurrent management sessions (http and https connections) per user. Default value: 10 (20 in Ultra Secure Mode) Range: 4 - 80
SESSION_TIMEOUT_IN_MINUTES	The connection to RealPresence Collaboration Server terminates if there's no user input or the connection is idle for longer than the set number of minutes. • If the ULTRA_SECURE_MODE=NO: ◦ Default value: 0 (Feature is inactive) ◦ Range: 0-999 • If the ULTRA_SECURE_MODE=YES: ◦ Default value: 10 ◦ Range: 0-999
USER_LOCKOUT	When set to YES, locks out a user after three consecutive login failures. Only the administrator can enable the user within the system. Default value: NO (in Ultra Secure Mode: YES) Possible values: YES/NO
USER_LOCKOUT_DURATION_IN_MINUTES	Defines the duration of user lockout. 0 means that permanent user lockout until the administrator re-enables the user within the system. Default value: 0 Range: 0 - 480

Flag Name	Description
USER_LOCKOUT_WINDOW_IN_MINUTES	Defines the time period during which the three consecutive login failures occur. 0 means that three consecutive Login failures in any time period will result in User Lockout. Default value: 60 Range: 0 - 45000

Media Redundancy System Flags

Flag Name	Description
LAN_REDUNDANCY	Enables LAN port redundancy on the RealPresence Collaboration Server 2000 or 4000 RTM LAN Card. Default value: NO Possible values: YES/NO **Note:** If the flag value is YES and either of the LAN connections (LAN1 or LAN2) experiences a problem, it displays an active alarm stating that there's no LAN connection. It also specifies both the card and port number.
MULTIPLE_SERVICES	Determines whether the Multiple Services option can be activated once the appropriate license is installed. Default value: NO Possible Values: YES/NO **Note:** Displays an active alarm if the flag value is YES and no RTM ISDN or RTM LAN cards are installed in the RealPresence Collaboration Server.

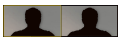
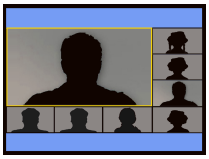
Global Address Book Integration Flags

Flag Name	Description	Platform	Add?
EXTERNAL_CONTENT_DIRECTORY	The Web Server folder name. Change this name if you've changed the default names used by the Poly Clariti Manager application. Default value: /PlcmWebServices	HW/VE	Yes

Flag Name	Description	Platform	Add?
`EXTERNAL_CONTENT_IP`	Enter the IP address of the Poly Clariti Manager server in the format: For example, `http://172.22.185.89` This flag is also a trigger for replacing the internal RealPresence Collaboration Server address book with Poly Clariti Manager global Address Book. When empty, it disables the integration of Poly Clariti Manager address book with RealPresence Collaboration Server.	HW/VE	Yes
`EXTERNAL_CONTENT_PASSWORD`	The password associated with the user name defined for RealPresence Collaboration Server in Poly Clariti Manager server.	HW/VE	Yes
`EXTERNAL_CONTENT_PORT`	The Poly Clariti Manager port used by the RealPresence Collaboration Server to send and receive XML requests/ responses. Default value: `80`	HW/VE	Yes
`EXTERNAL_CONTENT_USER`	The login name defined for the RealPresence Collaboration Server in the Poly Clariti server defined in the format: `domain name/user name`	HW/VE	Yes
`EXTERNAL_CONTENT_DIRECTORY`	The Web Server folder name. Change this name if you've changed the default names used by the Poly Clariti Manager application. Default value: `/PlcmWebServices`	HW/VE	Yes

Auto Layout - Default Layouts in CP Conferences Flags

No. of Video Participants	Auto Layout Flag	Auto Layout Default	Default Value
0	`PREDEFINED_AUTO_LAYOUT_0`		`CP_LAYOUT_1X1`
1	`PREDEFINED_AUTO_LAYOUT_1`		`CP_LAYOUT_1X1`
2	`PREDEFINED_AUTO_LAYOUT_2`		`CP_LAYOUT_1X1`

No. of Video Participants	Auto Layout Flag	Auto Layout Default	Default Value
3	PREDEFINED_AUTO_LAYOUT_3		CP_LAYOUT_1x2VER
4	PREDEFINED_AUTO_LAYOUT_4		CP_LAYOUT_2X2
5	PREDEFINED_AUTO_LAYOUT_5		CP_LAYOUT_2X2
6	PREDEFINED_AUTO_LAYOUT_6		CP_LAYOUT_1P5
7	PREDEFINED_AUTO_LAYOUT_7		CP_LAYOUT_1P5
8	PREDEFINED_AUTO_LAYOUT_8		CP_LAYOUT_1P7
9	PREDEFINED_AUTO_LAYOUT_9		CP_LAYOUT_1P7
10	PREDEFINED_AUTO_LAYOUT_10		CP_LAYOUT_2P8
11	PREDEFINED_AUTO_LAYOUT_11		CP_LAYOUT_2P8

No. of Video Participants	Auto Layout Flag	Auto Layout Default	Default Value
12	PREDEFINED_AUTO_LAYOUT_12		CP_LAYOUT_1P12
13	PREDEFINED_AUTO_LAYOUT_13		CP_LAYOUT_1P12
14	PREDEFINED_AUTO_LAYOUT_14		CP_LAYOUT_1P12
15	PREDEFINED_AUTO_LAYOUT_15		CP_LAYOUT_1P12
16	PREDEFINED_AUTO_LAYOUT_16		CP_LAYOUT_1P12
17	PREDEFINED_AUTO_LAYOUT_17		CP_LAYOUT_1P12
18	PREDEFINED_AUTO_LAYOUT_18		CP_LAYOUT_1P12
19	PREDEFINED_AUTO_LAYOUT_19		CP_LAYOUT_1P12
20	PREDEFINED_AUTO_LAYOUT_20		CP_LAYOUT_1P12
21	PREDEFINED_AUTO_LAYOUT_21		CP_LAYOUT_1P12
22	PREDEFINED_AUTO_LAYOUT_22		CP_LAYOUT_1P12
23	PREDEFINED_AUTO_LAYOUT_23		CP_LAYOUT_1P12
24	PREDEFINED_AUTO_LAYOUT_24		CP_LAYOUT_1P12
25	PREDEFINED_AUTO_LAYOUT_25		CP_LAYOUT_1P12

Available Layout Flags

No. of Cells	Layout Flag Value	Layout
1	`CP_LAYOUT_1X1`	
2	`CP_LAYOUT_1X2`	
2	`CP_LAYOUT_1X2HOR`	
2	`CP_LAYOUT_1x2VER`	
2	`CP_LAYOUT_2X1`	
2	`CP_LAYOUT_1X2_FLEX`	
3	`CP_LAYOUT_1P2HOR`	
3	`CP_LAYOUT_1P2HOR_UP`	
3	`CP_LAYOUT_1P2VER`	
3	`CP_LAYOUT_1P2HOR_RIGHT_FLEX`	
3	`CP_LAYOUT_1P2HOR_LEFT_FLEX`	
3	`CP_LAYOUT_1P2HOR_UP_RIGHT_FLEX`	
3	`CP_LAYOUT_1P2HOR_UP_LEFT_FLEX`	
4	`CP_LAYOUT_2X2`	
4	`CP_LAYOUT_1P3HOR`	
4	`CP_LAYOUT_1P3HOR_UP`	
4	`CP_LAYOUT_1P3VER`	

No. of Cells	Layout Flag Value	Layout
4	CP_LAYOUT_2X2_UP_RIGHT_FLEX	
4	CP_LAYOUT_2X2_UP_LEFT_FLEX	
4	CP_LAYOUT_2X2_DOWN_RIGHT_FLEX	
4	CP_LAYOUT_2X2_DOWN_LEFT_FLEX	
4	CP_LAYOUT_2X2_RIGHT_FLEX	
4	CP_LAYOUT_2X2_LEFT_FLEX	
5	CP_LAYOUT_1P4HOR_UP	
5	CP_LAYOUT_1P4HOR	
5	CP_LAYOUT_1P4VER	
6	CP_LAYOUT_1P5	
8	CP_LAYOUT_1P7	
9	CP_LAYOUT_1P8UP	
9	CP_LAYOUT_1P8CENT	
9	CP_LAYOUT_1P8HOR_UP	
9	CP_LAYOUT_3X3	
9	CP_LAYOUT_1TOP_LEFT_P8	
10	CP_LAYOUT_2P8	

No. of Cells	Layout Flag Value	Layout
10	`CP_LAYOUT_2TOP_P8`	
13	`CP_LAYOUT_1P12`	
16	`CP_LAYOUT_4X4`	
20	`CP_LAYOUT_4X5`	
25	`CP_LAYOUT_5X5`	
Overlay Layouts		
2	`CP_LAYOUT_OVERLAY_1P1`	
3	`CP_LAYOUT_OVERLAY_1P2`	
3	`CP_LAYOUT_OVERLAY_ITP`	
4	`CP_LAYOUT_OVERLAY_1P3`	

Secure Communication Mode

Topics:

RealPresence Collaboration Server can be configured to work in Secure Mode or Ultra Secure Mode.

In Secured mode the RealPresence Collaboration Server and the RMX Web Client are configured to work with SSL/TLS. In this mode, an SSL/TLS Certificate is installed on the MCU, setting the MCU Listening Port to secured port 443.

TLS is a cryptographic protocol used to ensure secure communications on public networks. TLS uses a Certificate purchased from a trusted third-party Certificate Authority to authenticate public keys that are used along with private keys to ensure secure communications across the network.

The RealPresence Collaboration Server supports:

- TLS 1.0
- SSL 3.0 (Secure Socket Layer)

SSL 3.0 uses 1024-bit RSA public key encryption.

TLS certificates can be generated using the following methods: CSR, PFX, and PEM; each giving different options for Encryption Key length. The table below lists the SIP TLS Encryption Key length support for the various system components.

SIP TLS - Encryption Key Support by System Component

System Component	Key Generation Method	Key Length (bits)	Key Generated by
SIP Signaling	CSR	2048	RealPresence Collaboration Server
SIP Signaling	PFX / PEM	1024 or 2048	User
Management	CSR	2048	RealPresence Collaboration Server
LDAP	CSR	2048	RealPresence Collaboration Server

Switching to Secure Mode

This section describes the process to switch to Secure Mode.

The following operations are required to switch the RealPresence Collaboration Server to Secure Mode:

- Purchase and Install the SSL/TLS certificate
- Modify the Management Network settings
- Create/Modify the relevant System Flags

System Flags Controlling Secure Communication

The following System Flags control secure communications.

- RMX_MANAGEMENT_SECURITY_PROTOCOL
- EXTERNAL_DB_PORT

The table below lists both flags and their settings.

If the System Flag RMX_MANAGEMENT_SECURITY_PROTOCOLdoesn't exist in the system, it must be created by using the **Setup** menu.

The RealPresence Collaboration Server must be restarted for modified flag settings to take effect.

System Flags

Flag	Description
RMX_MANAGEMENT_SECURITY_PROTOCOL	Enter the protocol to be used for secure communications. Default: TLSV1_SSLV3 (Both). Default for U.S. Federal Licenses: TLSV1.
EXTERNAL_DB_PORT	The external database server port used by the RealPresence Collaboration Server to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005

Related Links

System Flags on page 264

Enable Secure Communication Mode

After the SSL/TLS Certificate is installed, secure communications are enabled by modifying the properties of the Management Network in the Management Network properties dialog box.

When Secure Communications Mode is enabled:

- Only https:// commands from the browser to the Control Unit IP Address of the RealPresence Collaboration Server are accepted.
- The RealPresence Collaboration Server listens only on secured port 443.
- All connection attempts on port 80 are rejected.
- A secure communication indicator is displayed in the browser's status bar.

Procedure

1. In the **RealPresence Collaboration Server Management** pane, click IP Network Services.
2. In the **IP Network Services** list pane, double-click the **Management Network** entry.
3. Click the **Security** tab and in the **Management Security Properties** dialog, select the **Secured Communication** check box. This box is selected by default when the MCU is in Ultra Secure Mode.
4. Select the **Certificate Validation** mode by checking or clearing the **Skip certificate validation for user logging session** field as set out in the following table:

Status	RealPresence Collaboration Server (RMX) and Client Certificate Requirements
De-selected (Restricted Mode)	• The RealPresence Collaboration Server (RMX) must install a personal certificate issued by a CA. • The Client must install a personal certificate issued by a CA. • The public key of the CA must be installed in the RealPresence Collaboration Server (RMX). **Note:** When the RMX Manager is the Client, all Personal Certificates in the workstation's Certification Repository are sent to the RealPresence Collaboration Server (RMX). When using the RMX Web Client, Internet Explorer gives the user the option to select the Personal Certificate to be used from the workstation's Certification Repository.
Selected (Unrestricted Mode)	• The RealPresence Collaboration Server (RMX) must install a personal certificate issued by a CA. • No additional configuration is required for the Client.

5. Click **OK**.

Related Links

Alternate Management Network on page 342

Alternate Management Network

Alternate Management Network enables direct access to the RealPresence Collaboration Server for support purposes.

Access to the Alternate Management Network is via a cable connected to a workstation. The Alternate Management Network is accessible only via the dedicated LAN 3 port.

Note: Connection to the Alternate Management Network bypasses LAN and Firewall security. Strict control of access to LAN 3 port is recommended.

Related Links

Connect RealPresence Collaboration Server 2000/4000 to the Alternate Management Network on page 396
Perform a Comprehensive Restore While in Ultra Secure Mode on page 447
Enable Secure Communication Mode on page 341

Security Certificates

Topics:

User certificates between systems within your video conferencing environment (such as servers and endpoints) to build a trust/authentication and to support encryption.

Certificates confirm that the servers within your infrastructure can communicate and have the option to encrypt the data. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

The CA, or certificate authority, is a single, centralized authority such as an enterprise's IT department or a commercial certificate authority that each computer on the network is configured to trust. Each server on the network has a public certificate that identifies it. When a client connects to a server, the server shows its signed public certificate to the client. The certificate authority signs the public certificates of those servers that clients should trust. Trust is established because the certificate has been signed by the certificate authority (CA), and the client has been configured to trust the CA.

Requesting and Adding Certificates

The RealPresence Collaboration Server can generate a Certificate Signing Request (CSR) to send to a certificate authority (CA), a trusted entity that validates and officially issues, or signs, PKI certificates.

The RealPresence Collaboration Server uses those certificates for client and server authentication.

If your system is in an environment without a PKI, you don't need a CA-signed certificate; the system comes with a self-signed certificate for its TLS connections. When a PKI is deployed, however, self-signed certificates aren't trusted and CA-signed certificates are needed.

Once a certificate is purchased and received, it's stored in the RealPresence Collaboration Server and used for all subsequent secured connections.

Note: Certificates are deleted when an administrator performs a Restore Factory Defaults with the Comprehensive Restore option selected.

Create a Certificate Signing Request

The following procedure creates a certificate signing request (CSR) that you can submit to your chosen certificate authority.

This method uses the private key generated at software installation time.

Procedure

1. In RMX Manager, go to **Setup** > **RMX Secured Communication** > **Certification Repository**.
2. Go to **Personal Certificates** and click **Add**.
3. Select the **Network Service** for which to request a certificate (commonly **Default IP** or **IP Network Service**) and the **Certificate Method** of **CSR** and click **Create Certificate Request**.

4. Complete the following fields:

CSR Information	Description
Country Name	Two letter code for the country where your organization is located.
State or Province	Specifies the state or province where your organization is located.
Locality	Specifies the city where your organization is located.
Organization	Specifies your organization's name.
Organizational Unit	Specifies the business group defined by your organization. **Note:** The system supports only one OU field. If you want the CA-signed certificate to include more than one OU, download and manually edit the CSR.
Common Name (DNS)	Specifies the system name. Polycom recommends the following guidelines for this field: • For systems registered in DNS, use the system's fully qualified domain name (FQDN). • For systems not registered in DNS, use the system's IP address.

CSR Information	Description
Subject Alternative Name (SAN)	The SAN field allows you to specify additional host names to be protected by a single SSL Certificate. It allows you to secure host names on different base domains in a single SSL certificate or allows you to virtual host multiple SSL sites on a single IP address. This field may be required when using EAP-TLS in conjunction with a Network Policy Server (MS-NPS). When it's selected, you can modify the example values provided, to match local certificate requirements and delete those that aren't applicable. • Principle Name - Specifies the user and domain name for logging in to a Windows domain (for example, `user@example.com`). (This is the userPrincipalName attribute of the account object in Active Directory). It should be related to the 802.1X identity and password. • DNS Name - If DNS/MCU Host name is configured, the configured name will display, otherwise a default example will display: `DNS Name=myhost.example.com` Replace `myhost.example.com` with either FQDN of the RealPresence Collaboration Server Management Network Interface or the MCU Host name. • IP addresses ◦ If RealPresence Collaboration Server (RMX) is configured with IPv4, then the IPv4 address displays. ◦ If RealPresence Collaboration Server (RMX) is configured with IPv6, then the IPv6 address displays, besides you can also enter additional IPv6 addresses. ◦ If RealPresence Collaboration Server (RMX) is configured with both IPv4 and IPv6, then both IP addresses displays.
Hash Method	Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).

5. Click **Copy Request**.
6. Go to the Certificate Authority (CA) website and request a certificate from them as required and documented by them.
7. Paste the copied CSR content into the certificate request and complete the request process.

Install the Certificate

You can add, edit, and remove certificates from the system.

Procedure

1. In RMX Manager, go to **Setup** > **RMX** > **Certification Repository**.
2. Go to **Personal Certificates**, click **Add**, and then **Send Certificate**.
3. Copy the certificate text and click **Paste Certificate** and then **Send Certificate**.
4. Click **Activate Certificate** and then **OK** to disconnect, which is required to activate the certificate.

Certificate Configuration and Management

All Polycom devices used in a Maximum Security Environment require security certificates.

Related Links

Perform a Comprehensive Restore While in Ultra Secure Mode on page 447

Certificate Template Requirements

This section lists the Certificate Template Requirements.

The specific security certificate requirements for RealPresence Collaboration Servers used in Maximum Security Environments are:

- Support of 2048-bit encryption keys.
- Support of Extended Key Usage (EKU) for both:
  - Client Authentication
  - Server Authentication

The certificate template used by your CA server may need modification to meet the RealPresence Collaboration Server requirements.

Certificate Requirements

In Secure Mode, the certificate requirements depend on the Skip certificate validation for user logging session field.

Configuring Certificate Management

Within a PKI environment, certificate revocation policies are used to ensure that certificates are valid.

Certificates can expire or be revoked for various reasons (RFC 5280).

The RealPresence Collaboration Server enforces these certificate revocation policies through Certificate Revocation Lists (CRLs). CRLs are required for each CA Chain in use by the RealPresence Collaboration Server. These CRL files must be kept current.

Removing a CRL

Administrators can remove a CRL.

Procedure

1. In the certificate list, select the CRL List to be removed, and click **Remove**.

   The certificate is removed and the Collaboration Server displays a disconnection confirmation dialog.
2. Click **OK**.

Login to the Collaboration Server to proceed with further management tasks.

Modular MCU

Topics:

Beginning with version 8.6, and further on version 8.7.1, a new infrastructure for RealPresence Collaboration Server is introduced - the Modular MCU, or in short MMCU.

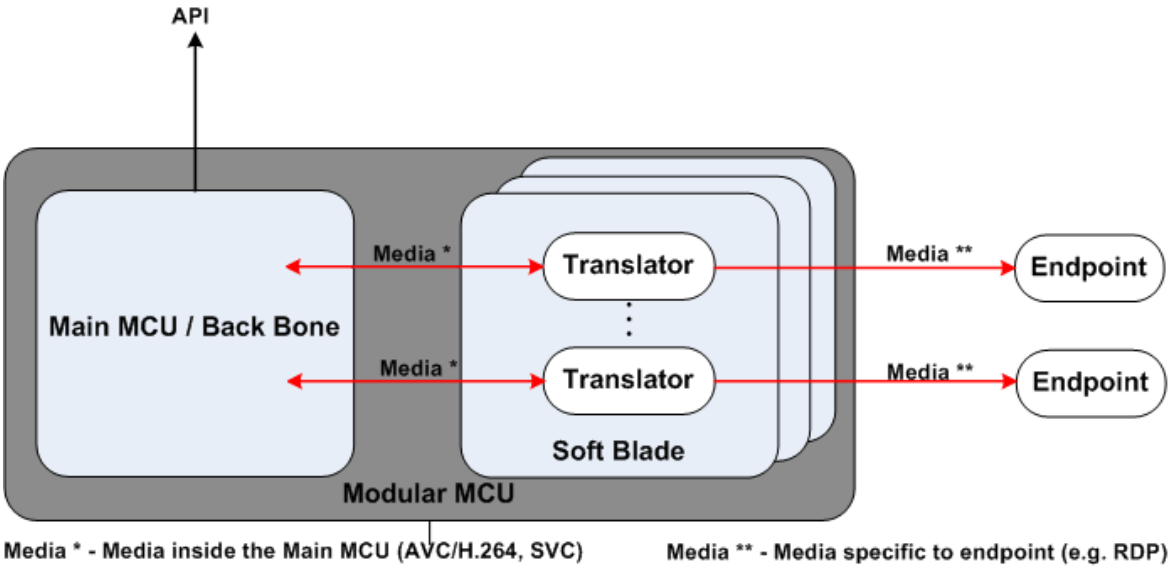
The new infrastructure is to separate the RealPresence Collaboration Server functionalities for better using of resources. For this purpose, Polycom extended the RealPresence Collaboration Server infrastructure to include:

- A Main MCU - May be either RealPresence Collaboration Server, Virtual Edition, or one of the Hardware MCUs, that is, RealPresence Collaboration Servers 1800, 2000, 4000.
- Soft Blades - Polycom Soft Blade proprietary software installed on a virtual machine (currently only VMWare machines). Each Soft Blade is assigned to a Main MCU.

The Soft Blade is aimed at providing new media types to endpoints (in 8.7.1, RDP content media to MS Lync clients), via a Translator residing within it, for each media type connection. The purpose of the Translator is translating the standard media sent by the RealPresence Collaboration Server to endpoints, into the new media type, and vice versa.

It is important to note however, that this change in the infrastructure isn't imperative should there be no need of media types other than those until now supplied by the RealPresence Collaboration Server, and the former infrastructure can be maintained, and is actually the default state of the MCU.

Figure 48: Modular MCU (MMCU) infrastructure



MCU Operation Mode

The MODULAR_MCU_MODE system flag indicates whether the system is in MMCU mode.

The ENABLE_MODULAR_MCU system flag, along with the IP services existing in the system, indicate the MCU mode with respect to the Modular MCU infrastructure. This flag is visible, and modifying it requires restart for it to take effect.

Possible states:

- NO (default) - MMCU is completely inactive.
- YES - System is in MMCU mode; existing Lync RDP IP service enables external translators for RDP content. If no such IP services exit, the corresponding translator isn't supported.
- MIX - Obsolete state.

Modular MCU Implementation Aspects

This section describes the Modular MCU Implementation Aspects.

Following, are the descriptions for the various aspects necessarily comprising the new MMCU infrastructure:

- Deployment of Soft Blades in a Modular MCU
- Monitoring Modular MCU Components
- RDP Content
- Modular MCU Resource Consumption and Management
- Modular MCU Security Aspects
- Modular MCU Logger
- Modular MCU Upgrade Process

Deploy a Main MCU from an Existing MCU

A Soft Blade is deployed on a virtual machine.

A single Main MCU may control up to 20 Soft Blades.

Attempting to assign a Soft Blade to a Main MCU with full Soft Blade assignment results in generating a fault event on the Main MCU, indicating the maximum number of Soft Blades was reached for this particular Main MCU.

Soft Blade Prerequisites:

- For Soft Blade Host Hardware Profile, refer to RealPresence Collaboration Server 1800, 2000, 4000, and Virtual Edition Release Notes.
- The virtual machine must use VMWare.
- All the MMCU components should be located on a single premise (co-located).

Procedure

1. To turn your current MCU into a Main MCU, set its ENABLE_MODULAR_MCU system flag value to MIX (recommended) or YES.

Add system flag `MMCU_BLOCK_TR_ABORTED MMCU` and set the value to `NO` to enable the recovery mechanism.

2. To install the Soft Blades, download from Polycom support site the **Soft Blade OVA** file (includes Operating System, a console wizard, and a Salt minion), and install it.

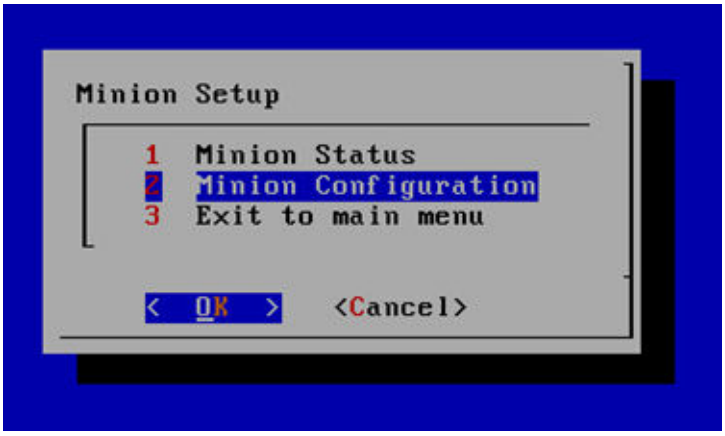
   In the support site, there are two OVA files. The **Soft MCU OVA** file name contains `caxis-mcu`, whereas the one for the Soft Blade contains `rppbase`, and is also significantly smaller sized.

3. Deploy OVA file through **vSphere client** > **File** > **Deploy OVA Template**.

Note:
- Deploy one OVA file at a time.
- If the Main MCU is a RealPresence Collaboration Server VE, verify both the Main MCU and the Soft Blade OVA files are the latest, which may entail a required upgrade of the Main MCU.

---

4. Via `putty`, log into the intended Soft Blade machine via the console wizard, with `polycom` as both username and password, to display the **Minion Setup** menu.



5. If soft blade IP address is allocated by the DHCP server, skip to next step, otherwise select **Exit to main menu** in this menu, and there set the static value of the soft blade IP.
6. In the **Minion Setup** menu, select **Minion Configuration**, and press **Enter**.
7. Enter the Main MCU IP address, and press **Enter**.

Note: For all RealPresence Collaboration Servers acting as Main MCU, use only the Management IP.

A message appears, indicating you should wait for the PFX file, containing the password, from the Main MCU (primary).

In parallel, the Soft Blade appears as a new **Translator.<unique ID>** on the Main MCU System Monitor with a Pend Authentication status, and no IP address.

8. Once the Soft Blade IP address appears on the System Monitor, right-click the Soft Blade, and select **Accept**.

Note: To Remove the Soft Blade at this point, select **Reject**; selecting **Delete** removes it from the Main MCU System Monitor only temporarily, and once another Salt message from the Soft Blade to the Main MCU is received, the Soft Blade reappears in the System Monitor.

---

9. When prompted, enter a password of your choice.

The password you entered is sent in a PFX file to the Soft Blade, and the Soft Blade Status changes to **Soft Blade Pend Authentication**.

10. At the Soft Blade console wizard, enter the password received in the PFX file (from the previous step), and press **Enter**.

    The Soft Blade automatically reboots.

    In the System Monitor at the Main MCU, the Soft Blade Status changes to **Installing**. At this point, its deployment begins, and assuming a smooth process through Installing and Initializing, the Soft Blade Status at the System Monitor becomes **Ready**, which indicates the Soft Blade is now operational.
11. Create in your machine the appropriate IP services as required.
12. Add system flag `MMCU_BYPASS_ENABLE_RDP` and set it to `YES`.
13. Select **Enable MS RDP content**.
14. To share content in the encrypted Direct Call, set `Set-CsClientPolicy -P2PAppSharingEncryption` to `Supported` on the Skype for Business Front End server.
15. Change cascade link from **Attendees** to **Presenters** in Skype for Business.

Monitor Modular MCU Components

Provided the RealPresence Collaboration Server is in MMCU mode, the **System Monitor** replaces the Hardware Monitor in the RMX Management pane.

The Main MCU rhythmically (Currently fixed - every 30 seconds) verifies each of the Soft Blades proper operation, and monitors its status.

Note: The monitoring applies to the connection between the endpoint and the Translator, and not to any internal communications.

Procedure

1. In the **RMX Management** pane, click **System Monitor** to display the list of machines comprising the MMCU.

   The System Monitor is displayed, with the Main MCU at the top, followed by the list of its assigned Soft Blades.
2. Double-click on any of the MMCU machines to view its specific component information as follows:
   - Double-clicking a hardware Main MCU (RealPresence Collaboration Servers 1800/2000/4000), results in displaying its Hardware Monitor.
   - Double-clicking a soft Main MCU (RealPresence Collaboration Server, Virtual Edition), results in displaying the VM Monitor, which includes information on the cores, clock frequency, memory, storage, and CPU model.
   - Double-clicking one of the Soft Blades, results with displaying the Soft Blade Monitor, with similar information, as well as the Soft Blade use percentage, and the number of active Translators.From this point:
     - Right-click **Active Translators**, and select **View Properties**, or double-click **Active Translators**, to display the list of Translators on this Soft Blade, aggregated according to their type.
     - If the Soft Blade information cannot be viewed, since the Soft Blade is in one of the dysfunctional states in the State Machine, an error message pops-up, indicating Soft Blade details cannot be viewed.

- If the Soft Blade resources are all consumed, an Active Alarm is generated indicating no resources are available on this Soft Blade.

Click the Up-Arrow on the monitor until the original System Monitor is displayed.

3. Do one of the following:
   - Right-click on the Main MCU to display its properties.
   - Right-click on any of the Soft Blades to select one of the currently available actions for this Soft Blade.

Note: When not in MMCU mode, the MCU operates as it used to before this infrastructure was created: Soft Blades aren't visible, and Main is replaced by RealPresence Collaboration Server (RMX) (for HW MCUs).

Related Links

Monitoring RDP Content on page 359

Monitoring Guidelines

This section describes the Monitoring Guidelines.

- Only an Administrator user may perform actions or changes on any of the Soft Blades.
- All columns specific to MMCU mode are hidden while not in MMCU mode, for Main MCU, Soft Blades and participants.

MMCU Impact on Participant Monitoring

The MMCU infrastructure impacts not only in the general system operation, but also the participant monitoring in general, as well as the **Participant Properties - General** tab.

When monitoring conference participants, the participant type is indicated by the Alias Name.

In the **Participant Properties - General** tab, when in MMCU mode, and for participants using a Translator (such as RDP content), the **Participant Properties** reflect the Soft Blade IP address, as well as the Translator ID and type, which reflect the endpoint type, thus making the **Endpoint Type** field at the top (disabled) irrelevant.

Note that a Translator ID equaling 0, denotes a non-Translator participant, since it's either AVC or SVC.

In addition, viewing a specific Translator Properties (or double-clicking it), results in opening the **Participant Properties** for the participant serviced by that Translator, meaning the information reflects the endpoint and not the translator itself.

Faults and Active Alarms

When an attempt is made to assign a Soft Blade to a Main MCU with full Soft Blade assignment, a fault event is generated indicating the maximum number of Soft Blades was reached for this Main MCU.

In the Main MCU, there are two generated Active Alarms:

- When the Main MCU can't communicate with the Soft Blade application, though it does manage to ping it - `Soft Blade <name> status has changed to Faulty`.
- When the Main MCU can't communicate with the Soft Blade application, nor ping it - `Soft Blade <name> status has changed to Disconnected`.

System Operation Description for Deployment and Monitoring

The MMCU infrastructure operates mostly independently, though at its starting point, it depends on the Administrator intervention.

In addition, the Administrator may intervene at some points, to effect a change in Soft Blade operation.

The table below describes the Soft Blade operation, and the states in which the Administrator can intervene to affect it, in the form of a State Transition Machine (STT).

Soft Blade Monitoring States

Soft Blade State	State Meaning	Soft Blade/Administrator Operation While in State	Soft Blade New State
Authentication Phase			
Pend Authentication	Soft Blade awaits Administrator password at the Main MCU.	Administrator performs **Accept**, and enters password.	**Soft Blade Pend Authentication**
	Soft Blade awaits Administrator password at the Main MCU.	Administrator performs **Reject**.	**Rejected**
	Soft Blade awaits Administrator password at the Main MCU.	Administrator performs **Delete**. **Note:** If the console wizard is active at the Soft Blade, the Soft Blade reappears in System Monitor (Salt ping). Use Reject for complete deletion.	**Soft Blade erased****
Soft Blade Pend Authentication	Soft Blade awaits Administrator password at Soft Blade.	Administrator performs **Accept**, and enters password.	**Installing**
	Soft Blade awaits Administrator password at Soft Blade.	Administrator performs **Reject**.	**Rejected**
	Soft Blade awaits Administrator password at Soft Blade.	Administrator performs **Delete**. ***	**Soft Blade erased****

** Once a Soft Blade is erased, readding it requires reauthentication from the starting point.
*** Warning to ongoing conferences is generated.

Soft Blade State	State Meaning	Soft Blade/Administrator Operation While in State	Soft Blade New State
Rejected	Soft Blade awaits the Administrator next action.	Administrator performs **Accept**, and enters password.	**Soft Blade Pend Authentication**
	Soft Blade awaits the Administrator next action.	Administrator **Delete**.	**Soft Blade erased** **
Operational Phase			
Installing	The Soft Blade installation is launched	Installation is successfully completed.	**Initializing**
	The Soft Blade installation is launched	Installation fails.	**Faulty**
Initializing	Initializing the Soft Blade	Initialization is successfully completed.	**Ready**
	Initializing the Soft Blade	Initialization fails.	**Faulty (ping)** **Disconnected (no ping)**
Ready	Soft Blade is operational.	Administrator performs **Restart** ***	**Ready (on success)** **Faulty (on failure)**
	Soft Blade is operational.	Administrator performs **Disable**. **	**Disabled**
	Soft Blade is operational.	No communication with Blade, ping	**Faulty**
	Soft Blade is operational.	No communication with Blade, no ping	**Disconnected**
	Soft Blade is operational.	Administrator performs **Delete**. ***	**Soft Blade erased** **
Operational Phase Error Handling			
Disabled	Ongoing conferences continue, no new ones.	Administrator performs **Enable**.	**Ready**
	Ongoing conferences continue, no new ones.	Administrator performs **Delete**. ***	**Soft Blade erased** **

Soft Blade State	State Meaning	Soft Blade/Administrator Operation While in State	Soft Blade New State
Disconnected	No communication with Soft Blade, and no ping. Generates Active Alarm indicating Soft Blade status changed to **Disconnected**.	Soft Blade is alive following restart, but installation isn't complete.	**Installing**
	No communication with Soft Blade, and no ping. Generates Active Alarm indicating Soft Blade status changed to **Disconnected**.	Soft Blade is alive following restart, and installation is complete.	**Initializing**
	No communication with Soft Blade, and no ping. Generates Active Alarm indicating Soft Blade status changed to **Disconnected**.	Administrator performs **Delete**, which turns off the Active Alarm.	**Soft Blade erased** **
Faulty	No communication with Soft Blade but ping succeeds. Internal recovery is ran to verify installation and configuration. Generates Active Alarm indicating Soft Blade status changed to **Faulty**.	Administrator performs **Restart for a service** ***	**Ready (on successful Restart)** **Faulty (on failed Restart)**
	No communication with Soft Blade but ping succeeds. Internal recovery is ran to verify installation and configuration. Generates Active Alarm indicating Soft Blade status changed to **Faulty**.	Administrator performs **Rescue**, triggering reinstallation of internal package followed by reboot.	**Installing**

Soft Blade State	State Meaning	Soft Blade/Administrator Operation While in State	Soft Blade New State
	No communication with Soft Blade but ping succeeds. Internal recovery is ran to verify installation and configuration. Generates Active Alarm indicating Soft Blade status changed to **Faulty**.	Administrator performs **Disable**.	**Disabled**
	No communication with Soft Blade but ping succeeds. Internal recovery is ran to verify installation and configuration. Generates Active Alarm indicating Soft Blade status changed to **Faulty**.	Administrator performs **Delete**.	**Soft Blade erased** **
	No communication with Soft Blade but ping succeeds. Internal recovery is ran to verify installation and configuration. Generates Active Alarm indicating Soft Blade status changed to **Faulty**.	No ping	**Disconnected**

Initiating a Restore to Factory Defaults operation on a Soft Blade, results in the Soft Blade requiring reauthentication before resuming its normal operation (see the Pend Authentication state in the State Machine above).

Using Backup of an operational MMCU, to Restore on a different machine, requires reauthentication of the assigned Soft Blades.

MMCU Components Restart

The MMCU system strives to return to the state it was in at the point of restart, or improve it, whether the restart was performed on the Main MCU or on one of the Soft Blades.

The most significant point of improvement being when a Soft Blade had a **Disconnected** status before its restart, and could be pinged right after it, in which case it goes through the process described above from its starting point, and ends either as **Ready** or **Faulty**.

There's however, a single irregular behavior if a Soft Blade is in Soft Blade Pend Authentication state before the Main MCU restart. In this case following this restart, due to the lack of Salt ping, the Soft Blade is perceived by the Main MCU as Disconnected, and is displayed as such. Thus, once the Administrator enters the password at the Soft Blade, the Soft Blade is ready to continue from Soft Blade Pend Authentication (and not from Disconnected), and its state becomes Installing.

During restart of:

- Soft Blade - The Main MCU modifies the Soft Blade state to **Disconnected**.
- Main MCU - All conferences and translators, both on the Main MCU and the Soft Blades, are disconnected.

IP Address Management

The Soft Blades' initial IP address is provided by the DHCP server.

Note: Currently, only IPv4 address type is supported for Soft Blade IP addresses.

However, the Soft Blades management is independent of their IP addresses. Therefore, following restart, though some of the Soft Blades may be assigned a new IP address by the DHCP server during their Initialization state, the Main MCU is not affected by that change - the Soft Blades are recognized in the system, and are assigned a state relevant to their state before restart. For example, if a Soft Blade already passed both authentication states, it doesn't require reacceptance by the Administrator.

If a new Soft Blade is assigned an IP address, which was previously assigned to a currently Disconnected Soft Blade, it goes through the authentication phases from the beginning. The **Disconnected** machine, when it becomes operable, is reassigned a new IP address by the DHCP server, though during its **Disconnected** state it does appear in the list of Soft Blades in the UI.

When a Soft Blade is reassigned to an alternate Main MCU, until deleted from its original Main MCU, it's considered as Disconnected by this MCU.

Configure Main MCU IP Address mode

Once the Soft Blades' initial IP address is provided, an Administrator user is required to log on.

Procedure

1. The Administrator logs on to the Soft Blade Console Wizard.
2. Set the Main MCU IP address mode to one of the following:
    - DHCP
    - Static

RDP Content

Skype for Business clients can share content using a Remote Desktop Protocol (RDP).

Standard endpoints doesn't support RDP and hence it uses the H.239 (for H.323 endpoints) or BFCP (for SIP endpoints). To enable content sharing between Skype for Business clients and standard room endpoints, RealPresence Collaboration Server can be used (when configured to work in Modular MCU mode).

Two use cases are supported for content sharing:

- Polycom RealConnect Mode - RealPresence Collaboration Server calls the AS-MCU

- Direct Call Mode - Lync client calls a VMR

Both cases require RealPresence Collaboration Server configured to MMCU mode.

Polycom RealConnect Call Mode

Polycom RealConnect's capability to translate between RDP and H.264, and vice versa, is embedded in the MMCU and is referred to as Polycom RealConnect Mode or Gateway Mode.

This requires a single transcoding resource, between the virtual meeting room (VMR) and the Microsoft Application Sharing MCU (ASMCU). This resource resides on a soft blade MMCU.

This option can be used in place of a separate Polycom® ContentConnect™ gateway solution.

- If the are insufficient resources for a RDP-content translator, content isn't shared between Polycom endpoints and Skype for Business clients.
- In the event of soft blade failure the MCU recovers Polycom RealConnect content calls if another soft blade is available.
- In the event of MCU fail-over, Polycom RealConnect content calls are recovered immediately after the MCU recovers the A/V Polycom RealConnect call.

Set Polycom RealConnect Call Mode

This setting allows participants to connect and receive multiple video streams.

Procedure

» On the Skype for Business Front End Server, set `AllowMultiView` to `TRUE`.

Direct Call Mode

RDP content can be shared in the Direct Call mode, in which Skype for Business clients share the content directly and Poly clients still share the RDP content through RDP translator in the Soft blade.

- A transcoding resource is allocated to each direct call from a Skype for Business client to the VMR.
- The MMCU allocates transcoding resources to RDP content for each Skype for Business client connected to a VMR.
- Poly Clariti Core routes Skype for Business content call to the same MCU where the A/V call is being hosted.
- In cases of MCU fail-over, only nonencrypted Skype for Business A/V calls can be re-established. Recovery requires a reinvite, including the exchange of keys for the encrypted call, which is not supported by Skype for Business clients.
- If there are insufficient resources for a RDP-content translator, whether content is sent through the people video channel depends on the setting of the Send Content to Legacy Endpoints check box in the Profile - Video Quality dialog. In this case, Skype for Business clients will not be able to share content.
- RDP Content calls aren't supported on MMCUs that don't have an encryption license.
- In the event of soft blade failure the MCU will recover Direct Calls if another soft blade is available. If the content was being shared by the Skype for Business client, the content will be shared again by the Skype for Business client.

Note: The transcoded content call reaches the main MCU.

Common Behavior - Polycom RealConnect / Direct Call Modes

This section describes the common behavior for Polycom RealConnect or Direct Call Modes.

- In the event of MCU failure Poly Clariti Core attempts to find another MMCU on which to create the content stream. For Polycom RealConnect calls there are two calls to the Lync side of the topology. The first call is to subscribe or notify. The second call, created when content is shared, is to establish the content media channel. The subscription call is created when the A/V call is created. If successful, a Content gateway call is established immediately after the call to the ASMCU is established. If another MMCU isn't found, the conference is created on a nonmodular MCU without RDP content capability, resulting in Polycom and Lync clients not being able to share content.
- ICE credentials are updated on the system in both Polycom RealConnect and Direct Call modes for both on-premise and federated environments.
- Ongoing calls may be disconnected, but the system recovers automatically from the following failures:
  - ICE Server
  - Microsoft Lync Server
  - Enabling RDP Content

Enabling RDP content needs configurations on Poly Clariti Core and IP Network Service.

Enable Microsoft RPD Content on Poly Clariti Core

Enable RPD content on Poly Clariti Core.

Before enabling MS RDP on Poly Clariti Core, make sure no ContentConnect server is configured in Poly Clariti Core.

Procedure

1. Go to **Polycom MCU Video Quality** > **Content Video Definition**.
2. Select **Enable MS RDP content**.

IP Network Services - SIP Servers Dialog

If the SIP Server Type is configured to Microsoft, an additional information box for the Translator SIP Proxy displays.

Set Translator SIP Proxy parameters

The RDP-content data section contains the Translator SIP Proxy parameters.

Procedure

1. In the **IP Network Services Properties** dialog, open the **SIP Servers** tab.
2. In the **SIP Server Type** field, select **Microsoft**.
3. The **RDP-content data** section is displayed and contains the following parameters:

Field	Value
Server Address	Poly Clariti Core Server name/address
SIP Authorization Name	Optional. Poly Clariti Core server authorization name.

Field	Value
SIP Password	Optional. Poly Clariti Core server password.

Change a Cascade Link (Polycom Participants) from an Attendee to a Presenter in Skype for Business

Content can only be shared by the cascade link who are presenters and not attendees in the Skype for Business.

If conference participants attempt to share content without having the correct presenter privilege through the AVMCU cascade connection, they receive a `Skype for Business users are unable to view the shared content without the VTC being promoted to a presenter` error message. You can change the privilege access to enable these users to share content.

Procedure

1. Click **Meet Now**.
2. Click **Invite More People** and select cascade link of VMR for the meeting.
3. Click **Open Participant List**, verify if VMR cascade link is in the Presenters list.
4. If VMR cascade link is in the Attendees list, right-click the cascade link from the list and select **Make a Presenter**.

Monitoring RDP Content

Both Polycom RealConnect (RDPConnect) and Direct Call Mode (RDPDirect) translators can be monitored using the System Monitor.

Related Links

Monitor Modular MCU Components on page 350

Modular MCU Resource Consumption and Management

Some changes in the resource consumption and resource report result from the changes introduced into the RealPresence Collaboration Server infrastructure.

There's an inherent difficulty in estimating the resource usage, since it may be due to either one of the Main MCU, one of the Soft Blades, or both (such as in H.265).

In addition, the Translator consumes Soft Blade cores according to the type of media/endpoint.

Resource Weight Factoring in Resource Management

A resource weight is the amount of resources required by any Translator of a certain type.

Resource weights are constant across the MMCU system per each Translator (media/endpoint) type, and a table containing these values resides at the TC, to enable resource allocation planning.

In addition, each Translator consumes H.264 resources of identical resolution on the Main MCU.

The TC allocates Translators on each Soft Blade, taking into account the resource weight of the required Translator type, until a predefined upper threshold is reached, at which point Translator-allocation moves to the next Soft Blade in the system. Each Soft Blade reports to the TC on its own resource availability/usage, thus the TC acts as a Poly Clariti Manager for the Translators (only).

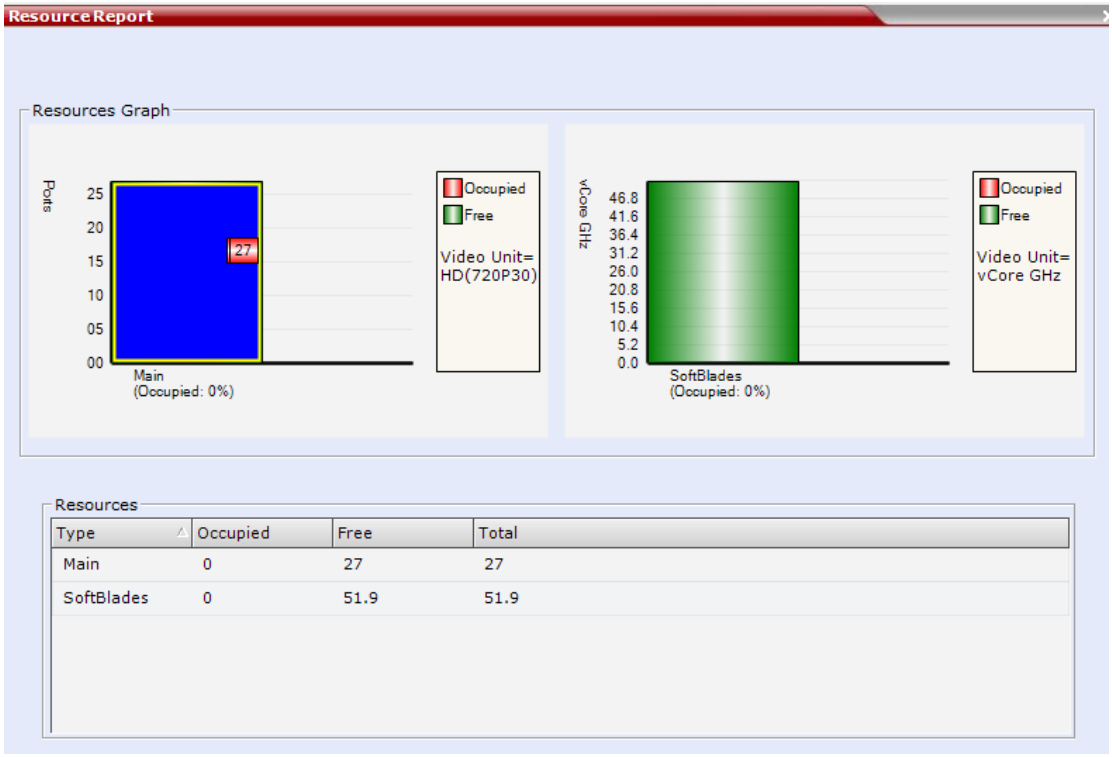
The Main MCU resource management remains as it was.

Resource Report

Two separate resource reports are available, as before, only now they're separated into a report on the Main MCU, and a report on the Soft Blades assigned to that Main MCU.

These reports are:

- The bar-graph representation:



  This report can be viewed by selecting, in the RealPresence Collaboration Server (RMX) Menu, **Administration** > **Resource Report**.

- Real-time resource report at the RealPresence Collaboration Server Status Bar:

Figure 49: Resource Report With no Translators Used on Soft Blade

Figure 50: Resource Report With Translators Used on Soft Blade

These numbers are reported for resource balancing purposes via XML API, as before.

Note: The previous Voice resource report is removed, since it's only applicable to systems with MPMx media cards, which aren't supported from version 8.6.

Note that in the Main MCU, AVC HD720p30 is used as the measuring unit in the resource report, whereas in the Soft Blades, cores in terms of GHz is used, which allows for easy calculation of the number of Soft Blades requiring allocation.

Upon each Soft Blade initiation, its computing power is calculated, and is aggregated by the TC with the computing power of the other Soft Blades in the MMCU, to yield the general Soft Blades resource pool usage information.

The TC also keeps track of the resource pool on the Main MCU, to be able to pass on this information to external entities.

Note: A Disabled Soft Blade is presented as having 0 resources, unless Translators were already running on it at the point of Disabling, in which case its maximum resources are considered as the used resources at that point.

Port Usage for Skype for Business

Following table shows port usage for Skype for Business client.

One additional audio port is consumed per participant for the connection between RealPresence Collaboration Server and Soft Blade.

Port Usage for Skype for Business Client by Resolution

Resolution	Port Usage
720p	1
1080p	2

Modular MCU Security Aspects

This section describes the Modular MCU Security Aspects.

The MMCU model ensures that security is preserved on several levels:

- Salt and Soft Blade APIs.
- SIP signaling connections - Both between the RealPresence Collaboration Server and the Soft Blade, and between the Soft Blade and Poly Clariti Core.
- Media - Both between the RealPresence Collaboration Server and the Soft Blade, and between the Soft Blade and the endpoint.

When the Administrator wants to accept a Soft Blade currently in **Pend Authentication** state, it's required to install a self-signed certificate with the properties:

- Common Name - The host name for which the certificate was generated. Since this is a self-signed certificate, this name is the Soft Blade name as it appears in the Soft Blade monitoring.
- Certificate expiration period - 10 years.

The Administrator then enters the Soft Blade password.

Modular MCU Logger

The Logger aggregates and standardizes the logging at the Soft Blades, or as they're sometimes related to, Translator Machines.

It also allows the Main MCU to gather the Translators/Soft Blades logs from a centralized gathering point.

Logger Guidelines:

- The Main MCU writes logs into the regular Main MCU log file, including API messages sent to the Soft Blades.
- All logging operations use the same infrastructure elements, thus are consistent across the MMCU various components.

Logs Format

This section descibes the Logs format.

In all Soft Blades, logs are formated as

```
D:<Date and time stamp> E:<Entity> P:<Process> U:<Unit> L:<Log level> SN:<#>
Lcnt:<code location>
```

Log Component	Description and Structure
Date and time stamp	Date and time of log generation, in the format dd/mm/yy-hh:mm:ss.ms
Entity	System entity generating the log
Process	Soft Blade application process generating the log
Unit	Unit generating the log
Log level	Logging level at the point of log generation. One of: • TRACE • DEBUG • INFO (default) • WARN • ERROR • FATAL
#	Log message serial number
Code location	Code file name, and line number

Logs generated with ERROR/FATAL logging level are immediately sent to the Logger of the TC at the Main MCU as faults, as well as logged on the Soft Blade.

Configure Logging

All logging performed at the Soft Blades, share the same configuration, especially their logging level, and are configurable via the Main MCU, although the Main MCU may use different logging configuration.

Nevertheless, the system initial state, is that of the Main MCU sharing its default logging configuration (INFO) with the Soft Blades.

In normal situations, INFO is the logging level. To obtain detailed logs, logging level at both the Main MCU and the Soft Blades should be set to TRACE/DEBUG.

Logging volume varies according to the logging level. However, it's designed so that, assuming a total of 15GB storage, approximately one month worth of logs can be stored.

Procedure

1. In the RealPresence Collaboration Server main menu, select **Administration** > **Tools** > **Logger Configuration**.
2. Click **Customize** for the Local Log File.

A new check-box for Soft Blades logging is displayed, with the same logging level and the same processes selected. You can modify both the logging level and the process selection.

3. Click **OK** to save and return to the Logger Configuration dialog, and then **OK** to exit.

Soft Blade Call Logs

The Soft Blade log files are located under `/opt/polycom/Translator/Logs`.

Note: Salt logs are stored in a dedicated folder under that location.

Each such log file is dedicated to a single participant in a conference, and is named:

`Log_SN<log serial #>_FMD<1st msg date>_FMT<1st msg time>_LMD<last msg date>_LMT<last msg time>_C<Conf ID>_P<Party ID>_SZ<size>_SU<1st log in process? Y/N>_CF<Compression format>_NFV<File version>_ RT<File retrieved? Y/N>_<process name>.log`

Example:
`Log_SN0000000023_FMD04112015_FMT142815_LMD04112015_LMT142815_C0000110_P0000001_SZ0000130_SUY_CFzlib_NFV02_RTN_WebRtcWrapper50103.log`

Each file is limited to 1MB, thus there may be more than one file for a conference-participant combination.

Soft Blade General Logs

The Soft Blade log files are located under `/opt/polycom/Translator/Logs`.

Note: Salt logs are stored in a dedicated folder under that location.

All logs pertaining to information unrelated to conferences. Upon Soft Blade startup the first log file is created. Each such log file is limited to 1MB, and is named:

`Log_SN<log serial #>_FMD<1st msg date>_FMT<1st msg time>_LMD<last msg date>_LMT<last msg time>_SZ<size>_SU<1st log in process? Y/N>_CF<Compression format>_NFV<File version>_RT<File retrieved? Y/N>_<process name>.log`

Example: `Log_SN0000000023_FMD04112015_FMT142815_LMD04112015_LMT142815_SZ0000130_SUY_CFzlib_NFV02_RTN_Container50103.log.`

Logging volume varies according to the logging level. However, it's designed so that, assuming a total of 15GB storage per Soft Blade machine, approximately one month worth of logs can be stored.

Filter Logs

This section descibes the process of filtering the logs.

Logs from all MMCU machines, may be filtered according to any combination of the following criteria:

- A specified time stamp/interval - Mandatory
- A specific conference
- A specific participant in a conference

The resulting log files are stored in the Main MCU, under `MMCU/Logger/Collector FS check` as follows:

- `CollectInfo_<begin date&time>-<end date&time>.tgz` - A log file for the Main MCU.
- A folder named `Blades`, for log files filtered from all the Soft Blades. Under this folder there are:
  - Folders named `Translator.<ID>`, for each of the Soft Blades log files.

- A folder named `Translator.777777`, for log files filtered from the local Translators (Translators residing on the Main MCU).

When a filter specifies a conference/participant, for which one of the involved Soft Blades is inoperable, the user is notified that the returned logs are partial (for a conference), or cannot be supplied (for a participant in the specified conference).

Each of the filtered log files is limited to 100 MB.

Procedure

1. In the RealPresence Collaboration Server main menu, select **Administration** > **Tools** > **Information Collector**.
2. Determine the time frame of the desired logs.
3. To filter the logs of a specific conference beginning within this time frame:
   a. Click **Select Conference**.
   b. Select the conference to use for the filter, and click **OK**.

   The time frame you previously selected, is modified to that of the selected conference; for an ongoing conference, the end time is determined to be the current time.
4. To filter the logs of a specific participant in the selected conference:
   a. Click **Select Participants**.
   b. Select the participant to use for the filter, and click **OK**.
5. Determine the location in which the filtered logs are stored, by entering it or via **Browse**.
6. Click **Collect Information** to generate the appropriate log files.

Error Handling

This section describes the Error Handling process.

Should a failure occur at one of the Soft Blades - from best case scenario of the RealPresence Collaboration Server application level, down to the worst case scenario of the Soft Blade machine termination - all retrievable log files are sent to the Main MCU, accompanied by a notification listing the files which could not be retrieved.

Modular MCU Upgrade Process

For both of nonmodular MCU and modular MCU, to upgrade from any versions earlier than version 8.5 to version 8.7.1, the intermediate upgrade to 8.5, 8.6, or the maintenance releases of both versions is needed.

The modular MCU and its soft blades can be upgraded together with one upgrade software and the same is also used for nonmodular MCU upgrade. All soft blades get upgraded automatically during the modular MCU reboot.

Upgrade Modular MCU

You can upgrade modular MCU in the same way of upgrading nonmodular MCU. The only difference is that upgrading modular-MCU may take extra 1 or 2 minutes.

Procedure

1. Select the upgrade software from one of the following:
   - *.bin for RealPresence Collaboration Server (RMX) 1800, 2000, and 4000

- *.upg for Virtual Edition

2. Navigate to RMX Management pane, and select **System Monitor** to monitor the soft blades upgrade status.

   The System Monitor is displayed, with the Main MCU at the top, followed by the list of its assigned Soft Blades.

Virtual Edition Modular MCU Upgrade Storage Requirements

This section descibes the Virtual Edition Modular MCU Upgrade Storage requirements.

If the modular MCU is virtual edition, sufficient storage for modular MCU and its soft blades is required:

- For modular MCU storage requirements, see Virtual Edition Host Server Platform Profile.
- For soft blades storage requirements, see Soft Blade prerequisites.

In case of insufficient storage, the upgrade won't start, and an active alarm "Insufficient storage space for upgrade" will be raised.

Monitor the Soft Blades Upgrade

You can monitor the modular MCU and its soft blades upgrade process through the pane.

Procedure

1. Go to **RMX Management** > **MMCU System Monitor**.
2. View the soft blades upgrade status:
   - If soft blades upgrade normally, **Upgrading** displays in each soft blade row.

     Note: Only the soft blades that upgrade successfully work actively with the modular MCU.

   - If soft blades fail to upgrade, **Upgrade failed** displays in the modular MCU row.

   The following table shows other soft blades status and behaviors:

Soft Blade Status and Expected Behavior

Status	Behaviors
Pending authentication	No action. Once the modular MCU is authenticated, it will be upgraded.
Soft blade pending authentication	No action. Once the soft blade is authenticated, it will be upgraded.
Rejected	Remain rejected.
Initializing	Start upgrade.
Ready	Start upgrade.
Faulty	Start upgrade.
Disconnected	No action.
Disabled	Start upgrade.

3. If any upgrades fail, you can manually install the new software version on the soft blades.

Note: During the modular reboot process, if the modular MCU is verified as an invalid system, the modular MCU uses the previous version software instead and issue an active alarm. In this case, the soft blades downgrade automatically to match the main MCU version.

System Maintenance

Topics:

This section includes information on administering, monitoring, and maintaining RealPresence Collaboration Server hardware and software.

- Administration and Utilities
- Hardware Monitoring
- Media Traffic Shaping
- Direct Connection to the RealPresence Collaboration Server
- Call Detail Records
- Restoring System Defaults
- Polycom Lab Features

Administration and Utilities

Topics:

This section describes the tasks that you may need to administer and maintain the RealPresence Collaboration Server.

Resource Management

This section describes how the MCU resources are managed by the MCU and how they are used by the MCU to connect participant to conferences.

This section describes:

- Forcing Video Resource Allocation to CIF Resolution
- Displaying Resource Report
- MCU Resource Management by Poly Clariti Manager, and Poly Clariti Core System

Force Video Resource Allocation to CIF Resolution

You can set the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters.

This forcing saves resources and enables more endpoints to connect to conferences.

The forcing is done by modifying the system configuration and it applies to all conferences running on the MCU.

You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. For example, you can force the system to allocate one CIF video resource to CMAD and VSX endpoints while HDX endpoints can connect using SD or HD video resources.

Once the endpoint connects to the conference, its type is identified by the RealPresence Collaboration Server and, if applicable, the RealPresence Collaboration Server will connect it using one CIF resource, even if a higher resolution can be used.

Procedure

1. In RMX Manager, go to **System Configuration**.
2. Add a new flag by the name: `FORCE_CIF_PORT_ALLOCATION`.
3. Set the flag value to the product type to which the CIF resource should be allocated. Possible values are `VSX nnnn`, where `nnnn` represents the model number, for example, VSX 8000.

   You can define several endpoint types, listing them one after the other separated by a semicolon.
4. Reset the MCU for changes to take effect.

Cancel the Forcing of Video Resource Allocation to CIF Resolution

You can cancel the forcing of video resource allocation to CIF resolution by modifying the system configuration.

This is applicable to all conferences running on the MCU.

Procedure

1. In RMX Manager, go to **System Configuration**.
2. Select the flag `FORCE_CIF_PORT_ALLOCATION` and clear its value.
3. In the **New Value** field, clear the value entries.
4. Click **OK**.
5. Reset the MCU for changes to take effect.

View the Resource Report

Resource allocations are described in AVC HD720p30 units, although they are used for both AVC and SVC ports.

A port ratio of 1 AVC HD port equals 2 AVC SD ports, or 5 SVC ports (in a non-mixed conference). When the RealPresence Collaboration Server is reporting the available capacity, it rounds up the remaining capacity to the nearest whole value of available ports.

For example, 1 to 5 SVC endpoints in a conference consume 1/5 to 1of the resource value, thus the resource report refers this as one full resource used. 6 to 10 SVC endpoints consume 1.2 to 2 of the resource value, thus the resource report refers this as two full resources used, and so forth.

The following table demonstrates the actual resource capacity utilization for both CP only and mixed CP and SVC conferences in AVC HD720p30 units.

Resource Capacity Allocation Per Port Type

Port Type	Non-Mixed Conferences	Mixed CP and SVC Conferences
AVC HD	1	1.5*
AVC SD	0.5	0.75*
AVC CIF	0.333	0.75*
SVC	0.2	0.333

* Resources are consumed at this rate only **after** the conference contains a mix of both AVC and SVC endpoints.

The **Resource Report** includes a graphic representation of the resource usage. One resource report is available for all resource usage including SVC-based endpoints.

Procedure

» In RMX Manager, go to **Administration** > **Resource Report**.

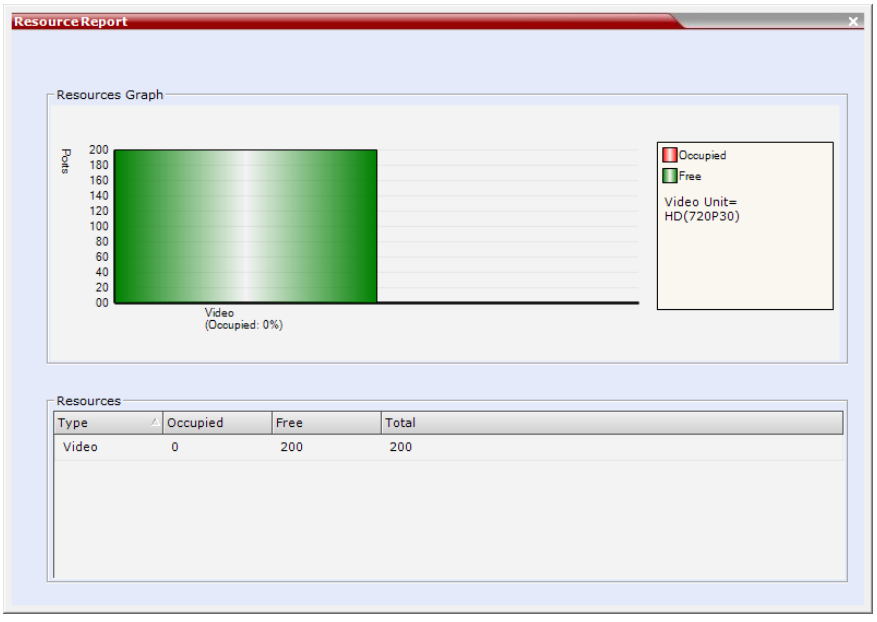
For each resource type, the **Resource Report** includes the following columns:

Column	Description
Type	The type of audio/video resources available.
Occupied	The number of MCU resources that are used by connected AVC and SVC-based participants or reserved for defined participants.
Free	The number of MCU resources available for connecting AVC and SVC-based endpoints.
Total	The total number of resources of that type, and their allocation status (**Occupied** and **Free**). This number reflects the current audio/video port configuration (for AVC and SVC-based conferencing). Changes in the resource allocation affect the resource usage displayed in the Resource Report.

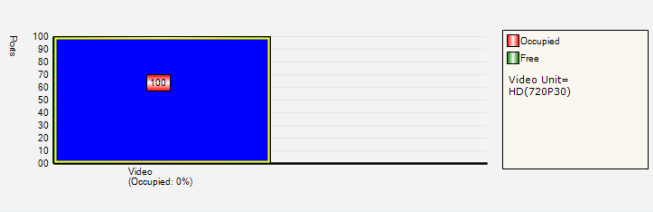
Resource Reports for RealPresence Collaboration Server 2000/4000

RealPresence Collaboration Server 2000/4000 do not differentiate between Video and Voice (Audio) resources.

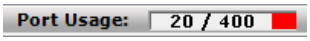
These MCUs allocate the same amount of system resources to Voice (Audio) participants, as those allocated to CIF Video participants.



The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph. Moving the cursor over the **Video** bar displays the following view:



The **Port Gauge** in the **Status Bar** show the numbers as they appear in the resource report. In the following example, 20 of the 400 system resources are shown as occupied.



Set the Port Usage Threshold

The RealPresence Collaboration Server can be set to alert the administrator to potential port capacity shortages.

A capacity usage threshold can be set as a percentage of the total number of licensed ports in the system. When the threshold is exceeded, a System Alert is generated. The default port capacity usage threshold is 80%.

The administrator can monitor the MCU port capacity usage via the **Port Gauge** in the **Status Bar** of the RMX Manager. The **Port Usage Gauge** displays for the RealPresence Collaboration Server:

- The total number of **Video** ports in the system.
- The number of **Video** ports in use.
- The **High Port Usage** threshold.

Procedure

1. In RMX Manager, go to **Setup** > **Port Gauge** to open the **Port Gauge** dialog.
2. Enter the value of the percentage capacity usage threshold.

   In HW MCUs, the value is applied to the Audio and video resources according to the Video/Voice Port Configuration.

   The high Port Usage threshold represents a percentage of the total number of video or audio ports available. It is set to indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes. The default port usage threshold is 80%.
3. Click **OK**.

View System Information

System Information includes License Information and general system information, such as system memory size and Media Card Configuration Mode.

Procedure

» In RMX Manager, go to **Administration** > **System Information**.

The following information displays:

System Information

Field	Description
Card Configuration Mode (RealPresence Collaboration Server 2000/4000)	The MCU configuration as derived from the installed media cards: • MPMRx - Currently only MPMRx cards are supported.
RMX Version	The RealPresence Collaboration Server Software Version.
Serial Number	The Serial Number of the RealPresence Collaboration Server unit.

Enable SNMP

Simple Network Management Protocol (SNMP) enables managing and monitoring of the MCU status by external managing systems, such as HP OpenView or through web applications.

The RealPresence Collaboration Server implementation of SNMPv3 is FIPS 140 compliant.

The addresses of the Managers monitoring the MCU and other security information are defined in the RMX Manager and are saved on the MCU hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the RMX Manager.

Procedure

1. In RMX Manager, go to **Setup** > **SNMP**.

   The **RMX SNMP Properties - Agent** dialog displays.
2. In the **Agent** dialog, select **SNMP Enabled**.
3. Click **Retrieve MIB Files** to obtain a file listing the MIBs defining the managed object properties.
4. Click **Browse** and navigate to the desired directory to save the MIB files.
5. Click **OK**.

   The path of the selected directory is displayed in the **Retrieve MIB Files** dialog.
6. Click **Save**.

   The MIB files are saved to the selected directory.
7. Click **Close** to exit the **Retrieve MIB Files** dialog.
8. In the **Agent** dialog, define the parameters allowing the SNMP Management System and its user to easily identify the MCU.

   RealPresence Collaboration Server-SNMP Properties - Agent Options

Field	Description
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.
MCU Location	Type the location of the MCU (address or any description).
MCU System Name	Type the MCU's system name.

9. Open the **Traps** tab.

Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the **Trap Destinations** field.

10. Define the following parameters:

Field	Description
SNMP Trap Version	Specifies the version, either Version 1 2 or 3 of the traps being sent to the IP Host. Polycom software supports the standard SNMP version 1 and 2 traps, which are taken from RFC 1215, convention for defining traps for use with SNMP. **Note:** The SNMP Trap Version parameters must be defined identically in the external SNMP application.
Trap Destination	This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent. • **IP** - Enter the IP address of the SNMP trap recipient. All Versions. • **Community Name** - Enter the Community Name of the manager terminal used to monitor the MCU activity. Version 1 and Version 2. • **User Name** - Enter the name of the user who is to have access to the trap. Version 3. • **Authentication Protocol** - Enter the authentication protocol: **MD5** or **SHA**. Version 3. • **Privacy Protocol** - Enter the privacy protocol: **DES** or **AES**. Version 3. • **Engine ID** - Enter an Engine ID to be used for both the Agent and the Trap. ◦ Default: Empty ◦ Version 3

11. Click **Add** to add a new Manager terminal.

Depending on the **SNMP Trap Version** selected, one of two **New Trap Destination** dialog opens.

12. Define the following parameters:

Field	Description	Version
IP Address	Enter the IP address of the SNMP trap recipient.	1,2,3
Enable Trap Inform	An Inform is a Trap that requires receipt confirmation from the entity receiving the Trap. If the Engine ID field (Version 3) is empty when Enable Trap Inform has been selected, the Engine ID is set by the Client.	1,2,3
Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	1, 2
User Name	Enter the name of the user who is to have access to the trap.	3

Field	Description	Version
Engine ID	Enter an Engine ID to be used for the Trap. This field is enabled when the Enable Trap Inform check box is selected. If the Enable Trap Inform check box is cleared the Engine ID of the Agent is used. The Engine ID is comprised of up to 64 Hexadecimal characters. Default: Empty	3
Security Level	Select a **Security Level** from the drop-down menu. Range: **No Auth, No Priv**; **Auth, No Priv**; **Auth, Priv** Default: **Auth, Priv**	3
Authentication Protocol	Enter the authentication protocol: **MD5** or **SHA**. The availability of the MD5 Authentication Protocol as a selectable option is controlled by adding the `SNMP_FIPS_MODE` System Flag to `system.cfg` and setting its value. A value of `YES` means that MD5 will neither be displayed as selectable option nor supported. Range: `YES`/`NO` Default: `NO`	3
Authentication Password		
Privacy Protocol	Enter the privacy protocol: **DES** or **AES**. The availability of the **DES** Privacy Protocol as a selectable option is controlled by adding the `SNMP_FIPS_MODE` System Flag to `system.cfg` and setting its value. A value of `YES` means that **DES** will neither be displayed as a selectable option nor supported. Range: `YES`/`NO` Default: `NO`	3
Privacy Password		3

13. Type the **IP Address** and the **Community name** of the manager terminal used to monitor the MCU activity, and then click **OK**.

The **Community name** is a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminal.

The new IP Address and Community name is added to the **Trap Destinations** field.

- To delete the IP Address of a Manager terminal, select the address you wish to delete, and click Remove.

  The IP address in the **Trap Destinations** field is removed.

14. Open the **Security** tab.

This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. When **Accept SNMP packets from all Hosts** is disabled, a valid query must contain the

appropriate community string and must be sent from one of the Manager terminals whose IP address is listed in this dialog.

15. Define the following parameters:

Field	Description		Version
Send Authentication Trap	Select this check box to send a message to the SNMP Manager when an unauthorized query is sent to the MCU. When cleared, no indication will be sent to the SNMP Manager.		Versions 1 & 2
Accept Host Community Name	Enter the string added to queries that are sent from the SNMP Manager to indicate that they were sent from an authorized source. **Note:** Queries sent with different strings are regarded as a violation of security, and, if the Send Authentication Trap check box is selected, an appropriate message is sent to the SNMP Manager.		Versions 1 & 2
Accept SNMP Packets from all Host	Select this option if a query sent from any Manager terminal is valid. When selected, the Accept SNMP Packets from These Hosts option is disabled.		Versions 1 & 2
Accept SNMP Packets from the following Hosts	Lists specific Manager terminals whose queries will be considered as valid. This option is enabled when the Accept SNMP Packets from any Host option is cleared.		Versions 1 & 2
User Name	Enter a User Name of up to 48 characters Default: Empty		Version3
Security Level	Select a Security Level from the drop-down menu. Range: **No Auth, No Priv**; **Auth, No Priv**; **Auth, Priv** Default: **Auth, Priv**		Version3
Authentication Protocol	Select the authentication protocol Range: **MD5**, **SHA** Default: **MD5**	These fields are enabled if **Authentication** is selected in the **Security Level** field.	Version3

Field	Description		Version
Authentication Password	Enter an Authentication Password. Range: 8 - 48 characters Default: Empty	These fields are enabled if **Authentication** is selected in the **Security Level** field.	Version3
Privacy Protocol	Select a Privacy Protocol. Range: **DES**, **AES** Default: **DES**	These fields are enabled if **Privacy** is selected in the **Security Level** field.	Version3
Privacy Password	Enter a Privacy Password. Range: 8 - 48 characters Default: Empty	These fields are enabled if **Privacy** is selected in the **Security Level** field.	Version3
Engine ID	Enter an Engine ID to be used for both the Agent and the Trap. Default: Empty	These fields are enabled if **Privacy** is selected in the **Security Level** field.	Version3

16. To specifically define valid terminals, de-select the **Accept SNMP Packets from any Host** check box, and click **Add**.

    The **Accepted Host IP Address** dialog opens.
17. Enter the IP Address of the Manager terminal from which valid queries may be sent to the MCU, and click **OK**.
18. Click **Add** to define additional IP Addresses.

    The IP Address or Addresses are displayed in the **Accept SNMP Packets from These Hosts** box.

Note: Queries sent from terminals not listed in the **Accept SNMP Packets from These Hosts** box are regarded as a violation of the MCU security, and if **Send Authentication Trap** is enabled, an appropriate message is sent to all the terminals listed in the **SNMP Properties - Traps** dialog.

19. In the **SNMP Properties - Security** dialog, click **OK**.

Managing Configuration Files

The **Software Management** menu is used to backup and restore the RealPresence Collaboration Server's configuration files and to download MCU software.

Software Management operations include:

- Configuration files backup

- Configuration files restoring
- RealPresence Collaboration Server software files download
  - SNMP settings
  - Time configuration
- CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

Back Up Configuration Files

This section describes the guidelines for backing-up Configuration Files.

Backup and Restore Guidelines are:

- Direct access to the RealPresence Collaboration Server file system is disabled in both Ultra Secure Mode and standard security mode.
- System Backup can only be performed by an administrator.
- The System Backup procedure creates a single backup file that can be viewed or modified only by developers.
- A System Backup file from one RealPresence Collaboration Server can be restored on another of the same type.
- To ensure file system consistency, do not perform any configuration changes as the system does not suspended them during the backup procedure.
- The following parameters, settings and files are backed up:
  - MCMS configuration files (/mcms/Cfg):
  - Network and service configurations
  - Rooms
  - Profiles
  - Reservations
  - System Flags
  - Resource Allocation
  - IVR messages, music
  - RealPresence Collaboration Server Web Client user setting - fonts, windows
  - RealPresence Collaboration Server Web Client global settings - notes, address book, language
  - Private keys and certificates (TLS)
  - Conference participant settings
  - Operation DB (administrator list)

Procedure

1. In RMX Manager, go to **Administration** > **Software Management** > **Backup Configuration**.

   The **Backup Configuration** dialog opens.
2. Browse to select the **Backup Directory Path**, and click **Backup**.

Note: Changes made during RealPresence Collaboration Server system backup are not registered.

Restore Configuration Files

You can restore configuration files from the RMX Manager.

Procedure

1. In RMX Manager, go to **Administration** > **Software Management** > **Restore Configuration**.
2. Browse to the **Restore Directory Path** where the backup configuration files are stored, and click **Restore**.

Download Configuration Files

You can download and install configuration files from the RMX Manager.

Procedure

» In RMX Manager, go to **Administration** > **Software Management** > **Software Download**.

Browse to the **Install Path**, and click **Install**.

Hot Backup

Hot backup implements a high availability and rapid recovery solution.

Two RealPresence Collaboration Servers are configured in a primary/secondary relationship: the primary MCU is active while the secondary acts as a passive, fully redundant hot backup of the primary MCU.

All conferencing activities and configuration changes that do not require a System Reset are mirrored on the secondary MCU five seconds after they occur on the primary MCU.

In the event of failure of the primary MCU, the secondary MCU transparently becomes active and assumes the activities and functions with the backed up settings of the failed primary MCU. Both dial-in and dial-out participants are automatically dialed out and reconnected to their conferences. However, the hot backup solution is optimized for dial-out participants as all the dial-out numbers are defined in the system and are available for redialing.

The following entities are automatically backed up and updated on the secondary MCU:

- Ongoing Conferences
  - Layout
  - Video Force
  - Participant Status (Muted, Blocked, Suspended)
- Reservations
- Meeting Rooms
- Entry Queues
- SIP Factories
- Gateway Profiles
- IVR services (excluding .wav files)
- Recording Link
- Profiles
- IP Network Settings:

- H.323 settings
- SIP settings
- DNS settings
- Fix Ports (TCP, UDP) settings
- QoS settings

The guidelines for Implementing hot backup are:

- Both primary and secondary MCUs must have the same software version installed.
- The Users list and Passwords must be the same on both the primary and secondary MCUs.
- There must be connectivity between the primary and secondary MCUs, either on the same network or on different networks connected through routers.
- In the event of failure of the primary MCU the secondary MCU assumes the role of the primary MCU. The primary/secondary relationship is reversed: the secondary, now active, remains the primary and the previous primary MCU, when restarted, assumes the role of secondary MCU.
- No changes to the secondary MCU are permitted while it is functioning as the hot backup. Therefore no ongoing conferences or reservations can be added manually to the secondary MCU.
- If hot backup is disabled, all ongoing conferences and Reservations backed up on the secondary MCU are automatically deleted.
- In hot backup configuration, the SIP and H.323 Authentication configuration of the User Name and Password in the IP Network Service Properties - Security tab of the primary RealPresence Collaboration Server are not backed up in the secondary RealPresence Collaboration Server.
- Primary and secondary initial roles can be reversed only after all ongoing conferences and Reservations are deleted.
- Changes to the primary MCU that require a System Reset can only be made after hot backup is disabled.
- RealPresence Collaboration Server 2000/4000 only: Video/Voice Port Configurations on the primary MCU are not synchronized with the secondary MCU. You must manually set the Video/Voice Port Configurations on both the primary and secondary MCUs to the same level.

Enable Hot Backup

You can enable hot backup by using the RMX Manager.

Procedure

1. In RMX Manager, go to **Setup** > **Hot Backup**.

   The **Hot Backup** dialog is displayed.
2. Complete or modify the following fields:

Field	Description
Hot Backup Enabled	Select this check box to enable hot backup.
MCU Role	This setting determines the role of the MCU in the hot backup configuration. Select either **Primary MCU** or **Secondary MCU** from the drop-down menu.

Field	Description
Paired MCU IP Address	Enter the Control Unit IP Address of the: • Secondary MCU (if this MCU is the primary) • Primary MCU (if this MCU is the secondary)
Synchronization Status	The status of the synchronization between the primary and secondary MCUs in the hot backup configuration is indicated as: • OK - Hot backup is functioning normally, and the primary and secondary MCUs are synchronized. • Attempting - Hot backup is attempting to synchronize the primary and secondary MCUs. • Fail - A failure occurred while trying to synchronize the paired MCUs. • None - Hot backup has not been enabled.

3. Click **OK**.

Configure the Hot Backup Triggers

Hot backup is initiated by the secondary MCU on detection of no response from the primary MCU on a keep alive operation.

The hot backup triggers initiates the hot backup swap from primary to secondary when the selected conditions on the primary MCU occur.

The guidelines for configuring hot backup triggers are:

- Hot backup triggers should be configured on both the primary and secondary MCUs.
- Hot backup triggers are not synchronized between the primary and secondary MCUs.

The hot backup triggers are configured in the **Hot Backup** dialog for the primary MCU when the hot backup feature is enabled.

Procedure

1. In RMX Manager, go to **Setup** > **Hot Backup**.
2. In the **Hot Backup** dialog, expand the **Hot Backup Triggers**.

   A dialog opens with a list of event triggers displayed.
3. Select the appropriate **Hot Backup Triggers** check boxes:

Hot Backup Trigger	Description
Lost connection with management port	Initiates the hot backup switch from the primary to the secondary MCU when the connection to the management port is lost on the primary MCU. This trigger is always set.
Lost connection with media port	Initiates the hot backup switch from the primary to the secondary MCU when the connection with an active media port is lost on the primary MCU.

Hot Backup Trigger	Description
Lost connection with signalling port	Initiates the hot backup switch from the primary to the secondary MCU when the connection with an active signaling port is inactive for a duration of 30 seconds on the primary MCU. A system flag, `ETH_INACTIVITY_DURATION`, can be added and configured to modify the duration of inactivity of the signaling port. Default value is 30 seconds; Minimum value is 20 seconds.
Lost connection with ISDN (audio/ video) card	Initiates the hot backup switch from the primary to the secondary MCU when the connection with an ISDN (audio/video) card is disconnected on the primary MCU.

4. Alternatively, click **Trigger Failover Manually** when you want to trigger the hot backup manually and activate the secondary MCU.

   A confirmation message is displayed.
5. Click **Yes** to continue the hot backup process or **No** to cancel the hot backup process.
6. Click **OK**.

Modify the Primary MCU Configuration

Modifications to the configuration of the primary MCU that require a system reset cannot be performed while hot backup is enabled.

Procedure

1. In RMX Manager, go to **Setup** > **Hot Backup**.
2. Disable the **Hot Backup** on the primary and secondary MCUs.
3. Modify the primary MCUs configuration.
4. Reset the primary MCU.
5. When the reset is complete, enable **Hot Backup** on the primary and secondary MCUs.
6. If required, reset the secondary MCU.

Ping the RealPresence Collaboration Server

The Ping administration tool enables the RealPresence Collaboration Server Signaling Host to test network connectivity by Pinging IP addresses.

- The IP addressing mode can be either IPv4 or IPv6.
- Both explicit IP addresses and Host Names are supported.
- The RMX Manager blocks any attempt to issue another Ping command before the current Ping command has completed. Multiple Ping commands issued simultaneously from multiple RMX Web Clients are also blocked.

Procedure

1. In RMX Manager, go to **Administration** > **Tools** > **Ping**.
2. Modify or complete the following fields:

Field	Description
IP Version	Select **IPv4** or **IPv6** from the drop-down menu.
IP Address	Enter the **IP Address** of the network entity to ping.

3. Click **Ping**.

   The Ping request is sent to the IP Address of the RealPresence Collaboration Server entity. The Answer is either OK or FAILED.

Configure Notification Settings

This section describes the process to configure notification settings.

The RealPresence Collaboration Server can display notifications when:

- A new RealPresence Collaboration Server user connects to the MCU.
- A new conference is started.
- Not all defined participants are connected to the conference or when a single participant is connected.
- A change in the MCU status occurs and an alarm is added to the alarms list.

  A welcome message is displayed to the RealPresence Collaboration Server user upon connection.

Procedure

1. In RMX Manager, go to **Setup** > **Notification Settings**.

   The following notification options are displayed.

Field	Description
New Connection	Notification of a new user/administrator connecting to the RealPresence Collaboration Server.
New Conference Created	New conference has been created.
Conference Not Full	The conference is not full and additional participants are defined for the conference.
Welcome Message	A welcome message after user/administrator logon.
Active Alarms Update	Updates you of any new alarm that occurred.
Fault List Updated	Updates you when the faults list is updated (new faults are added or existing faults are removed).

2. **Enable/Disable All Notifications** or **Custom** to select specific notifications to display.
3. Click **OK**.

ActiveX Bypass

At sites that, for security reasons, do not permit Microsoft ActiveX to be installed, you can use the MSI (Windows Installer File) utility to install .NET Framework and .NET Security Settings components on workstations throughout the network.

All workstation that connect to RealPresence Collaboration Server systems must have both.NET Framework and .NET Security Settings running locally. These components are used for communication with the RealPresence Collaboration Server and can only be installed on workstations by users with administrator privileges.

The MSI utility requires the IP addresses of all the RealPresence Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation is to connect to.

If the IP address of the any of the target RealPresence Collaboration Server is changed, the ActiveX components must be reinstalled.

Install ActiveX

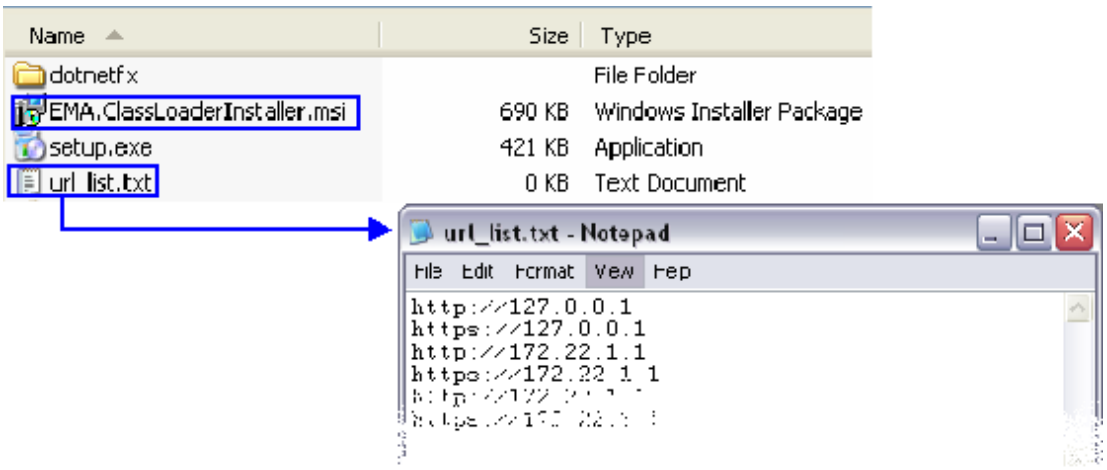
You can install ActiveX components on all workstations in the network via the Polycom Resource center.

Procedure

1. Download the MSI file `EMA.ClassLoaderInstaller.msi` from the Polycom Resource Center.

   The MSI file contains installation scripts for both .NET Framework and .NET Security Settings.
2. Create a text file to be used during the installation, containing the IP addresses of all the RealPresence Collaboration Server (both control unit and Shelf Management IP addresses) that each workstation in the network should connect.

   The file must be named `url_list.txt` and must be saved in the same folder as the downloaded MSI file.



3. Install the ActiveX components on all workstations on the network that connect to RealPresence Collaboration Server systems.

   The installation is done by the network administrator using a 3rd party network software installation utility and is transparent to all other users.

RealPresence Collaboration Server Reset

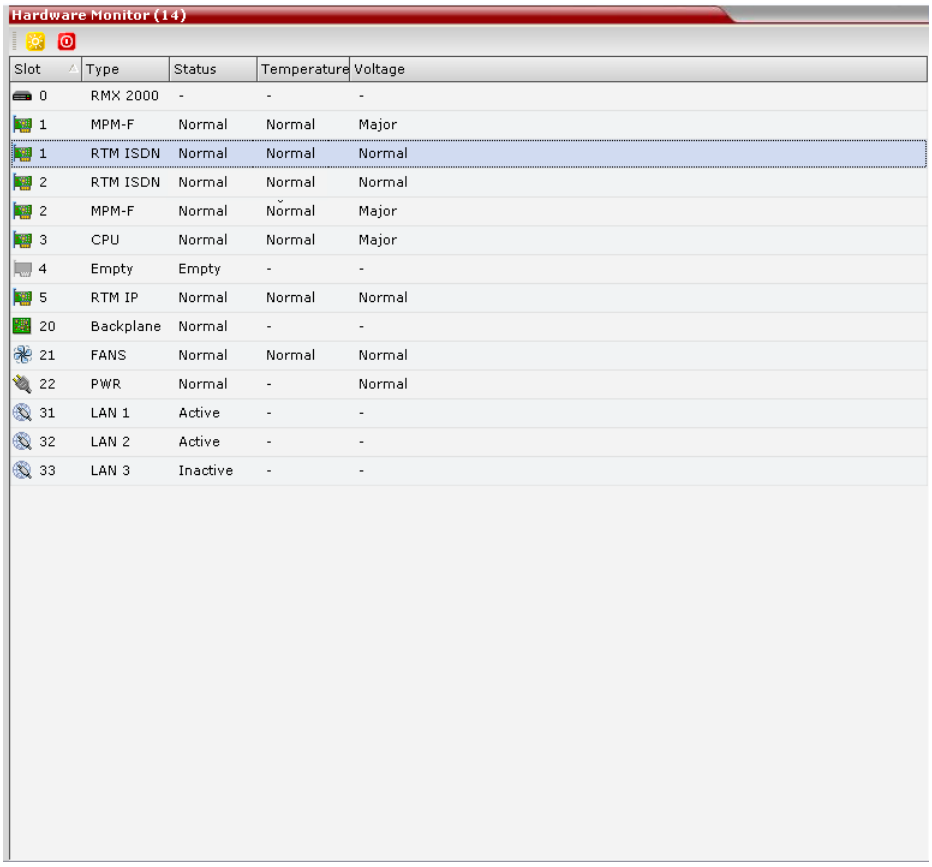
There are separate procedures for resetting RealPresence Collaboration Server 1800/2000/4000 and RealPresence Collaboration Server, Virtual Edition.

Reset the RealPresence Collaboration Server 18002000/4000

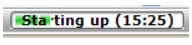
System Reset saves system configuration changes and restarts the system with the latest settings.

Procedure

1. In RMX Manager, go to the **RMX Management** pane and select **Hardware Monitor**.
2. Click **Reset** .



When the RealPresence Collaboration Server system is reset, during RealPresence Collaboration Server startup the **Progress Bar** appears at the bottom of the RealPresence Collaboration Server **Status** pane, displaying the amount of time remaining for the reset process to complete:



The Startup progress is also indicated by a green progress bar.

Startup duration depends on the activity preceding the MCU reset (such as Fast Configuration Wizard, New Version installation, Version Upgrade, Restore Last Configuration, etc.).

Note: Resetting the RealPresence Collaboration Server from the Hardware Monitor may not disconnect SIP endpoints previously connected even though the conference ends.

Reset RealPresence Collaboration Server, Virtual Edition

RealPresence Collaboration Server Virtual Edition may be deployed using different virtual platforms, and for each, a different restart method should be used, depending on the vendor.

Note: The System Reset option doesn't actually reboot the Virtual Machine, it only restarts the MCU service.

Procedure

» Refer to the instructions for your virtual instance platform:

- VMWare
- Hyper-V

Hardware Monitoring

Topics:

For the of the RealPresence Collaboration Server, Appliance Edition, 1800, 2000, and 4000, use the **Hardware Monitor** option to monitor the status and properties of MCU hardware components.

View the Status of the Hardware Components

For RealPresence Collaboration Server 2000/4000 models (also called MCUs), the **Hardware Monitor** connects to the MCU Shelf Management Server to provide hardware status information.

Procedure

» In the **RMX Management** section, click **Hardware Monitor**  .

The **Hardware Monitor** displays the list of monitored hardware (which will vary depending on the product model) and the following information about the hardware.

Field	Description
Slot	Displays an icon according to the hardware component type and the slot number. The icon displays the hardware status as follows: • An exclamation point (!) indicates errors in the hardware component. • Card icon with the reset button () indicates that the hardware component is currently resetting. • Card icon with diagnostic tools () indicates that the hardware component is in diagnostic mode.
Type	The type of hardware component.
Status	The current status of the hardware component; **Normal, Major**, **Critical**, **Resetting**, **Diagnostics**, or **Empty**.
Temperature	Monitors the temperature of the hardware components; **Normal**, **Major**, and **Critical**. **Note:** **Critical** condition invokes a system shut-down.

Field	Description
Voltage	The voltage threshold of the hardware component; either **Normal** or **Major**.

Identify the Types of Video Cards in an MCU

For RealPresence Collaboration Server 2000/4000 models, MCU features and functions may depend on the type of video cards within the MCU.

Use the **Hardware Monitor** to identify the types of video cards in an MCU.

This procedure doesn't apply to a RealPresence Collaboration Server 1800.

Procedure

1. In the **RMX Management** section, click **Hardware Monitor**  .

   The type of video card is indicated in the **Type** column.
2. To view the properties of a video card, in the **Hardware Monitor**, select the card of interest.
3. Right-click and select **Properties**.
4. Select the **Event Log** tab (if available) to view a log of events recorded by the MCU on the card.
5. Select the **Active Alarms** tab (if available) to view alarms related to the card, that is, temperatures and main power sensors.
6. Click **Close** to return to the **Hardware Monitor**.

View the Properties of Hardware Components

Use the **Hardware Monitor** to view the properties of MCU hardware components.

The properties displayed will depend on the type of component it is. Hardware components properties are grouped as follows:

- MCU Properties.
- Card Properties (MPMRx, CNTL/CNTL 4000, RTM IP, RTM ISDN, DSP card, RTM LAN, RTM-IP 4000).
- Supporting Hardware Components Properties (Backplane, FANS, LAN, PWR).

Procedure

1. In the **RMX Management** section, click **Hardware Monitor**  .
2. In the **Hardware Monitor**, select the component of interest (for example, Slot 0 RMX 4000).
3. Right-click and select **Properties**.

   For more information about the hardware properties displayed, see the hardware guide for the RealPresence Collaboration Server (RMX) appliance model you have.

View an MCU or Video Card Event Log

For RealPresence Collaboration Server 2000/4000 models, use the **Hardware Monitor** to view the MCU or video card event logs.

This procedure doesn't apply to a RealPresence Collaboration Server 1800.

Procedure

1. In the **RMX Management** section, click **Hardware Monitor**  .
2. In the **Hardware Monitor**, select the MCU or video card of interest.
3. Right-click and select **Properties**.
4. Click **Event Log** to view a log of events that were recorded by the MCU.
5. The logged events can be saved to a *.xls file by clicking **Save Event Log**. It isn't possible to save individual or multiple selected events; the entire log file must be saved.

View Active Alarms for an MCU

For RealPresence Collaboration Server 2000 and 4000 models, use the **Hardware Monitor** to view the MCU event log.

This procedure doesn't apply to a RealPresence Collaboration Server 1800.

Procedure

1. In the **RMX Management** section, click **Hardware Monitor**  .
2. In the **Hardware Monitor**, select the MCU of interest (for example, Slot 0 RMX 4000).
3. Right-click and select **Properties**.
4. Select the **Active Alarms** tab to view alarms for the MCU, such as temperatures and main power sensors.

   The **Active Alarms** dialog displays fields relating to faults and errors detected by sensors on the MCU. It includes a **Hardware Alarm List** and a **Software Alarm List**. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).
5. To save the two alarms lists to *.xls files, click **Save Hardware Alarm List** and **Save Software Alarm List** respectively.

Note: For RealPresence Collaboration Server (RMX) 2000 and 4000 systems, if you connect the Hardware Monitor via the Shelf Management server, the **Software Alarm List** section isn't displayed.

Run System Diagnostics

Administrators can use the **Hardware Monitor** to run the MCU diagnostics tool, which is a debugging tool that detect malfunctions in the hardware components' performance.

The MCU can run diagnostics on the MFA, CPU, and Switch (Cards: MPMRx, DSP media cards, CPU, RTM IP, and RTM ISDN) only.

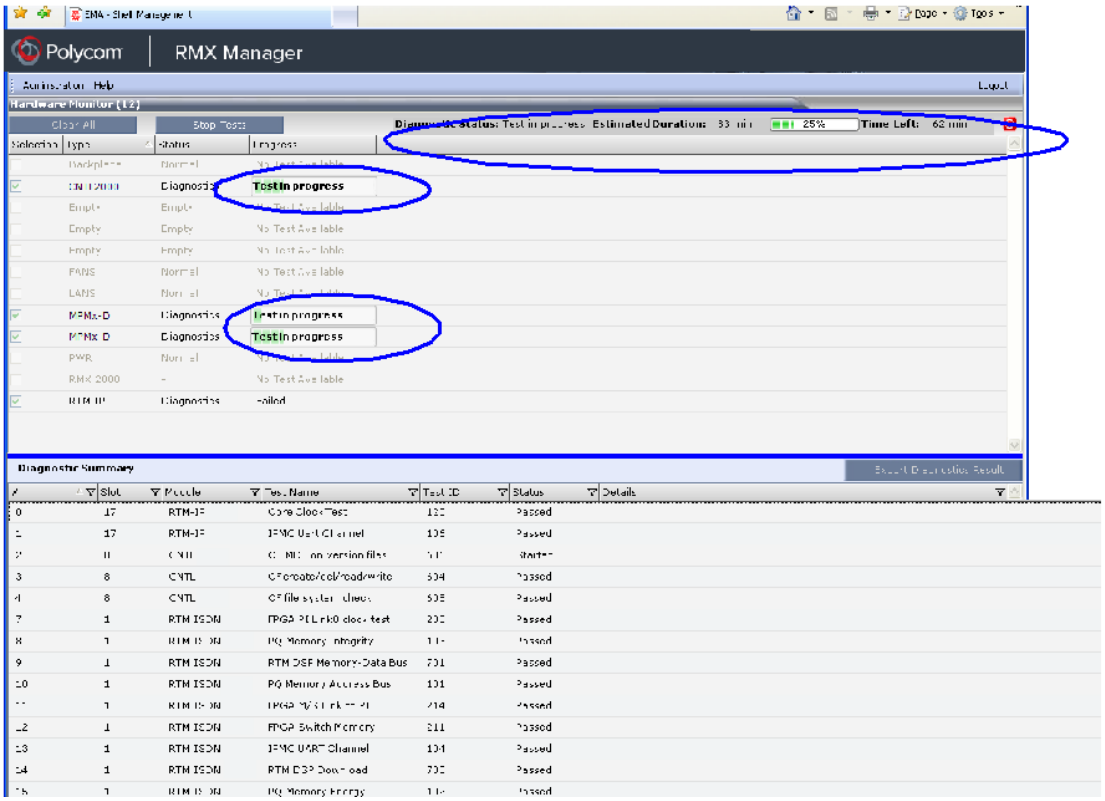
When the diagnostic tool is initialized, the MCU is reset and upon restarting, the MCU enters Diagnostic Mode. Entering this mode causes the MCU to terminate all active conferences and prohibits conferences from being started.

To access an MCU in Diagnostic Mode, the administrator must use the MCU Shelf Management IP address.

Procedure

1. In the **RMX Management** section, click **Hardware Monitor** .
2. In the **Hardware Monitor**, click **Active Diagnostic Mode** .
3. Click **Yes** to confirm.

   The MCU restarts.
4. Do one of the following:
   - For RealPresence Collaboration Server (RMX) 2000 and 4000 models, when the RMX Web Client reopens to the **Shelf Manager IP address**, log in as administrator.
   - For RMX 1800 models, re-enter the MCU system management IP in the browser address to access the RMX Web Client and log in as administrator.
5. To run diagnostics on one or several cards, select the cards and select **Run Tests**.
6. To stop the diagnostic tests, click **Stop Tests**.



7. When the tests are completed, to download a report for analysis click Export Diagnostics Result.
8. To exit Diagnostic Mode and reset the MCU, in the **Hardware Monitor**, click .

ISDN Diagnostic on RMX 1800

This section describes the ISDN Diagnostic supported on RMX 1800

RMX 1800 MCUs support the following diagnostic items:

- RTM DSP Memory-Data Bus.
- RTM DSP Memory-Address Bus.
- RTM DSP Memory-Energy.
- RTM DSP Memory-Integrity
- RTM DSP Core clock
- RTM DSP T1 FLAC3 Diag
- RTM DSP E1 FLAC3 Diag

Troubleshoting: Perform diagnostic on RMX 1800

If you perform diagnostics on an RMX 1800 MCU that has ISDN cards through the USB utility, the diagnostic program will check all items including DSP, system memory, and ISDN cards. The program will take about one hour to complete all tests.

Once you perform diagnostic on T1, you'll fail the diagnostic on E1. To carry out diagnostic on E1 perform the following steps:

Procedure

1. Reboot the system.
2. Re-enter Diagnostic Mode.
3. Perform diagnostic on E1.

Troubleshoting: Diagnostic fails on RMX 1800

Once RTM DSP T1 FLAC3 Diag or RTM DSP E1 FLAC3 Diag fails, you'll fail the diagnostic on other items.

Perform the following steps to troubleshoot it:

Procedure

1. Reboot the system.
2. Re-enter Diagnostic mode.
3. Perform the diagnostic.

Media Traffic Shaping

Topics:

Polycom integrated traffic shaping capabilities into the RealPresence Collaboration Server to enable deploying RealPresence Collaboration Server in networks limiting packet bursts within 100ms time intervals (or more).

Setting router policies to limiting of bandwidth within a time interval, causes the router to drop packets exceeding the allowed bandwidth within this interval. Therefore, using this feature enables the RealPresence Collaboration Server to flatten the traffic, and minimize traffic bursts, without exceeding the bandwidth allowed within the time interval.

Though the RealPresence Collaboration Server supports high-level network features, high Quality of Service requires end-to-end video network operation. The RealPresence Collaboration Server traffic shaping capabilities can't compensate for network level violations/limitations generated by elements outside the RealPresence Collaboration Server, such as endpoints, routers, etc.

Traffic shaping can flatten a momentary burst (meaning, within a 100ms time interval). However, it can't "flatten" longer bursts resulting from endpoints sharing content in video switching conferences. Similarly, this feature helps reducing packets dropping by routers following momentary traffic bursts, yet it doesn't resolve packet lost by faulty network connections or network congestion.

Note that during VSW content sessions, should source endpoint exceed the negotiated content rate for over 100ms, the RealPresence Collaboration Server can flatten the video channel but not the incoming content channel.

Note: Currently, traffic shaping is limited to conferences using a minimum of 384 bit rate. Under this bit rate, the user might experience bursts of data.

Traffic Shaping Guidelines

Refer to the following guidelines when using traffic shaping.

- Traffic shaping is applied in the following conferencing modes and scenarios:
  - AVC conferences (both CP and VSW)
  - Mixed CP and SVC conferences - applied only on AVC endpoints
  - Content VSW

  This feature isn't applied on TIP endpoints.
- Traffic shaping code is embedded in the DSP ART modules thus requiring enlarging PCI memory size to 18Mbps, and content memory size to that of video.
- Should license port capacity be lower than the number of hardware ports, the unlicensed ports are used for traffic shaping to decrease capacity reduction.
- Traffic shaping is applied on the aggregation of both content and people channels.
- Delays due to traffic shaping, if any, are limited to 10ms.
- This feature isn't applied on audio, since the encoder output audio rate is constant.

- When Polycom Lost Packet Recovery (LPR) is enabled, traffic shaping is applied following packets repair and before packets sending.

Traffic Shaping System Flags

This section describes the system flags used to control Traffic Shaping usage.

Traffic shaping usage is controlled by RealPresence Collaboration Server configuration system flags (for the entire bridge):

- `ENABLE_RTP_TRAFFIC_SHAPING` - Enables traffic shaping. When set to `YES`, traffic shaping is applied to all ports, resulting in some port capacity reduction. When set to `NO`, traffic shaping is disabled.
- `VIDEO_BIT_RATE_REDUCTION_PERCENT`- Indicates the percentage of actual reduction in bit rate sent from the MCU to the endpoint (negotiated bit rate is not reduced). This flag is applicable only when traffic shaping is enabled (`ENABLE_RTP_TRAFFIC_SHAPING` set to `YES`).

  Range: 0-60; Default value: 15
- `TRAFFIC_SHAPING_MTU_FACTOR` - Used for the MTU (Maximum transmitting Unit - the size of transmitted packets) dynamic calculation:

  New MTU = video bit rate / TRAFFIC_SHAPING_MTU_FACTOR

  Where the new MTU value is guaranteed to be a minimum of 410, and a maximum of 1460 (MAX_MTU). The purpose of this calculation is to match video rate in outgoing video to call rate, yet force lower encoder bit rates to avoid overflow.

  This flag is applicable only when traffic shaping is enabled.

  Range: 0-5000, where 0 signifies no change in MTU; Default value: 800

To modify any of these flags, manually add them into the MCMS user parameters section of the system configuration flags, and then modify their value.

Capacity Reduction During Traffic Shaping

The table below describes the maximum capacity left after reduction due to traffic shaping in RealPresence Collaboration Servers 2000/4000.

There's no capacity reduction in RealPresence Collaboration Servers 1800 and Virtual Edition.

Capacity Reduction

Resolution	Nonmixed Mode	Mixed Mode
CIF	150*	100*
SD	150 *	100*
HD720p	100	66
HD1080p	50	40
Audio Only	300	150

* Assuming conference bit rate ≤1024 Kbps

Direct Connection to the RealPresence Collaboration Server

Topics:

Connect to the RealPresence Collaboration Server 1800/2000/4000 directly to perform certain tasks.

You can perform the following tasks with direct connection to the RealPresence Collaboration Server:

- Connect to and modify the RealPresence Collaboration Server factory default management network settings without using the USB flash drive.
- Connect to the RealPresence Collaboration Server 2000/4000 alternate management network for support purposes.
    - While separate from all other networks, the alternate management network functions identically to the management network. However, you can't configure it and it operates based on factory defaults only
    - Connection to the alternate management network bypasses LAN and firewall security. Strictly control access to the LAN 3 port.
    - You can only access the alternate management network if you haven't performed network separation.
- Connect to the RealPresence Collaboration Server 2000/4000 via a modem.

You can't directly connect to the RealPresence Collaboration Server with the following editions or modes:

- RealPresence Collaboration Server, Virtual Edition
- Ultra Secure Mode

Establishing a Direct Connection to the RealPresence Collaboration Server

To establish a direct connection to the RealPresence Collaboration Server, you must configure the connecting workstation, connect the cables between the workstation and the MCU, and connect the MCU to the RMX Web Client.

Configure the Connecting Workstation

You must first configure the connecting workstation using the Windows New Connection Wizard before you connect to the RealPresence Collaboration Server.

Follow these guidelines when configuring the connecting workstation:

- The workstation's IP address must be in the same network neighborhood as the RealPresence Collaboration Server control unit IP address.

- The subnet mask and default gateway addresses should be the same as those for the RealPresence Collaboration Server management network.
- Don't use the reserved IP addresses listed in the following table for the IP address:

Reserved IP Addresses

Network Entity	Management Network (Factory Default) IP Address	Alternate Network IP Address
Control Unit IP Address	192.168.1.254	169.254.192.10
Control Unit Subnet Mask	255.255.255.0	255.255.240.0
Default Router IP Address	192.168.1.1	169.254.192.1
Shelf Management IP Address	192.168.1.252	169.254.192.16
Shelf Management Subnet Mask	255.255.255.0	255.255.240.0
Shelf Management Default Gateway	192.168.1.1	169.254.192.1

See the workstation's operating system documentation for specific information about how to configure the network values.

Procedure

» Launch the Windows New Connection Wizard and configure the following workstation settings for either the default management network or the alternate management network:
- IP address
- Subnet mask
- Default gateway

Cable the Workstation Connection to the RealPresence Collaboration Server

Direct connect to the RealPresence Collaboration Server is achieved by correct cabling.

Procedure

1. Using a LAN cable, connect the workstation:
   - To the LAN 1 Port on the RealPresence Collaboration Server (RMX) 1800 back panel.
   - To the LAN 2 Port on the RealPresence Collaboration Server (RMX) 2000/4000 back panel.

Figure 51: RealPresence Collaboration Server (RMX) 1800

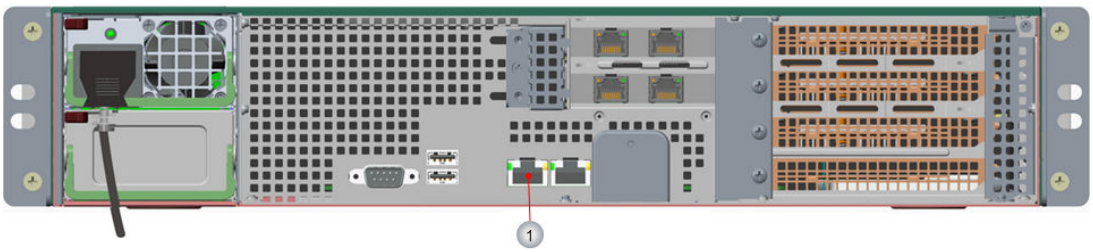


Figure 52: RealPresence Collaboration Server (RMX) 2000

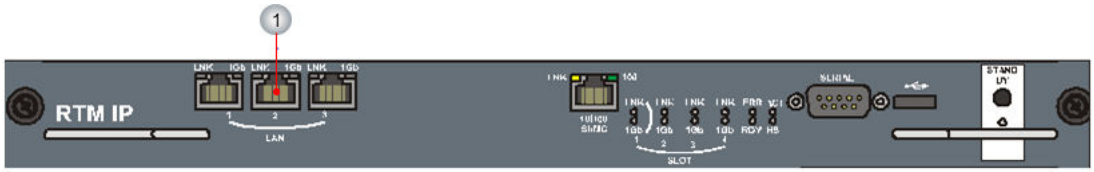


Figure 53: RealPresence Collaboration Server (RMX) 4000

2. Connect the power cable and power the RealPresence Collaboration Server `On`.

Connect to the MCU with the RMX Web Client

Use the RMX Web Client to directly access to a single RealPresence Collaboration Server, Appliance Edition.

Procedure

1. Open Internet Explorer browser window, enter the factory setting Management IP address in the browser's address line, and press **Enter**.
2. In the RMX Web Client Login screen, enter the default **Username** (`POLYCOM`) and **Password** (`POLYCOM`) and click **Login**.

   The Fast Configuration Wizard launches.

   For more information on First-time Power-up and the Fast Configuration Wizard, see the *Polycom RealPresence Collaboration Server Getting Started Guide*.

Configure the Primary Management Network

You can configure the Primary Management Network by using the Fast Configuration Wizard.

Procedure

1. Enter the following parameters into the Fast Configuration Wizard using the information supplied by your network administrator:
   - Control Unit IP Address
   - Shelf Management IP Address
   - Control Unit Subnet Mask
   - Default Router IP Address
2. Click **Save & Close**.

   The system prompts you to sign in with the new **Control Unit IP Address**.
3. Disconnect the LAN cable between the workstation and the LAN 2 Port on the RealPresence Collaboration Server's back panel.
4. Connect LAN 2 Port on the RealPresence Collaboration Server's back panel to the local network using a LAN cable.

5. Enter the new **Control Unit IP Address** in the browser's address line, using a workstation on the local network, and press **Enter** to start the RMX Web Client application.
6. In the RealPresence Collaboration Server Web Client Login screen, enter the default **Username** (`POLYCOM`) and **Password** (`POLYCOM`) and click **Login**.

Connect RealPresence Collaboration Server 2000/4000 to the Alternate Management Network

The alternate management network enables direct access to the RealPresence Collaboration Server 2000/4000 for support purposes.

You can't configure the alternate management network, as it operates solely on factory defaults.

You can access the alternate management network only via a LAN cable, connecting the preconfigured workstation to the appropriate port on the RealPresence Collaboration Server:

- RealPresence Collaboration Server (RMX) 2000 - LAN 3 port
- RealPresence Collaboration Server (RMX) 4000 - LAN 1 port

Figure 54: RealPresence Collaboration Server (RMX) 2000

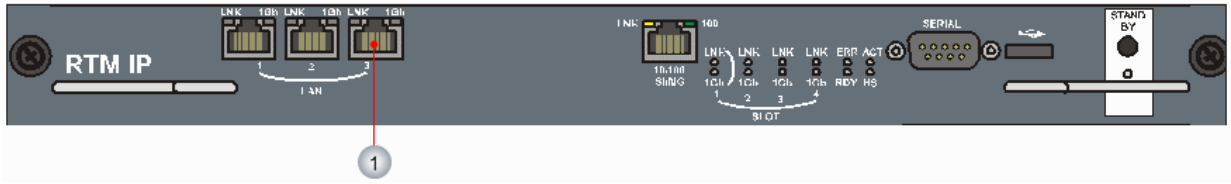
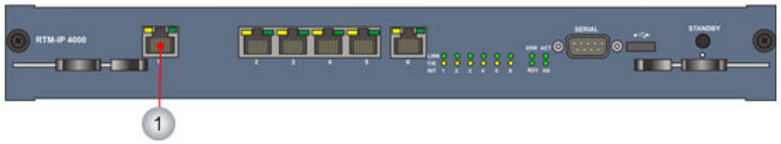


Figure 55: RealPresence Collaboration Server (RMX) 4000



Procedure

1. Connect the cable between the relevant RealPresence Collaboration Server port and the LAN port configured on the workstation.
2. Start the RMX Web Client application on the workstation, by entering `http://169.254.192.10` the **Control Unit IP Address** in the browser's address line and press **Enter**.

   The **RealPresence Collaboration Server Welcome Screen** dialog displays.
3. Enter the administrator's **Username** and **Password**, and click **Login**.

   The RMX Web Client starts. You can manage the RealPresence Collaboration Server in the same manner as if you had logged on to the regular management network.

Related Links

Alternate Management Network on page 342

Connect to RealPresence Collaboration Server 2000/4000 via Modem

You can remotely access the RealPresence Collaboration Server alternate management network via an external PSTN/IP modem.

Procedure

1. Install the RMX Manager.

   The web client enables direct access to the RealPresence Collaboration Server for support purposes.
2. Assign the modem an IP address on a specific subnet in the alternate management network by configuring the modem with the following settings:
   - **IP address** - near 169.254.192.nn
   - **Subnet Mask** - 255.255.240.0
3. Create a dial-up connection using the Windows **New Connection Wizard**.

   You only need to perform this procedure once, but you can modify the **Dial** field in the **Connect** applet for connection to different modems.
4. Connect to the RealPresence Collaboration Server with the RMX Manager.

Call Detail Records

Topics:

RealPresence Collaboration Server (RMX) creates call detail records (CDRs) for every conference started on it.

This section discusses the CDR options that you can configure and the CDR tasks you may want to perform.

CDR Options:

- Enabling a CDR backup alarm
- Enabling multipart CDRs

CDR Tasks:

- View the MCU CDR list
- Retrieve and save a CDR for viewing
- Retrieve and save CDRs for billing and reporting

You can delete the CDRs by performing a Comprehensive Restore.

Enable a CDR Backup Alarm

You can enable an alarm to warn you before the MCU overwrites older CDRs so you can back up the CDR information before it's deleted.

Businesses can use CDRs to generate billing information and resource usage reports. MCU system backups don't include CDRs, so if you require CDRs for reporting and billing purposes, you must back them up manually.

RealPresence Collaboration Server 1800/2000 stores the CDRs of up to 2000 conferences.
RealPresence Collaboration Server 4000 stores the CDRs of up to 4000 conferences.

Procedure

» Set the system flag `ENABLE_CYCLIC_FILE_SYSTEM_ALARMS` to `YES`.

If you set the `ULTRA_SECURE_MODE` system flag to `YES`, your MCU automatically enables the `ENABLE_CYCLIC_FILE_SYSTEM_ALARMS` system flag.

When your MCU reaches the file storage threshold limit, the system triggers an active alarm with the following message: `Backup of CDR files is required.`

Enable Multi-Part CDRs

By default, the RealPresence Collaboration Server (also called MCU) limits the CDR file size to 1MB.

When a CDR file reaches that size, the MCU saves the CDR and further call data recording is stopped. In that case, the additional data is lost.

The MCU can be configured to keep recording the data in multiple CDR file sets of 1MB each. Multi-Part CDR ensures that all conference call data from long duration or permanent conferences is recorded.

Procedure

1. Set the value of `ENABLE_MULTI_PART_CDR` system flag to `YES`.
2. To modify the default setting, the flag must be manually added to the **System Configuration**.

   When the Multi-Part CDR option is enabled, a Part Index is added to the CDR List. It displays the CDR file sequence in the CDR file set. The files included in a set have the same unique Display Name.

Related Links

System Flags on page 264

View the MCU CDR List

Each conference is a separate record in the MCU memory and is archived as a separate CDR file.

Procedure

» In RMX Manager, go to **Administration** > **CDR**.

The **CDR List** identifies conference by their display name and includes information such as start times, duration, status, and whether or not the CDR was saved and retrieved.

Retrieve and Save a CDR for Viewing

Your MCU keeps each conference as a separate record in the MCU memory and archives each conference as a separate CDR file.

To view the content of a single CDR, you must retrieve and save it in a viewable format.

Procedure

1. In RMX Manager, go to **Administration** > **CDR**.
2. Select the CDR for the conference and do one of the following (depending on the format you prefer):
   - Select **Retrieve Formatted**  .
   - Select **Retrieve Formatted XML**  .
3. Browse to a location to save the file and select **OK**.
4. Open the saved file.

   The file contains the following information:
   - General information about the conference

    - Conference name
    - Conference ID
    - Start time
    - Duration
- Participant information
    - Display name
    - IP address
    - SIP URI/Tel-URI
    - Calling number
    - H.323 alias name
- Events occurring during the conference
    - Adding a new participant
    - Disconnecting a participant
    - Extending the length of the conference

  The event sections or records include an event type heading or event type code, followed by the event data.

Retrieve and Save CDRs for Billing and Reporting

Businesses that must generate video conferencing billing information or resource usage reports should retrieve and archive MCU CDRs on a periodic basis.

You can retrieve and archive all available CDRs, which can then be used to generate billing information, resource usage reports and more by any third-party applications.

Procedure

1. On your system, create an archive folder for the CDRs.
2. In RMX Manager, go to **Administration** > **CDR** and multi-select all of the CDRs of interest.
3. To retrieve and save the CDRs in .cdr format, click **Retrieve**  .
4. To retrieve and save the CDRs in .xml format, click **Retrieve Formatted XML**  .
5. To retrieve and save the CDRs in .txt format, click **Retrieve Formatted**  .
6. Browse to the archive folder location and click **OK**.

   The MCU saves the selected CDRs to the selected location.

CDR Fields in Unformatted Files

This section describes the fields and values in the unformatted CDR records.

Although the formatted files contain basically the same information, in a few instances a single field in the unformatted file is converted to multiple lines in the formatted file, and in other cases, multiple fields in the unformatted file are combined into one line in the formatted file.

The CDR (Call Detail Records) utility is used to retrieve conference information to a file. The CDR utility can retrieve conference information to a file in both formatted and unformatted formats.

Unformatted CDR files contain multiple records. The first record in each file contains information about the conference in general, such as the conference name and start time. The remaining records each contain information about one event that occurred during the conference, such as a participant connecting to the conference, or a user extending the length of the conference. The first field in each record identifies the event type, and this is followed by values containing information about the event. The fields are separated by commas.

Formatted files contain basically the same information as unformatted files, but with the field values replaced by descriptions. Formatted files are divided into sections, each containing information about one conference event. The first line in each section is a title describing the type of event, and this is followed by multiple lines, each containing information about the event in the form of a descriptive field name and value.

Note: Field names and values in the formatted file appear in the language used for the RMX Web Client user interface at the time of CDR information retrieval.

The value of fields supporting Unicode values, such as the info fields, are stored in the CDR file in UTF8. The application that reads the CDR file must support Unicode.

The MCU sends the entire CDR file via API or HTTP, and the RealPresence Collaboration Server or external application does the processing and sorting. The RealPresence Collaboration Server ignores events that it doesn't recognize, that is, events written in a higher version that don't exist in the current version. Therefore, to enable compatibility between versions, instead of adding new fields to existing events, new fields are added as separate events, so as not to affect the events from older versions. This allows users with lower versions to retrieve CDR files that were created in higher versions.

Conference Summary Record

The conference summary record (the first record in the unformatted CDR file) contains the following fields.

Conference Summary Record Fields

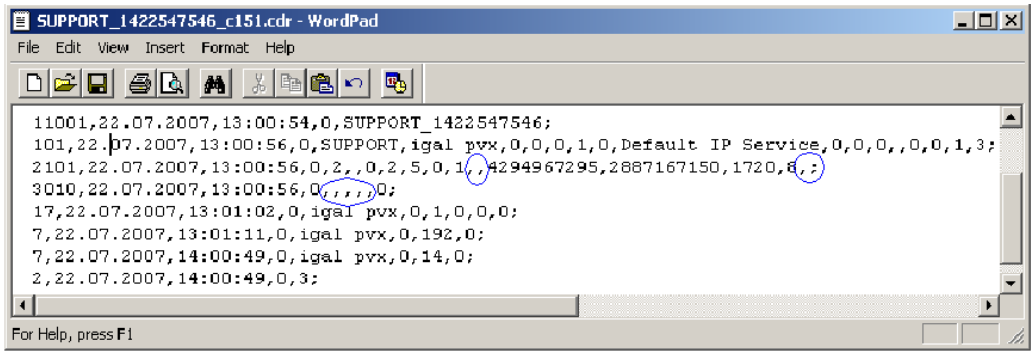
Field	Description
File Version	The version of the CDR utility that created the file.
Conference Routing Name	The Routing Name of the conference.
Internal Conference ID	The conference identification number as assigned by the system.
Reserved Start Time	The time the conference was scheduled to start in Greenwich Mean Time (GMT). The reservation time of a reservation that was started immediately or of an ongoing conference is the same as the Actual Start Time.
Reserved Duration	The amount of time the conference was scheduled to last.
Actual Start Time	The actual time the conference started in GMT.
Actual Duration	The actual conference duration.

Field	Description
Status	The conference status code as follows: 1 - The conference is an ongoing conference. 2 - The conference was terminated by a user. 3 - The conference ended at the scheduled end time. 4 - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. 5 - The conference never started. 6 - The conference could not start due to a problem. 8 - An unknown error occurred. 9 - The conference was terminated by a participant using DTMF codes. **Note:** If the conference was terminated by an MCU reset, this field contains the value **1** (ongoing conference).
File Name	The name of the conference log file.
GMT Offset Sign	Indicates whether the GMT Offset is positive or negative. The possible values are: 0 - Offset is negative. GMT Offset to be subtracted from the GMT Time. 1 - Offset is positive. GMT Offset to be added to the GMT Time.
GMT Offset	The time zone difference between Greenwich and the RealPresence Collaboration Server's physical location in hours and minutes. Together with the GMT Offset Sign field the GMT Offset field is used to define the RealPresence Collaboration Server local time. For example, if the GMT Offset Sign is 0 and GMT Offset is 3 hours then the time zone of the RealPresence Collaboration Server's physical location is -3, which will be subtracted from the GMT time to determine the local time. However, if the GMT Offset Sign is 1 and GMT Offset is 4 hours then the time zone of the RealPresence Collaboration Server's physical location is +4, which is added to the GMT time to determine the local time.
File Retrieved	Indicates if the file has been retrieved and saved to a formatted file, as follows: 0 - No 1 - Yes

Event Records

The event records, that is, all records in the unformatted file except the first record, contain standard fields, such as the event type code and the time stamp, followed by fields that are event-specific.

The event fields are separated by commas. Two consecutive commas with nothing between them (,,), or a comma followed immediately by a semi-colon (;,), indicates an empty field, as in the following example:



Standard Event Record Fields

This section describes the Standard Event Record fields.

All event records start with the following fields:

- The CDR event type code.
- The event date.
- The event time.
- The structure length. This field is required for compatibility purposes, and always contains the value **0**.

Event Types

The table below contains the list of events logged in the CDR file and indicates where to find details on fields specific to that type of event.

Note: The event code identifies the event in the unformatted CDR file, and the event name identifies the event in the formatted CDR file.

CDR Event Types

Event Code	Event Name	Description
1	CONFERENCE START	The conference started. **Note:** There's one CONFERENCE START event per conference. It's always the first event in the file, after the conference summary record. It contains conference details, but not participant details.
2	CONFERENCE END	The conference ended. **Note:** There's one CONFERENCE END event per conference, and it's always the last event in the file.
3	ISDN/PSTN CHANNEL CONNECTED	This field isn't applicable for RealPresence Collaboration Server, Virtual Edition.

Event Code	Event Name	Description
4	ISDN/PSTN CHANNEL DISCONNECTED	This field isn't applicable for RealPresence Collaboration Server, Virtual Edition.
5	ISDN/PSTN PARTICIPANT CONNECTED	This field isn't applicable for RealPresence Collaboration Server, Virtual Edition.
7	PARTICIPANT DISCONNECTED	A participant disconnected from the conference.
10	DEFINED PARTICIPANT	Information about a defined participant, that is, a participant who was added to the conference before the conference started. **Note:** There's one event for each participant defined before the conference started.
15	H323 CALL SETUP	Information about the IP address of the participant.
17	H323 PARTICIPANT CONNECTED	An H.323 participant connected to the conference.
18	NEW UNDEFINED PARTICIPANT	A new undefined participant joined the conference.
20	BILLING CODE	A billing code was entered by a participant using DTMF codes.
21	SET PARTICIPANT DISPLAY NAME	A user assigned a new name to a participant, or an end point sent its name.

Event Code	Event Name	Description
22	DTMF CODE FAILURE	An error occurred when a participant entered a DTMF code.
23	SIP PARTICIPANT CONNECTED	A SIP participant connected to the conference.
26	RECORDING LINK	A recording event, such as recording started or recording resumed, occurred.
28	SIP PRIVATE EXTENSIONS	Contains SIP Private Extensions information.
30	GATEKEEPER INFORMATION	Contains the gatekeeper caller ID, which makes it possible to match the CDR in the gatekeeper and in the MCU.
31	PARTICIPANT CONNECTION RATE	Information about the line rate of the participant connection. This event is added to the CDR file each time the endpoint changes its connection bit rate.
32	EVENT NEW UNDEFINED PARTY CONTINUE IPV6 ADDRESS	Information about the IPv6 address of the participant's endpoint.
33	PARTY CHAIR UPDATE	Participants connect to the conferences as standard participants and they're designated as chairperson's either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code.
34	PARTICIPANT MAXIMUM USAGE INFORMATION	This event includes information of the maximum line rate, maximum resolution, and maximum frame rate used by H.323 or SIP participant during the conference.

Event Code	Event Name	Description
35	SVC SIP PARTICIPANT CONNECTED	An SVC user connected over SIP.
100	USER TERMINATE CONFERENCE	A user terminated the conference.
101	USER ADD PARTICIPANT	A user added a participant to the conference during the conference.
102	USER DELETE PARTICIPANT	A user deleted a participant from the conference.
103	USER DISCONNECT PARTICIPANT	A user disconnected a participant.
104	USER RECONNECT PARTICIPANT	A user reconnected a participant who was disconnected from the conference.
105	USER UPDATE PARTICIPANT	A user updated the properties of a participant during the conference.
106	USER SET END TIME	A user modified the conference end time.
107	OPERATOR MOVE PARTY FROM CONFERENCE	The participant moved from an Entry Queue to the destination conference or between conferences.

Event Code	Event Name	Description
108	OPERATOR MOVE PARTY TO CONFERENCE	The RealPresence Collaboration Server User moved the participant from an ongoing conference to another conference.
109	OPERATOR ATTEND PARTY	The RealPresence Collaboration Server User moved the participant to the Operator conference.
111	OPERATOR BACK TO CONFERENCE PARTY	The RealPresence Collaboration Server User moved the participant back to their Home (source) conference.
112	OPERATOR ATTEND PARTY TO CONFERENCE	The RealPresence Collaboration Server User moved the participant from the Operator conference to another conference.
1001	NEW UNDEFINED PARTICIPANT CONTINUE 1	Additional information about a `NEW UNDEFINED PARTICIPANT` event.
2001	CONFERENCE START CONTINUE 1	Additional information about a `CONFERENCE START` event.
2007	PARTICIPANT DISCONNECTED CONTINUE 1	Additional information about a `PARTICIPANT DISCONNECTED` event.
2010	DEFINED PARTICIPANT CONTINUE 1	Additional information about a `DEFINED PARTICIPANT` event.

Event Code	Event Name	Description
2011	RESERVED PARTICIPANT CONTINUE PV6 ADDRESS	Additional information about a DEFINED PARTICIPANT event that includes the IPv6 addressing of the defined participant.
2012	RESERVED PARTICIPANT CONTINUE 2	Additional information about a DEFINED PARTICIPANT event.
2015	USER UPDATE PARTICIPANT CONTINUE 1	Additional information about a USER UPDATE PARTICIPANT event.
2016	USER UPDATE PARTICIPANT CONTINUE 2	Additional information about a USER UPDATE PARTICIPANT event.
2101	USER ADD PARTICIPANT CONTINUE 1	Additional information about a USER ADD PARTICIPANTevent.
2102	USER ADD PARTICIPANT CONTINUE 2	Additional information about a USER ADD PARTICIPANT event.
2105	USER UPDATE PARTICIPANT CONTINUE 1	Additional information about a USER UPDATE PARTICIPANT event.
2106	USER UPDATE PARTICIPANT CONTINUE 2	Additional information about a USER UPDATE PARTICIPANT event.

Event Code	Event Name	Description
3010	PARTICIPANT INFORMATION	The contents of the participant information fields.
5001	CONFERENCE START CONTINUE 4	Additional information about a CONFERENCE START event. **Note:** An additional CONFERENCE START CONTINUE 4event is written to the CDR each time the value of one of the following conference fields is modified: • **Conference Password** • **Chairperson Password** • **Info1**, **Info2**, or **Info3** • **Billing Info** These additional events only contain the value of the modified field.
6001	CONFERENCE START CONTINUE 5	Additional information about a CONFERENCE START event.
11001	CONFERENCE START CONTINUE 10	Additional information about a CONFERENCE START event. This event contains the Display Name.

Event-Specific Fields

These tables describe the Event Fields for all the different events.

Event Fields for Event 1 - CONFERENCE START

Field	Description
Dial-Out Manually	Indicates whether the conference was a dial-out manually conference or not. Currently the only value is: 0 - The conference wasn't a dial-out manually conference, that is, the MCU initiates the communication with dial-out participants, and the user doesn't need to connect them manually.

Field	Description
Auto Terminate	Indicates whether the conference was set to end automatically if no participant joins the conference for a predefined time period after the conference starts, or if all participants disconnect from the conference and the conference is empty for a predefined time period. Possible values are: 0 - The conference wasn't set to end automatically. 1 - The conference was set to end automatically.
Line Rate	The conference line rate, as follows: 0 - 64 kbps 6 - 384 kbps 12 - 1920 kbps 13 - 128 kbps 15 - 256 kbps 23 - 512 kbps 24 - 768 kbps 26 - 1152 kbps 29 - 1472 kbps 32 - 96 kbps
Line Rate (cont.)	33 - 1024 kbps 34 - 4096 kbps
Restrict Mode	Not supported. Always contains the value **0**.
Audio Algorithm	The audio algorithm. Currently the only value is: 255 - Auto
Video Session	The video session type. Currently the only value is: 3 - Continuous Presence
Video Format	The video format. Currently the only value is: 255 - Auto
CIF Frame Rate	The CIF frame rate. Currently the only value is: 255 - Auto

Field	Description
QCIF Frame Rate	The QCIF frame rate: Currently the only value is: 255 - Auto
LSD Rate	Not supported. Always contains the value **0**.
HSD Rate	Not supported. Always contains the value **0**.
T120 Rate	Not supported. Always contains the value **0**.

Event Fields for Event 2 - CONFERENCE END

Field	Description
Conference End Cause	Indicates the reason for the termination of the conference, as follows: 1 - The conference is an ongoing conference or the conference was terminated by an MCU reset. 2 - The conference was terminated by a user. 3 - The conference ended at the scheduled end time. 4 - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. 5 - The conference never started. 6 - The conference couldn't start due to a problem. 8 - An unknown error occurred. 9 - The conference was terminated by a participant using DTMF codes.

Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Number of Channels	The number of channels being connected for this participant.

Field	Description
Connect Initiator	Indicates who initiated the connection, as follows: 0 - RealPresence Collaboration Server 1 - Participant Any other number - Unknown
Call Type	The call type, as follows: 68 - 56 KBS data call 72 - 1536kbs data call (PRI only) 75 - 56 KBS data call 77 - Modem data service 79 - 384kbs data call (PRI only) 86 - Normal voice call
Network Service Program	The Network Service program, as follows: 0 - None 1 - ATT_SDN or NTI_PRIVATE 3 - ATT_MEGACOM or NTI_OUTWATS 4 - NTI FX 5 - NTI TIE TRUNK 6 - ATT ACCUNET 8 - ATT 1800 16 - NTI_TRO
Preferred Mode	The value of the preferred/exclusive field for B channel selection (the PRF mode), as follows: 0 - None 1 - Preferred 2 - Exclusive For more details, refer to the Q.931 standard.
Calling Participant Number Type	The type of calling number, as follows: 0 - Unknown, default 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated

Field	Description
Calling Participant Number Plan	The calling participant number plan. 0 - Unknown 1 - ISDN (audio/video) 9 - Private
Calling Participant Presentation Indicator	The calling participant presentation indicator, as follows: 0 - Presentation allowed, default 1 - Presentation restricted 2 - Number not available 255 - Unknown
Calling Participant Screening Indicator	The calling participant screening indicator, as follows: 0 - Participant not screened, default 1 - Participant verification succeeded 2 - Participant verification failed 3 - Network provided 255 - Unknown
Calling Participant Phone Number	The telephone number used for dial-in.
Called Participant Number Type	The type of number called, as follows: 0 - Unknown, default 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated
Called Participant Number Plan	The called participant number plan, as follows: 0 - Unknown 1 - ISDN (audio/video) 9 - Private
Called Participant Phone Number	The telephone number used for dial-out.

Event Fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED

Field	Description
Participant Name	The participant name.

Field	Description
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Disconnect Initiator	Indicates who initiated the disconnection, as follows: 0 - RealPresence Collaboration Server 1 - Participant Any other number - Unknown
Disconnect Coding Standard	The disconnection cause code standard. For values and explanations, see the Q.931 Standard.
Disconnect Location	The disconnection cause location. For values and explanations, see the Q.931 Standard.
Q931 Disconnection Cause	The disconnection cause value. For values and explanations, see the Q.931 Standard.

Event Fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange 7 - Deleted by a user 8 - Secondary. The participant couldn't connect the video channels and is connected via audio only 10 - Connected with problem 11 - Redialing
Remote Capabilities	**Note:** This field is only relevant to ISDN-video participants. The remote capabilities in H.221 format.

Field	Description
Remote Communication Mode	**Note:** This field is only relevant to ISDN-video participants. The remote communication mode in H.221 format.
Secondary Cause	**Note:** This field is only relevant to ISDN-video participants and only if the Participant Status is Secondary. The cause for the secondary connection (not being able to connect the video channels), as follows: 0 - Default 11 - The incoming video parameters aren't compatible with the conference video parameters. 12 - H.323 card failure. 13 - The conference video settings aren't compatible with the endpoint capabilities. 14 - The new conference settings aren't compatible with the endpoint capabilities.
Secondary Cause (cont.)	15 - Video stream violation due to incompatible annexes or other discrepancy. 16 - Inadequate video resources. 17 - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards. 18 - Video connection couldn't be established. 24 - The endpoint closed its video channels. 25 - The participant video settings aren't compatible with the conference protocol. 26 - The endpoint couldn't reopen the video channel after the conference video mode was changed. 27 - The gatekeeper approved a lower bandwidth than requested. 28 - Video connection for the SIP participant is temporarily unavailable. 29 - AVF problem. Insufficient bandwidth. 30 - H2.39 bandwidth mismatch 255 - Other

Event Fields for Event 7 - PARTICIPANT DISCONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Call Disconnection Cause	The cause of disconnection.

Field	Description
Q931 Disconnect Cause	If the disconnection cause is "No Network Connection" or "Participant Hang Up", then this field indicates the Q931 disconnect cause.

Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT

Field	Description
User Name	The login name of the user who added the participant to the conference, or updated the participant properties.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows: 0 - Dial-out 5 - Dial-in
Bonding Mode	Not supported. Always contains the value 0.
Number Of Channels	The number of channels being connected for this participant. **Note:** This field is only relevant to ISDN (audio/video) participants.
Net Channel Width	Not supported. Always contains the value 0.
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value 0.
Audio Only	Indicates the participant's Audio Only setting, as follows: 0 - The participant isn't an Audio Only participant. 1 - The participant is an Audio Only participant. 255 - Unknown

Field	Description
Default Number Type	The type of telephone number, as follows: 0 - Unknown 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated 255 - Taken from Network Service, default. **Note:** • For dial-in participants, the only possible value is 255 - Taken from Network Service. • This field is only relevant to ISDN (audio/video) participants.
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel. **Note:** This field is only relevant to ISDN (audio/video) participants.
Number of MCU Phone Numbers	The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant. **Note:** This field is only relevant to ISDN (audio/video) participants.
Party and MCU Phone Numbers	One or more fields, each per a participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers. **Note:** This field is only relevant to ISDN (audio/video) participants.

Field	Description
Identification Method	The method by which the destination conference is identified, as follows: 1 - Called phone number, IP address, or alias. 2 - Calling phone number, IP address, or alias. **Note:** This field is only relevant to dial in participants.
Meet Me Method	The meet-me per method. Currently the only value is: 3 - Meet-me per participant. **Note:** This field is only relevant to dial in participants.

Event Fields for Event 15 - H323 CALL SETUP

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Connect Initiator	Indicates who initiated the connection, as follows: 0 - MCU 1 - Remote participant. Any other number - Unknown.
Min Rate	The minimum line rate used by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Max Rate	The maximum line rate achieved by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Source Party Address	The IP address of the calling participant. A string of up to 255 characters.
Destination Party Address	The IP address of the called participant. A string of up to 255 characters.
Endpoint Type	The endpoint type, as follows: 0 - Terminal 1 - Gateway 2 - MCU 3 - Gatekeeper 4 - Undefined

Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in. 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange. 7 - Deleted by a user. 8 - Secondary. The participant couldn't connect the video channels and is connected via audio only. 10 - Connected with problem. 11 - Redialing
Capabilities	Not supported. Always contains the value 0.
Remote Communication Mode	Not supported. Always contains the value 0.

Field	Description
Secondary Cause	**Note:** This field is only relevant if the Participant Status is Secondary. The cause for the secondary connection (not being able to connect the video channels), as follows: 0 - Default 11 - The incoming video parameters aren't compatible with the conference video parameters. 13 - The conference video settings aren't compatible with the endpoint capabilities. 14 - The new conference settings aren't compatible with the endpoint capabilities. 15 - Video stream violation due to incompatible annexes or other discrepancy 16 - Inadequate video resources. 17 - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards. 18 - Video connection couldn't be established. 24 - The endpoint closed its video channels. 25 - The participant video settings aren't compatible with the conference protocol. 26 - The endpoint couldn't reopen the video channel after the conference video mode was changed. 27 - The gatekeeper approved a lower bandwidth than requested. 28 - Video connection for the SIP participant is temporarily unavailable. 255 - Other

Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows: 0 - Dial-out 5 - Dial-in
Bonding Mode	Not supported. Always contains the value 0.
Number of Channels	The number of channels being connected for this participant. **Note:** This field is only relevant to ISDN (audio/video) participants.

Field	Description
Net Channel Width	Not supported. Always contains the value 0.
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value 0.
Audio Only	Indicates the participant's Audio Only setting, as follows: 0 - The participant isn't an Audio Only participant. 1 - The participant is an Audio Only participant. 255 - Unknown
Default Number Type	The type of telephone number. Note: Since undefined participants are always dial-in participants, the only possible value is: 255 - Taken from Network Service. **Note:** This field is only relevant to ISDN (audio/video) participants.
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	The number of participant phone numbers. The participant phone number is the CLI (Calling Line Identification) as identified by the MCU. **Note:** This field is only relevant to ISDN (audio/video) participants.
Number of MCU Phone Numbers	The number of MCU phone numbers. The MCU phone number is the number dialed by the participant to connect to the MCU. **Note:** This field is only relevant to ISDN (audio/video) participants.
Party and MCU Phone Numbers	No, one or more fields, one field for each participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers. **Note:** This field is only relevant to ISDN (audio/video) participants.

Field	Description
Identification Method	The method by which the destination conference is identified, as follows: 1 - Called phone number, IP address, or alias. 2 - Calling phone number, IP address, or alias. **Note:** This field is only relevant to dial-in participants.
Meet Me Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method, as follows: 3 - Meet-me per participant.
Network Type	The type of network between the participant and the MCU, as follows: 0 - ISDN (audio/video) 2 - H.323 5 - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value 0.
Video Protocol	The video protocol, as follows: 1 - H.261 2 - H.263 4 - H.264 255 - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest). Each unit movement increases or decreases the volume by 3 dB.
Undefined Participant	Indicates whether aren't the participant is an undefined participant, as follows: 0 - The participant isn't an undefined participant. 2 - The participant is an undefined participant.
Node Type	The node type, as follows: 0 - MCU 1 - Terminal

Field	Description
Bonding Phone Number	**Note:** This field is only relevant to ISDN (audio/video) participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases, the address overrides the gatekeeper.
Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of 65535 is ignored by MCU.
H.323 Participant Alias Type/SIP Participant Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Participant Alias Name/SIP Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants - the participant alias. May contain up to 512 characters. For SIP participants - the participant address. May contain up to 80 characters.

Event Fields for Event 20 - BILLING CODE

Field	Description
Participant Name	The name of the participant who added the billing code.
Participant ID	The identification number, as assigned by the MCU, of the participant who added the billing code.
Billing Info	The numeric billing code that was added (32 characters).

Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME

Field	Description
Participant Name	The original name of the participant, for example, the name automatically assigned to an undefined participant, such as, "<conference name>_(000)."
Participant ID	The identification number assigned to the participant by the MCU.
Display Name	The new name assigned to the participant by the user, or the name sent by the end point.

Event Fields for Event 22 - DTMF CODE FAILURE

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Incorrect Data	The incorrect DTMF code entered by the participant, or an empty field "" if the participant didn't press any key.
Correct Data	The correct DTMF code, if known.
Failure Type	The type of DTMF failure, as follows: 2 - The participant didn't enter the correct conference password. 6 - The participant didn't enter the correct chairperson password. 12 - The participant didn't enter the correct Conference ID.

Event Fields for Event 26 - RECORDING LINK

Field	Description
Participant Name	The name of the Recording Link participant.
Participant ID	The identification number assigned to the Recording Link participant by the MCU.

Field	Description
Recording Operation	The type of recording operation, as follows: 0 - Start recording 1 - Stop recording 2 - Pause recording 3 - Resume recording 4 - Recording ended 5 - Recording failed
Initiator	Not supported.
Recording Link Name	The name of the Recording Link.
Recording Link ID	The Recording Link ID.
Start Recording Policy	The start recording policy, as follows: 1 - Start recording automatically as soon as the first participant connects to the conference. 2 - Start recording when requested by the conference chairperson via DTMF codes or from the RMX Web Client, or when the operator starts recording from the RMX Web Client.

Event Fields for Event 28 - SIP PRIVATE EXTENSIONS

Field	Description
Participant Name	The name of the participant.
Participant ID	The participant's identification number as assigned by the system.
Called Participant ID	The called participant ID.
Asserted Identity	The identity of the user sending a SIP message as it was verified by authentication.
Charging Vector	A collection of charging information.
Preferred Identity	The identity the user sending the SIP message wishes to be used for the P-Asserted-Header field that inserts the trusted element.

Event Fields for Event 30 - GATEKEEPER INFORMATION

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Gatekeeper Caller ID	The caller ID in the gatekeeper records. This value makes it possible to match the CDR in the gatekeeper and in the MCU.

Event Fields for Event 31 - PARTICIPANT CONNECTION RATE

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Current Rate	The participant line rate in Kbps.

Event Fields for Event 32

Field	Description
IP V6	IPv6 address of the participant's endpoint.

Event Fields for Event 33 - PARTY CHAIR UPDATE

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Chairperson	Possible values: • True - participant is a chairperson. • False - Participant isn't a chairperson participant (is a standard participant).

Event Fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Maximum Bit Rate	The maximum bit rate used by the participant during the call.
Maximum Resolution	The maximum resolution used by the participant during the call. **Note:** The reported resolutions are: CIF, SD, HD720, and HD1080. Other resolutions are rounded up to the nearest resolution. For example, 2SIF is reported as SD resolution.
Maximum Frame Rate	The maximum frame rate used by the participant during the call.

Field	Description
Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange. 7 - Deleted by a user 8 - Secondary. The participant couldn't connect the video channels and is connected via audio only. 10 - Connected with problem. 11 - Redialing.
Receive line rate	Negotiated reception line rate
Transmit line rate	Negotiated transmission line rate
Uplink Video Capabilities	• Number of uplink streams • Video stream (multiple streams): ◦ Resolution width ◦ Resolution height ◦ Max frame rate ◦ Max line rate
Audio Codec	SAC, Other

Field	Description
Secondary Cause	

Event Fields for Event 100 - USER TERMINATE CONFERENCE

Field	Description
Terminated By	The login name of the user who terminated the conference.

Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT

Field	Description
User Name	The login name of the user who reconnected the participant to the conference, or disconnected or deleted the participant from the conference.
Participant Name	The name of the participant reconnected to the conference, or disconnected or deleted from the conference.
Participant ID	The identification number assigned to the participant by the MCU.

Event Fields for Event 106 - USER SET END TIME

Field	Description
New End Time	The new conference end time set by the user, in GMT.
User Name	The login name of the user who changed the conference end time.

Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY

Field	Description
Operator Name	The login name of the user who moved the participant.
Party Name	The name of the participant who was moved.
Party ID	The identification number of the participant who was moved, as assigned by the MCU.
Destination Conf Name	The name of the conference to which the participant was moved.
Destination Conf ID	The identification number of the conference to which the participant was moved.

Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE

Field	Description
Operator Name	The login name of the operator who moved the participant to the conference.
Source Conf Name	The name of the source conference.
Source Conf ID	The identification number of the source conference, as assigned by the MCU.
Party Name	The name of the participant who was moved.
Party ID	The identification number assigned to the participant by the MCU.
Connection Type	The connection type, as follows: 0 - Dial-out 5 - Dial-in
Bonding Mode	Possible values are: 0 - Bonding is disabled 1 - Bonding is enabled 255 - Auto **Note:** This field is only relevant to ISDN (audio/video) participants.
Number Of Channels	The number of channels, as follows: 255 - Auto Otherwise, in range of 1 - 30. **Note:** This field is only relevant to ISDN (audio/video) participants.
Net Channel Width	The bandwidth of each channel. This value is always 0, which represents a bandwidth of 1B, which is the only bandwidth that is currently supported.
Net Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Indicates whether or not the line is restricted, as follows: 27 - Restricted line. 28 - Non-Restricted line. 255 - Unknown or not relevant.

Field	Description
Voice Mode	Indicates whether or not the participant is an Audio Only participant, as follows: 0 - The participant isn't an Audio Only participant. 1 - The participant is an Audio Only participant. 255 - Unknown
Number Type	The type of telephone number, as follows: 0 - Unknown 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated 255 - Taken from Network Service, default. **Note:** This field is only relevant to dial-out, ISDN (audio/video) participants.
Net Sub Service Name	The network sub-service name. An empty field "" means that MCU selects the default sub-service. **Note:** This field is only relevant to dial-out ISDN (audio/video) participants.
Number of Party Phone Numbers	The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel. **Note:** This field is only relevant to ISDN (audio/video) participants.
Number of MCU Phone Numbers	The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant. **Note:** This field is only relevant to ISDN (audio/video) participants.
Party and MCU Phone Numbers	The participant phone numbers are listed first, followed by the MCU phone numbers. **Note:** This field is only relevant to ISDN (audio/video) participants.

Field	Description
Ident. Method	The method by which the destination conference is identified, as follows: 0 - Password 1 - Called phone number, or IP address, or alias. 2 - Calling phone number, or IP address, or alias. **Note:** This field is only relevant to dial-in participants.
Meet Method	The meet-me per method, as follows: 1 - Meet-me per MCU-Conference. 3 - Meet-me per participant. 4 - Meet-me per channel. **Note:** This field is only relevant to dial-in participants.
Net Interface Type	The type of network interface between the participant and the MCU, as follows: 0 - ISDN 2 - H.323 5 - SIP
H243 Password	The H.243 password, or an empty field "" if there's no password.
Chair	Not supported. Always contains the value 0.
Video Protocol	The video protocol, as follows: 1 - H.261 2 - H.263 3 - H.264* 4 - H.264 255 - Auto
Audio Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest).
Undefined Type	The participant type, as follows: 0 - Defined participant. (The value in the formatted text file is "default"). 2 - Undefined participant. (The value in the formatted text file is "Unreserved participant").
Node Type	The node type, as follows: 0 - MCU 1 - Terminal

Field	Description
Bonding Phone Number	**Note:** This field is only relevant to ISDN (audio/video) participants. The phone number for Bonding dial-out calls.
Video Rate	**Note:** This field is only relevant to IP participants. The video rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Call Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of 65535 is ignored by MCU.
H.323 Party Alias Type/SIP Party Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 11 - URL ID alias type 12 - Transport ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Party Alias/SIP Party Address	**Note:** This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY

Field	Description
Operator Name	The login name of the operator moving the participant back to the conference.
Party Name	The name of the participant being moved.
Party ID	The identification number, as assigned by the MCU, of the participant being moved.

Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1

Field	Description
Encryption	Indicates the participant's encryption setting as follows: 0 - The participant isn't encrypted. 1 - The participant is encrypted. 2 - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Event Fields for Event 2001 - CONFERENCE START CONTINUE 1

Field	Description
Audio Tones	Not supported. Always contains the value **0**.
Alert Tone	Not supported. Always contains the value **0**.
Talk Hold Time	The minimum time that a speaker has to speak to become the video source. The value is in units of 0.01 seconds. Currently the only value is **150**, which indicates a talk hold time of 1.5 seconds.
Audio Mix Depth	The maximum number of participants whose audio can be mixed. RealPresence Collaboration Servers 2000/4000: 5. RealPresence Collaboration Server 1800/VE: AVC - 4; SVC - 5.
Operator Conference	Not supported. Always contains the value **0**.
Video Protocol	The video protocol. Currently the only value is: 255 - Auto

Field	Description
Meet Me Per Conference	Indicates the Meet Me Per Conference setting. Currently the only value is: 1 - The Meet Me Per Conference option is enabled, and dial-in participants can join the conference by dialing the dial-in number.
Number of Network Services	Not supported. Always contains the value **0**.
Chairperson Password	The chairperson password for the conference. An empty field "" means that no chairperson password was assigned to the conference.
Chair Mode	Not supported. Always contains the value **0**.
Cascade Mode	The cascading mode. Currently the only value is: 0 - None
Master Name	Not supported. This field remains empty.
Minimum Number of Participants	The number of participants for which the system reserved resources. Additional participants may join the conference without prior reservation until all the resources are utilized. Currently the only value is **0**.
Allow Undefined Participants	Indicates whether or not undefined dial-in participants can connect to the conference. Currently the only value is: 1 - Undefined participants can connect to the conference.
Time Before First Participant Joins	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse from the time the conference starts, without any participant connecting to the conference, before the conference is automatically terminated by the MCU.
Time After Last Participant Quits	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse after the last participant has disconnected from the conference, before the conference is automatically terminated by the MCU.
Conference Lock Flag	Not supported. Always contains the value **0**.

Field	Description
Maximum Number of Participants	The maximum number of participants that can connect to the conference at one time. The value 65535 (auto) indicates that as many participants as the MCU's resources allow can connect to the conference, up to the maximum possible for the type of conference.
Audio Board ID	Not supported. Always contains the value 65535.
Audio Unit ID	Not supported. Always contains the value 65535.
Video Board ID	Not supported. Always contains the value 65535.
Video Unit ID	Not supported. Always contains the value 65535.
Data Board ID	Not supported. Always contains the value 65535.
Data Unit ID	Not supported. Always contains the value 65535.
Message Service Type	The Message Service type. Currently the only value is: 3 - IVR
Conference IVR Service	The name of the IVR Service assigned to the conference. Note: If the name of the IVR Service contains more than 20 characters, it will be truncated to 20 characters.
Lecture Mode Type	Indicates the type of Lecture Mode, as follows: 0 - None 1 - Lecture Mode 3 - Presentation Mode
Lecturer	**Note:** This field is only relevant if the Lecture Mode Type is Lecture Mode. The name of the participant selected as the conference lecturer.
Time Interval	**Note:** This field is only relevant if Lecturer View Switching is enabled. The number of seconds a participant is to be displayed in the lecturer window before switching to the next participant. Currently the only value is 15.

Field	Description
Lecturer View Switching	**Note:** This field is only relevant when Lecture Mode is enabled. Indicates the lecturer view switching setting, as follows: 0 - Automatic switching between participants is disabled. 1 - Automatic switching between participants is enabled.
Audio Activated	Not supported. Always contains the value 0.
Lecturer ID	Not supported. Always contains the value 4294967295.

Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1

Field	Description
Rx Synchronization Loss	The number of times that the general synchronization of the MCU was lost.
Tx Synchronization Loss	The number of times that the general synchronization of the participant was lost.
Rx Video Synchronization Loss	The number of times that the synchronization of the MCU video unit was lost.
Tx Video Synchronization Loss	The number of times that the synchronization of the participant video was lost.
Mux Board ID	Not supported. Always contains the value 0.
Mux Unit ID	Not supported. Always contains the value 0.
Audio Codec Board ID	Not supported. Always contains the value 0.
Audio Codec Unit ID	Not supported. Always contains the value 0.
Audio Bridge Board ID	Not supported. Always contains the value 0.

Field	Description
Audio Bridge Unit ID	Not supported. Always contains the value 0.
Video Board ID	Not supported. Always contains the value 0.
Video Unit ID	Not supported. Always contains the value 0.
T.120 Board ID	Not supported. Always contains the value 0.
T.120 Unit ID	Not supported. Always contains the value 0.
T.120 MCS Board ID	Not supported. Always contains the value 0.
T.120 MCS Unit ID	Not supported. Always contains the value 0.
H.323 Board ID	Not supported. Always contains the value 0.
H323 Unit ID	Not supported. Always contains the value 0.

Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1

Field	Description
Network Type	The type of network between the participant and the MCU, as follows: 0 - ISDN (audio/video) 2 - H.323 5 - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value 0.

Field	Description
Video Protocol	The video protocol used by the participant, as follows: 1 - H.261 2 - H.263 4 - H.264 255 - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest). Each unit movement increases or decreases the volume by 3 dB.
Undefined Participant	Indicates whether aren't the participant is an undefined participant, as follows: 0 - The participant isn't an undefined participant. 2 - The participant is an undefined participant.
Node Type	The node type, as follows: 0 - MCU 1 - Terminal
Bonding Phone Number	The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel. **Note:** This field is only relevant to ISDN (audio/video) participants.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection.

Field	Description
H.323 Participant Alias Type/SIP Participant Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Participant Alias Name/SIP Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants - the participant alias. May contain up to 512 characters. For SIP participants - the participant address. May contain up to 80 characters.

Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2

Field	Description
Encryption	Indicates the participant's encryption setting as follows: 0 - The participant isn't encrypted. 1 - The participant is encrypted. 2 - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Event Fields for Events 2011, 2012, and 2016

Field	Description
IP V6	IPv6 address of the participant's endpoint.

Event Fields for Event 3010 - PARTICIPANT INFORMATION

Field	Description
Info1 Info2 Info3 Info4	The participant information fields. These fields enable users to enter general information about the participant, such as the participant's email address. The maximum length of each field is 80 characters.
VIP	Not supported. Always contains the value 0.

Event Fields for Event 5001 - CONFERENCE START CONTINUE 4

Field	Description
Conference ID	The conference ID.
Conference Password	The conference password. An empty field "" means that no conference password was assigned to the conference.
Chairperson Password	The chairperson password. An empty field "" means that no chairperson password was assigned to the conference.
Info1 Info2 Info3	The contents of the conference information fields. These fields enable users to enter general information for the conference, such as the company name, and the contact person's name and telephone number. The maximum length of each field is 80 characters.
Billing Info	The billing code.

Note: When this event occurs as the result of a change to the value of one of the event fields, the event only contains the value of the modified field. All other fields are empty.

Event Fields for Event 6001 - CONFERENCE START CONTINUE 5

Field	Description
Encryption	Indicates the conference encryption setting, as follows: 0 - The conference isn't encrypted. 1 - The conference is encrypted.

Event Fields for Event 11001 - CONFERENCE START CONTINUE 10

Field	Description
Display Name	The Display Name of the conference.

Restoring System Defaults

Topics:

Administrators can erase the current configurations and restore default system settings for RealPresence Collaboration Server, Appliance Edition, 1800, 2000, and 4000.

Administrators must have access to the RealPresence Collaboration Server and have the USB flash drive included as part of the installation accessory kit where the server's LAN configuration information was saved.

You can use one of the following options:

- **Standard restore**: Delete customer conferencing entities and keep only system default conferencing entities. However, the system doesn't delete the management network service and license information.
- **Comprehensive restore**: Restore the MCU to factory defaults for the current software version. The system deletes the default management network and license information and formats the system hard disk file partition.

Perform a Standard Restore from a USB Flash Drive

This section describes the process to perform a standard restore from a USB flash drive.

A standard restore deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition, a standard restore deletes all of the conferencing entities:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service

When the system restarts, it recreates these conferencing entities based on the system defaults. In addition, the **Fast Configuration Wizard** runs automatically, enabling the user to configure the Default IP Network Service.

Procedure

1. Connect a PC to the RealPresence Collaboration Server.
2. Using Internet Explorer, connect to the RealPresence Collaboration Server by entering its IP address into the browser address bar.

   The **RMX Web Client** starts up.
3. Insert the USB flash drive that includes the server's initial LAN configuration information (IP addresses, etc.) into the USB port on the RealPresence Collaboration Server back panel.
4. In the RMX Web Client, select **Administration** > **Tools** > **Restore Factory Defaults**.
5. In the **Restore Factory Defaults** dialog, select **Standard Restore**.
6. Choose **Backup & Continue** or **Continue**.

   Backup & Continue backs up the current RealPresence Collaboration Server configuration. Select this option to keep the current conferencing entities and system configuration.

   Continue erases all of the current system configuration files and conferencing entities and restores them to their system default values.
7. If you chose **Backup & Continue**, click **Browse** in the **Backup Configuration Dialog** dialog and browse to the location at which to store the backup.

   The system initiates the backup of the RealPresence Collaboration Server configuration files. When the **backup** completes, a confirmation dialog is displayed. To cancel the backup, click **Close**.
8. Click **Yes** or **Backup** to restore the RealPresence Collaboration Server.
9. When prompted to reset the system now, click **Yes**.

   Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview.

Comprehensive Restore

Restore the MCU to the default settings of the current software version.

In addition to files deleted when you perform a standard restore, the following files are also deleted:

- CFS license information
- Management Network Service

Note: After a Comprehensive Restore, the Product Activation Key is required to reconfigure the Management Network Service during the First Entry Configuration.

You can perform a comprehensive restore in one of the following ways:

- Using the RMX Web Client (recommended)
- Using the USB flash drive

Warning: Inserting a USB flash drive containing the following files causes the RealPresence Collaboration Server to exit Secure Mode and perform a Comprehensive Restore:

- RealPresence Collaboration Server (RMX) 2000/4000 - `RestoreToFactoryDefault.txt` and `lan.cfg`.
- RealPresence Collaboration Server (RMX) 1800 -`USB_action.cfg` and `lan.cfg`.

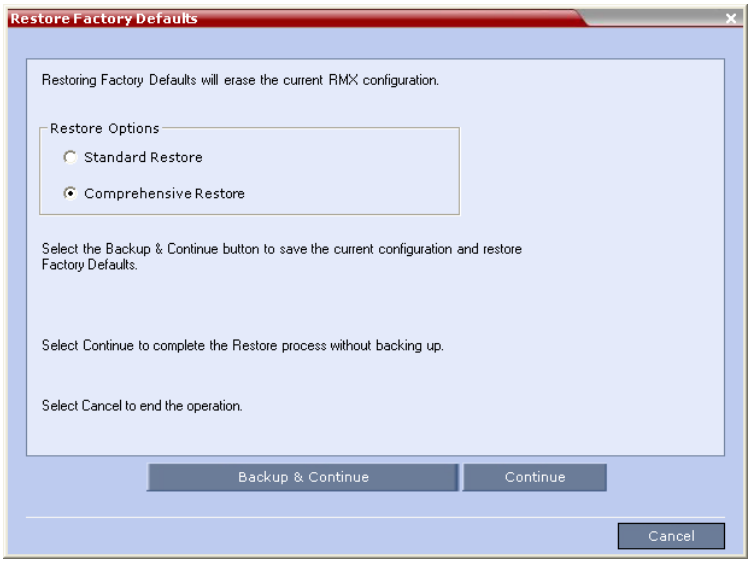
Don't insert a USB flash drive into the RealPresence Collaboration Server's USB port unless it is your intention to disable Secured Mode or perform a Comprehensive Restore to system defaults.

Perform a Comprehensive Restore Using the RMX Web Client

You should comprehensively restore your system using the RMX Web Client if possible.

Procedure

1. In the RMX Web Client, select **Administration** > **Tools** > **Restore Factory Defaults**.
2. In the Restore Factory Defaults dialog, select **Comprehensive Restore**.



3. Click one of the following buttons:
   - **Backup & Continue** - Backup of the current RealPresence Collaboration Server configuration. Select this option if you wish to restore the current conferencing entities and system configuration after the Standard Restore.Proceed with step 4.
   - **Continue** - Initializes all the current system configuration files and conferencing entities and then restores them to their system default values according to the selected restore level.Proceed with step 5.
   - **Cancel** - cancels and exits this dialog.
4. In the **Backup Configuration Dialog** dialog, click **Browse** to select the **Backup Directory Path** and select **Backup**.

The system initiates the backup of the RealPresence Collaboration Server configuration files. When the **backup** completes, a confirmation dialog box is displayed. To cancel the backup, click **Close**.

5. Click **Yes** to restore the RealPresence Collaboration Server.
6. When prompted to reset the system now, click **Yes**.
7. Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview.

Comprehensive Restore Using a USB Flash Drive

Use the USB flash drive for system restore only when you can't do it from the system Web Client. For example, when the Web Client is inaccessible.

Perform a USB Comprehensive Restore for RealPresence Collaboration Server 2000/4000

You can use a USB flash drive to perform a comprehensive restore for the RealPresence Collaboration Server.

Procedure

1. **Optional.**

   Back up the system configuration:

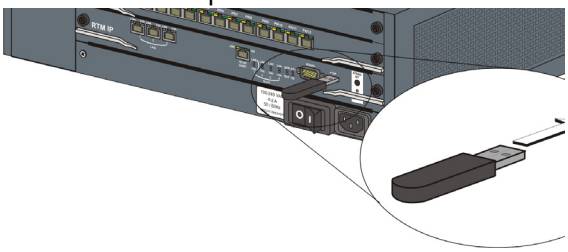
   a. In the RMX Web Client, select **Administration** > **Software Management** > **Backup Configuration.**

   b. Browse to select a backup directory, and click **Backup**.

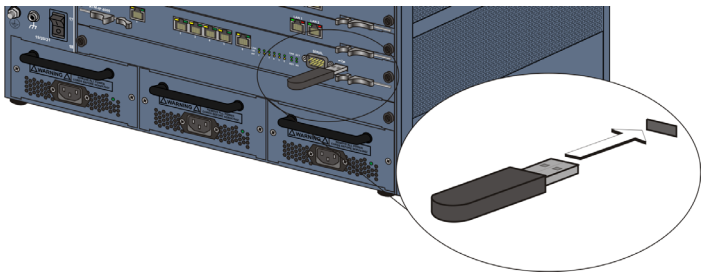
   Perform this step if you wish to restore the current conferencing entities and system configuration after the Comprehensive Restore.
2. Insert the USB flash drive that was included with your system into the workstation.

   By default, the USB flash drive contains files `ToFactoryDefault.txt` and a `lan.cfg` file, which are used to trigger the restore. However, if they're missing, you can create two blank .txt files with these names. (The content of these two files doesn't matter.)

   - RealPresence Collaboration Server (RMX) 2000 - At the bottom right corner of the RTM IP card on the back panel..

   - RealPresence Collaboration Server (RMX) 4000 - at the bottom right corner of the RTM IP 4000 card on the back panel.



3. Power off and then power on the RealPresence Collaboration Server.
4. Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview

Perform a USB Comprehensive Restore for RealPresence Collaboration Server 1800

You can use a USB flash drive to perform a comprehensive restore for the RealPresence Collaboration Server.

Procedure

1. Insert the USB flash drive that is included with the system into your workstation:
   - In Windows XP:

     The **Polycom Documentation** option is automatically selected. Click **OK**.
   - In Windows 7:

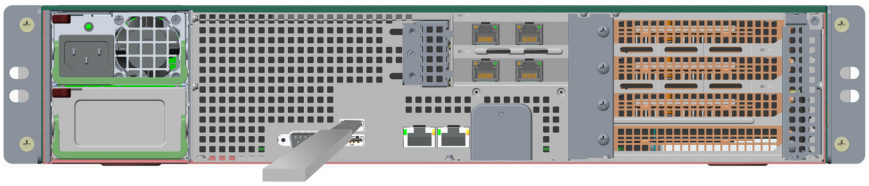
     Select **Open Folder to view files using Windows Explorer**.
2. Double-click the index.hta file.
3. In the **Language Menu** window, click the hyperlink for the required documentation language.
4. In the **Polycom End User Licenses Agreement** window, read the agreement and click the **Accept Agreement** button.

   In the **Product Type Selection** window, click **RealPresence Collaboration Server 1800**.
5. Under the **Support Utilities**, select **Restore to Factory Defaults**.
6. **Optional.**

   In **Restore to Factory Defaults** window, select **LAN Configuration** and configure the following:
   - Control Unit IP Address
   - Subnet Mask:
   - Default Router IP Address

   This configures the system to the local network so the administrator can access the RMX Web Client from the local workstation when the system restarts.

   If you skip this step, you can configure these settings later using the **LAN Configuration Utility** included on the USB flash drive.
7. Remove the USB flash drive from the workstation.
   - Insert the USB flash drive into either of the two USB ports on the back panel of the RealPresence Collaboration Server (RMX) 1800.



8. Power off and then power on the RealPresence Collaboration Server 1800.
9. Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview

Perform a Comprehensive Restore While in Ultra Secure Mode

When the RealPresence Collaboration Server is in Ultra Secure Mode, restoring RealPresence Collaboration Servers 1800, 2000, and 4000 using the USB port can be used to set it back to its factory default settings, if for any combination of factors the system becomes unstable or unmanageable.

Procedure

1. Backup Configuration Files. These files will be used to restore the system in Step 13.
2. Configure a workstation for Direct Connection.
3. Connect to the RealPresence Collaboration Server and the workstation using a LAN cable.
4. Into the RealPresence Collaboration Server's USB port, insert a USB flash drive containing a file named `RestoreToFactoryDefault.txt` and also containing a `lan.cfg` file.

Note: Don't insert a USB flash drive containing a file named `RestoreToFactoryDefault.txt` if the USB flash drive doesn't also contain a `lan.cfg` file.

---

5. Restart the RealPresence Collaboration Server.
6. If you aren't using an RealPresence Collaboration Server 4000 continue with Step 9.
7. Into the RealPresence Collaboration Server's USB port, insert a USB flash drive containing a file named `lan.cfg` file only.
8. Restart the RealPresence Collaboration Server.
9. From the workstation, connect to the RealPresence Collaboration Server's Alternate Management Network.
10. Apply the Product Activation Key.
11. Unplug the USB flash drive.
12. Restart the RealPresence Collaboration Server.
13. Restore the System Configuration from the backup by applying the backup files created in procedure step 1.
14. Restart the RealPresence Collaboration Server. (If the RealPresence Collaboration Server is unresponsive after these procedures a further restart may be necessary.)
15. Enable Secured Communication and reapply the Certification procedures.

Related Links

Alternate Management Network on page 342
Certificate Configuration and Management on page 346

Polycom Lab Features

Topics:

Polycom enables examining experimental features of Polycom® RealPresence® Collaboration Server.

These features may be later incorporated as constant features, but at this point are neither tested nor supported.

Only an Administrator may access the experimental features, provided the RealPresence Collaboration Server is in experimental mode.

Experimental features activation doesn't require system restart, and take effect immediately on newly created conferences.

Note: Don't activate any of the lab features in RealPresence Collaboration Server used at production sites. Any attempt to do so is at your own peril.

Inactivated features cannot be viewed or examined.

Lab Features Guidelines

Use the following guidelines when enabling experimental lab features.

- Experimental Features may be enabled both via user interface, as described above, or via XML API.
- The user interface displays the list of available Lab features according to the Interface / RMX Manager version, and not according to the RealPresence Collaboration Server version. Therefore, the used Interface / RMX Manager should match the current RealPresence Collaboration Server version, to allow enabling new Lab features.

  In that context, if the Interface / RMX Manager version is higher than that of the RealPresence Collaboration Server, the newer options are displayed, though the RealPresence Collaboration Server doesn't support them.
- Enabling a Lab feature merely results in display of feature-related check box in **Profile/Conference Properties** dialog. Selecting the check box at the conference/profile level activates the feature for that specific conference, or new conferences launched using this specific profile.
- Disabling Lab Features only inactivates them, but preserves their respective check boxes values. Thus, should the Lab Features be reactivated in general, their respective status from before the general inactivating is resumed.

  However, ongoing conferences retain the Lab features activation and status from their creation point.
- Lab Features settings are preserved during Backup & Restore operations, even when involving upgrading to a higher version, in which case an adjustment of the appropriate system flags and/or setting is performed.

- When Lab Features are enabled, conferencing profiles defined in the MCU are preferred to those defined in Poly Clariti Core.
- In cascaded environments, the Administrator should verify the Lab Features settings across all the cascaded MCUs are the same.

Activate Experimental Lab Features

You can activate and deactivate the experimental lab features by selecting Polycom Labs from the Setup menu.

Procedure

1. In the RealPresence Collaboration Server main menu, select **Setup** > **Polycom Labs**.
2. Select **Enable Polycom Lab Features** to enable experimental mode.
3. Select the check box of one or more features you wish to enable.
4. Click **OK** to confirm.

At this point, the selected lab features may be activated via their respective activation points in the UI.

Current RealPresence Collaboration Server Lab Features

This section lists the current RealPresence Collaboration Server lab features.

Discussion Mode Layout

RealPresence Collaboration Server can identify conferencing scenarios, in which either one or two participants are one or more main/only speakers.

Feature Description

AVC endpoints in CP Only or mixed CP and SVC conferences, view the conference in either a 1+7 or a 2+8 layout (depending on the number of main speakers), with the main speakers video displayed in one or more main cells, as shown in the table below.

Layouts Used in Discussion Mode

Number of Active Speakers	Layout Name	Layout
1	1+7	
2	2+8	

Discussion Mode is triggered once the number of participants reaches a minimum, and one of the participants becomes the active speaker by speaking over a time interval.

Feature Specifications

This brief specification documents the following Polycom Lab Feature.

Discussion Mode Layout Specifications

Specification	Scope
Release Feature Is Being Tested In:	Polycom RealPresence Collaboration Server 8.7.1
Level of Testing Performed to Date:	• None • Full Unit Tested • Feature Unit and Product Regresstion Tested • Full Feature Unit, Product Regression, and Solution Tested

To find out more about this Polycom Lab feature or provide feedback on this feature, contact Polycom Support.

Layout Usage Criteria

This section describes the Layout useage criteria.

- A 1+7 layout is used for single speaker scenarios.
- While a 1+7 layout is used, should another participant become an active speaker, the 1+7 layout is replaced by a 2+8 layout.
- While a 2+8 layout is used, once another participant becomes the active speaker, its video, if exists (i.e. not an audio participant and video isn't muted), replaces that of the active speaker preceding the last speaker. If no video is sent for the speaker, both the layout and speakers remain as is.
- While a 2+8 layout is used, and only one participant remains the active speaker, the 2+8 layout is replaced by a 1+7 layout, with the two least active participants moved out of the layout.
- The active speakers don't view their own video, but that of one or more last active speakers.
- At all times, the most recent active speaker is displayed in the top-left cell. The smaller cells are populated bottom up, right to left.
- More than 10 participants don't result in using layouts with larger number of cells.

Discussion Mode Layout System Flags

This section lists the System Flags for Discussion Mode Activation.

System Flags for Discussion Mode Activation

Flag Name	Flag Description
`DISCUSSION_DISPLAYED_PARTICIPNATS_TO_START`	The minimal visual participants required to trigger Discussion Mode. Visual participants are video participants with an active video, or one of the two static video participants included in the conference layout. This system flag required a manual addition to be modified, and immediately affects new conferences (that is, not reset required). Default value: 8 **Note:** A value of 7 results in activating Discussion Mode with 7 participants, with the speaker cell included.

Flag Name	Flag Description
DISCUSSION_MODE_ACTIVE_SPEAKER_FOCUS_INTERVAL	The time interval, in seconds, after which a participant becomes an active speaker, thus the minimum duration for its display in one or more main cells. This system flag required a manual addition to be modified, and immediately affects new conferences (that is, not reset required). Default value: 20 (seconds) Minimal value: 10 (seconds)

Related Links

System Flags on page 264

Guidelines for Implementing Discussion Mode Layout

Use the following guidelines for issues related to Discussion Mode layout.

- Recording link layout isn't altered, as well as the layout sent to the recording link. The recording link layout displays as many participants as possible, with the recording link cell the first to be discarded.
- Discussion Mode is inactive when in Legacy content mode (that is, content sent via people video layout).
- In cascading conferences, depending on the value of the system flag FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION:
  - When value is YES - Only the active speaker is sent over the cascading link, where that link is one of the participants in the Discussion Mode layout.
  - When value is NO - The Discussion Mode layout is sent over the cascading link, and is displayed in the cascading link participant cell.

Interactions Between Discussion Mode Layout and Other Features

This section describes the inetractions between Discussion Mode Layout and other features.

- Participants may be assigned a Personal Layout.
- A participant may set its own layout via Click & View.
- Participants layout may be modified via PCM.
- Discussion Mode is applicable in Same Layout scenarios.
- Discussion Mode is inactive in Presentation Mode, Lecturer Mode, and Telepresence Mode.
- When Exclude Static Room from Layout is on:
  - Static rooms video is the last to be displayed in Discussion Mode layout cells, unless it belongs to either the current or last active speaker.
  - The DISCUSSION_DISPLAYED_PARTICIPNATS_TO_START system flag counting may take up to two static rooms into account.

Enable the Discussion Mode Layout Feature

You can enable and disable the discussion mode feature in the conference properties.

Procedure

1. Do one of the following:
   - Right-click on a CP Only or Mixed CP and AVC conferencing profile, and select **Profile Properties**.
   - Right-click on a CP Only or Mixed CP and AVC conference, and select **Conference Properties**.
2. Select the **Video Settings** tab.
3. Select the **Discussion Mode** check box.
4. Click **Apply**, then click **OK**.

Exclude Inactive Video Participants from Layout

RealPresence Collaboration server can exclude inactive video participants from the call layout.

Feature Description

In many conferences, some cells displaying static video can be observed. This may occur either due to the endpoint camera not focusing on people, or when video is disabled.

To enhance the user experience, the RealPresence Collaboration Server preserves mainly significant video in the conference layout, by excluding inactive-video rooms from the conference layout, in both AVC and SVC endpoints.

Feature Specifications

This brief specification documents the following Polycom Lab Feature.

Exclude Inactive Video Participants from Layout Specifications

Specification	Scope
Release Feature Is Being Tested In:	Polycom RealPresence Collaboration Server 8.7.1
Level of Testing Performed to Date:	• None • Full Unit Tested • Feature Unit and Product Regresstion Tested • Full Feature Unit, Product Regression, and Solution Tested

To find out more about this Polycom Lab feature or provide feedback on this feature, contact Polycom Support.

Guidelines for Removing Static Room Video from Conference Layouts

Use the following guidelines when removing static room video from conference layouts.

How RealPresence Collaboration Server removes static room video from conference layouts depends on the conference mode.

AVC Endpoints:

- Auto Layout is defined by the number of active video participants + maximum of 2 static video participants.
- Free cells are populated by static video participants.
- Once an endpoint is detected as a static video endpoint, it's removed from the layout upon the next layout change, either participant join/leave, or change in active speaker.

  Note: The same applies to static video room becoming active video room.

- So long as the static video room is either the active or last speaker, it remains in the conference layout.

SVC Endpoints:

- The layout used by the endpoint is determined by the endpoint.
- This feature is active for SVC endpoints in mixed conferences:
  - In soft MCU - At beginning of conference
  - In HW MCU - Once the first AVC endpoint connects.
- SVC endpoints request numerous video streams, which populate the layout cells according to the MCU internal considerations, where static video rooms are prioritized lower than active video rooms, unless they represent the current or last active speakers.

Interactions Between Excluding Inactive-Video Participants from Layout and Other Features

This section describes the interactions between excluding video participant from layout and other features.

- Video participants count is unaffected by the exclusion of inactive-video participants from the conference layout. Therefore, so long as there are less than a hundred video participants, their presence is exposed by the count.
- Static video Telepresence rooms aren't removed from the conference layout, provided the **Telepresence Layout Mode** is defined as **Speaker Priority**.
- Recording link layout is not affected by this feature, however static video rooms have the lowest priority in the recording link layout population.
- This feature is fully compatible with the Discussion Mode Layout feature (see separate addendum).
- This feature is fully compatible with panoramic view:
  - If panoramic view is comprised of a multitude of endpoints - The same as with Auto Layout.
  - If panoramic view is comprised of a Telepresence room - The entire room is displayed, regardless of any static video components in the Telepresence room.
- A participant forced in the layout is always displayed, even if its video is inactive.

Enable the Exclude Inactive Video Participants from Layout Feature

You can enable and disable the Exclude Inactive Video Participants from Layout feature in the conference properties.

Procedure

1. Do one of the following:

- Right-click on a **CP Only** or **Mixed CP and AVC** conferencing profile, and select **Profile Properties**.
- Right-click on a **CP Only** or **Mixed CP and AVC** conference, and select **Conference Properties**.

2. Select the **Video Settings** tab.
3. Select the **Exclude static-video rooms from layout (Beta)** check box.
4. Click **Apply**, then click **OK**.

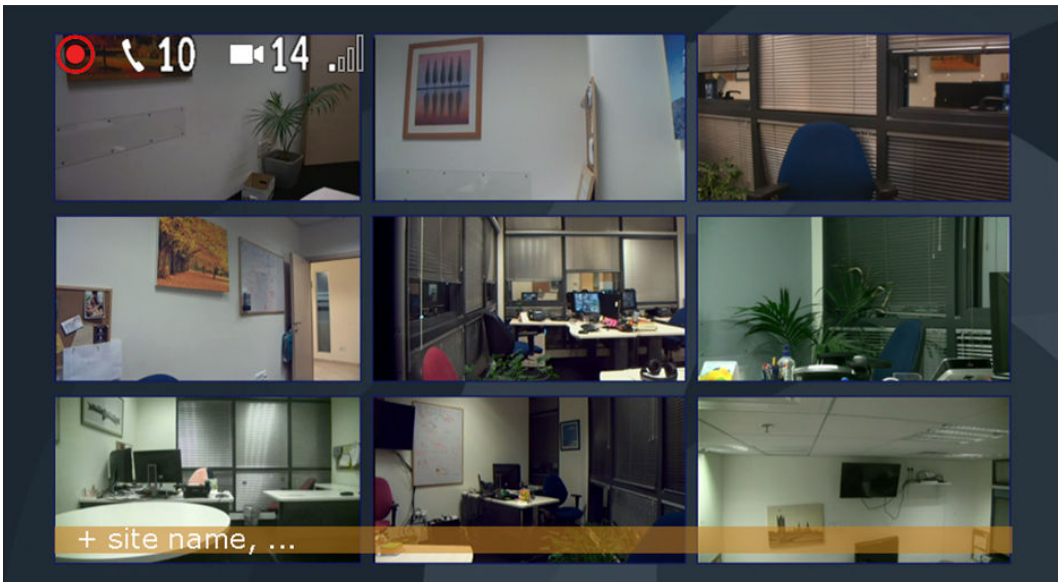
Pop-Up Site Name on Participant Join/Leave

RealPresence Collaboration Server provides video AVC endpoints with indication on participant names upon their joining / leaving the conference.

Feature Description

Site name (at most times, the participant name), when enabled, appears accompanied by either a **+** upon participant joining the conference, or a **-** upon leaving it. By default, the site name appears upon participant joining, but not upon its leaving. The site name display duration is the same for joining and leaving, and ranges between 5 and 240 seconds with 10 seconds as the default.

Additional participants joining or leaving the conference, result in adding **…** to the currently displayed site name, but no additional site names, as shown in the following image.



Feature Specifications

This brief specification documents the following Polycom Lab Feature.

Pop-Up Site Name on Particpant Join/Leave Specifications

Specification	Scope
Release Feature Is Being Tested In:	Polycom RealPresence Collaboration Server 8.7.1

Specification	Scope
Level of Testing Performed to Date:	• None • Full Unit Tested • Feature Unit and Product Regresstion Tested • Full Feature Unit, Product Regression, and Solution Tested

To find out more about this Polycom Lab feature or provide feedback on this feature, contact Polycom Support.

Guidelines for Implementing Site Name Pop-Up on Participant Join/Leave

Use the following guidelines when implementing site name pop-up when a particpants joins or leaves a conference.

- The site name display utilizes the message overlay mechanism, thus both are enabled/disabled simultaneously, and conform to identical settings, such as color, font size, and horizontal location.
- Message overlay is replaced by site name upon participant joining/leaving for the specified duration, after which the message overlay display is renewed for static message overlay.

  Also, site name display is replaced by message overlay until the next participant joining/leaving.

  The same applies to encrypted message overlay.

Site Name Display Triggering

Thise section describes how the site name display is triggered.

- Both SVC and audio participants, although incapable of viewing the site name, trigger their site name display at the AVC endpoints.
- Content participants don't trigger this feature.
- Lync clients RealConnect-ed to conferences, don't trigger this feature.
- ITP, non-TIP, room triggers this feature, but is considered as a single participant, even in scenarios where the ITP room includes multiple endpoints. In the ITP room itself, the site name is displayed only on its main screen.

  TIP enabled conferences are incompatible with this feature.
- Cloud Axis clients trigger display of site name, thus might view duplicate display of site name; one due to the Web client features, the other, due to this feature.
- When MCUs are cascaded, neither the cascading link, nor the cascaded MCU participants, trigger display of site name at the other MCU participants.
- Recording link participants don't trigger this feature (as there's already a recording indication), however, site names is sent over the recording link.

  The playback link acts exactly the opposite - The link triggers site name display, but the site name isn't sent over the playback link video.

Enable the Pop-Up Site Name Feature

You can enable and disable the Pop-Up Site Name feature in the conference properties.

- This feature is applicable only to AVC endpoints, and to CP Only and Mixed CP and SVC conferences.
- All user interface pertaining to this feature appear only if in the dialog below:

- Polycom Lab features are enabled in general.
- The feature check-box is selected.

Procedure

1. Right-click on a CP Only or Mixed CP and AVC conferencing profile, and select **Profile Properties**.
2. Select the **Layout Indications** tab.
3. In the **Textual site name display** section, configure the following options:
   - Whether to enable/disable site name display upon participant joining the conference.
   - Whether to enable/disable site name display upon participant leaving the conference.
   - The site name display **Duration**.
4. Click **Apply**, then click **OK**.

Using Video Clips for IVR Services

RealPresence Collaboration Server can use a video clip instead of a static slide for IVR services when connecting to a conference via an entry queue.

Feature Description

When you implement this feature, you can perform the following tasks:

- Using a motion slide (video clip) instead of a still slide.
- Replacing the default motion slide Poly supplies (within both installation and upgrade packages), which is named `General_Polycom_Slide_Motion`, with a different video slide.
- Receiving motion slides from Poly Clariti Core for external IVRs.

Note: The audio prompt to the video slide is taken from the IVR associated with it.

Feature Specifications

This brief specification documents the following Polycom Lab Feature.

Using Video Clips for IVR Services Specifications

Specification	Scope
Release Feature Is Being Tested In:	Polycom RealPresence Collaboration Server 8.7.1
Level of Testing Performed to Date:	• None • Full Unit Tested • Feature Unit and Product Regresstion Tested • Full Feature Unit, Product Regression, and Solution Tested

To find out more about this Polycom Lab feature or provide feedback on this feature, contact Poly Support.

Guidelines for Using Video Clips for IVR Services

Use the following guidelines when using video clips for IVR services.

- Since TIP endpoints are sometimes prone to encountering problems with customizing IVR slides, it's possible to block video slides for TIP endpoints via the `ENABLE_MOTION_SLIDE_TO_TIP_EPS` system flag (see below), in which case these endpoints can't view video clips.
- Video clips size is limited to 5M to prevent memory overflow. Thus, up to 10 motion slides per a local IVR may be loaded by the Administrator user.
- Bit rates are preset as described in the table below.

Bit rate values per Resolution

Resolution	Frame Rate	Preset bit rate (Kbps)
CIF	30	384
SD	30	768
HD720	30	1024
HD1080	30	2048

- Users should attempt slide customization for inactive time intervals (that is, with no active or scheduled conferences) due to the heaviness of the process of the clip customization to MCU video format.
- Video clips for customization are characterized by:
  - **Format** - avi, mp4, mov, mpeg only
  - **Resolution** - 1080p30 only
  - **Duration** - 10 seconds. Up to 30 seconds are accepted, though it's truncated to 10 seconds.

    Due to clips cyclic playing, it's recommended to harmonize the clip end and beginning.
  - **Effects** - Avoid light effects to prevent imperfect translation to MCU video format.

Motion Slide Blocking for TIP Endpoints System Flags

This section lists the System Flags for Motion Slide blocking for TIP Endpoints.

System Flags for Motion Slide Blocking for TIP Endpoints

Flag Name	Flag Description
`ENABLE_MOTION_SLIDE_TO_TIP_EPS`	Enables displaying motion slides to TIP endpoints. This system flag required a manual addition to be modified, and if modified, value takes effect immediately (that is, not requires reset) for new conferences. Range: `YES` (default), `NO` **Note:** Set this flag to `NO` if you experience difficulties in viewing motion slides in TIP endpoints connected to your RealPresence Collaboration Server.

Related Links

System Flags on page 264

Select a Video Clip for an IVR Service

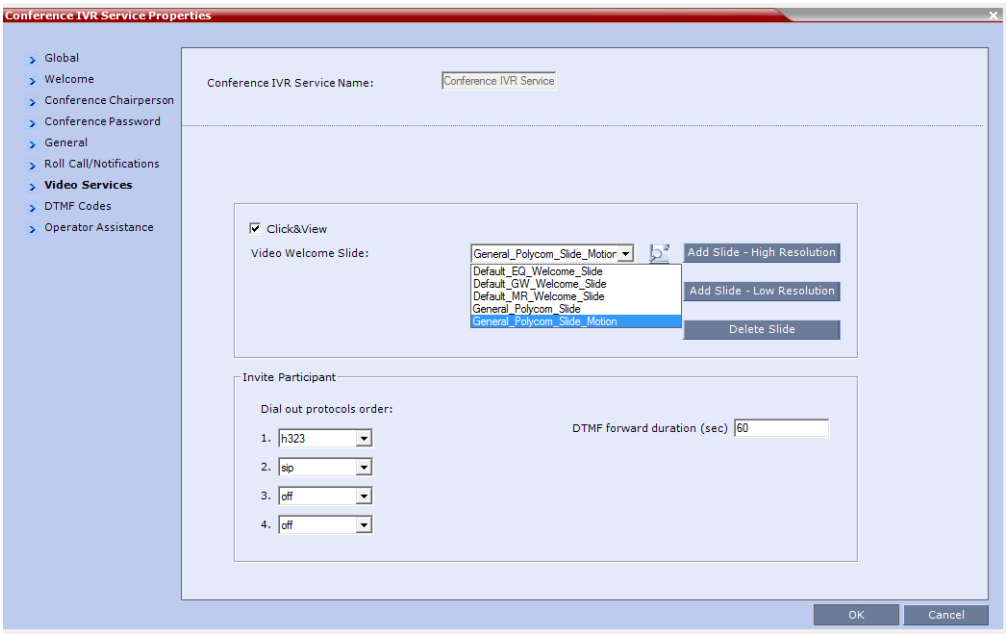
You can select a video clip to use for an IVR service in RMX Manger.

- This feature requires CIF as a minimum resolution supported by the endpoint.
- The media type supported by the endpoint may be H.263, H.264 (Base Profile only), RTV, and TIP. H.261 and H.264 High Profile endpoints aren't supported.

There are no additional steps to enable or disable this feature beyond activating the feature in the **Polycom Labs** screen.

Procedure

1. Open the **IVR Services** tab in RMX Manager.
2. Right-click on **Conference IVR Service** and select **Properties**.
3. Select the **Video Services** tab.



4. In the **Video Welcome Slide** list, select the video clip to use for the IVR service.
5. Click **OK**.

Troubleshooting

Topics:

This section includes information related to troubleshooting issues with your RealPresence Collaboration Server. You can also find information on downloading and using logs.

- Alerts and Active Alarms
- Disconnection Causes
- Event Auditor
- Log Management

Alerts and Active Alarms

Topics:

RealPresence Collaboration Server provides alerts and alarms to help you troubleshoot and respond to issues.

System and Participant Alerts

The MCU alerts users to any faults or errors encountered during operation.

Two indication bars labeled System Alerts and Participant Alerts signal users of system errors by blinking red in the event of an alert.

View System Alerts

The RealPresence Collaboration Server generates system alerts when the it detects errors.

The System Alerts indicator bar blinks red, prompting the user to view the active alarms. Once viewed, the System Alerts indicator bar stays red until the errors are resolved. The RealPresence Collaboration Server records system alerts and can generated a report that can be saved in *.txt format.

Procedure

1. In RMX Manager, click the red blinking **System Alerts** indication bar.

   The **Active Alarms** list identifies the errors that have not been resolved. The following columns appear in the **Active Alarms** pane:

   Active Alarms Pane Columns

Field	Description
ID	An identifying number assigned to the system alert.
Time	Lists the local date and time that the error occurred. This column also includes the icon indicating the error level (as listed in the level column).
GMT Time	Lists the date and time according to Greenwich Mean Time (GMT) that the error occurred.

Field	Description
Category	Lists the type of error. The following categories may be listed: • **File** - Indicates a problem in one of the files stored on the MCU's hard disk. • **Card** - Indicates a card problem. • **Exception** - Indicates a software error. • **General** - Indicates a general error. • **Assert** - Indicates an internal software error reported by the software. • **Startup** - Indicates an error during system startup. • **Unit** - Indicates a problem with a unit. • **MPL** - Indicates an error related to a Shelf Management component (MPL component) other than an MPM media card, RTM, or switch board (RealPresence Collaboration Server 2000/4000 only).
Level	Indicates the severity of the problem, or the type of event. There are three fault level indicators: Major Error. System Message. Startup Event.
Code	Indicates the problem, as indicated by the error category.
Process Name	Lists the type of functional process involved.
Description	When applicable, displays a more detailed explanation of the problem.

2. Click one of the following buttons to view a respective report in the **System Alerts** pane:

System Alerts Buttons

	Active Alarms (default) - The default report list displayed in the System Alerts indication bar. Contains the current system errors, and supplies a quick indication on MCU status.
	Faults Full List - A full list of system faults. **Note:** Viewed when logging in as a special support user.
	Faults List - A list of previous faults (whether they were solved or not) for support or debugging purposes.

3. To save the **Active Alarms**, **Faults Full List**, or **Faults** report:
   - To a text file, click **Save to Text** .
   - To an XML file, click **Save to XML** .The **Save to XML** button is only available when logged in as a special support user.
4. Select a destination folder and enter the file name.
5. Click **Save**.

View Participant Alerts

The Participants Alerts indication bar blinks red indicating participant connection difficulties in conferences.

Once viewed, the Participant Alerts indication bar becomes statically red until the errors have been resolved in the MCU.

Participant Alerts enables users, participants and conferences to be prompted and currently connected. This includes all participants that are disconnected, idle, on standby, or waiting for dial-in. Alerts are intended for users or administrators to quickly see all participants that need their attention.

Procedure

1. In RMX Manager, click the red blinking **Participants Alerts** indication bar.

   The **Participant Alerts** pane displays similar properties to that of the **Participant List** pane.
2. To resolve participant issues that created the Participant Alerts, the administrator can either **Connect**  , **Disconnect**  or **Delete**  a participant.

Note: Following MCU reset, a delay may occur when synchronizing with the external NTP server.

Related Links

Participant Properties on page 160

Monitor Participant Packet Loss

You can configure system flags to monitor participant packet loss in conferences.

RealPresence Collaboration Server alerts you when packet loss on any media stream exceeds your defined threshold.

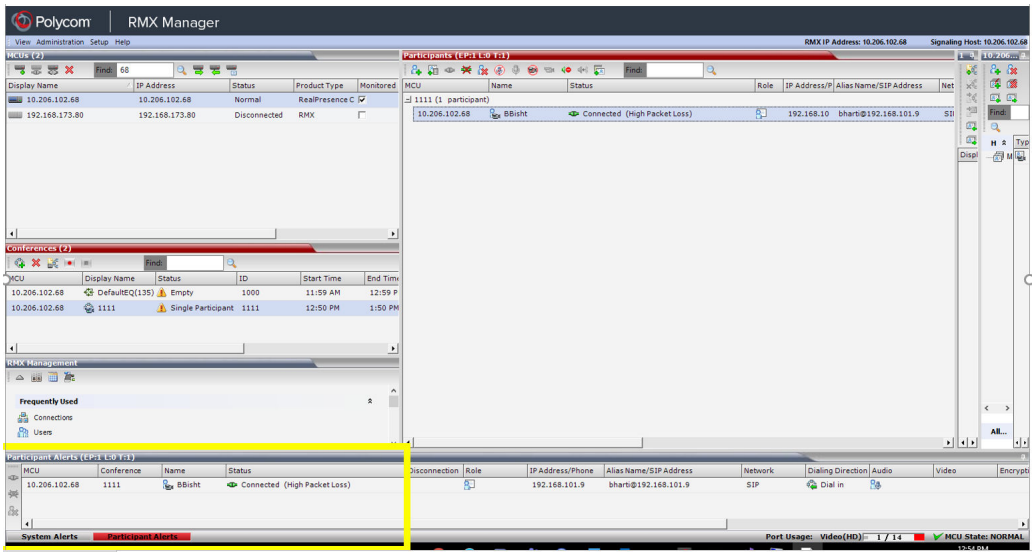
Note: This feature isn't available to audio-only dial-in or dial-out participants.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, select **New Flag**.
3. Enter `PARTY_MONITORING_TIMER_DURATION` in the **New Flag** field.
4. Enter the monitoring duration (in seconds) in the **Value** field.

   If no value entered, the system sets the value as 60 seconds.
5. Optional: To change the packet loss threshold from the default of 5%, add the system flag `THRESHOLD_FRACTION_LOSS` and set a desired value.
6. Select **OK**.
7. Select **Close**.

If the package loss exceeds the threshold, **High packet loss** alerts display in the **Participant Alerts** panel in RMX manager.



Disable Participant Packet Loss Monitoring

After you enable the participant packe loss monitoring, you can disable it by setting the system flag **PARTY_MONITORING_TIMER_DURATION** value to 0.

Note the following limitations:

- Disabling this feature during a meeting doesn't clear existing **High packet loss** alerts. This may result in faulty alerts.
- If you disable this feature during a meeting, the change takes effect for connected participants automatically and you can't re-enable it for those participants during this meeting.

Procedure

1. by setting the value of the flag **PARTY_MONITORING_TIMER_DURATION** to 0.
2. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
3. In the **MCMS_PARAMETERS_USER** tab, select the flag **PARTY_MONITORING_TIMER_DURATION** and select **Edit Flag**.
4. Enter the value 0 in the **New Value** field and click **OK**.

Disconnection Causes

Topics:

If a participant was unable to connect to a conference or was disconnected from a conference, the **Connection Status** tab in the **Participant Properties** dialog box indicates the call disconnection cause.

In some cases, a possible solution may be displayed.

A video participant who is unable to connect the video channels, but is able to connect as an audio only participant, is referred to as a Secondary participant. For Secondary participants, the Connection Status tab in the **Participant Properties** dialog box indicates the video disconnection cause. In some cases, a possible solution may be indicated.

The table below lists the call disconnection causes that can be displayed in the Call Disconnection Cause field and provides an explanation of each message.

IP Disconnection Causes

The following table lists the Call Disconnection causes.

Call Disconnection Causes

Disconnection Cause	Description
Disconnected by User.	The user disconnected the endpoint from the conference.
Remote device didn't open the encryption signaling channel.	The endpoint didn't open the encryption signaling channel.
Remote devices selected encryption algorithm doesn't match the local selected encryption algorithm.	The encryption algorithm selected by the endpoint doesn't match the MCUs encryption algorithm.
Resources deficiency.	Insufficient resources available.
Calls close. Call closed by MCU.	The MCU disconnected the call.
H323 call closed. No port left for audio.	Insufficient audio ports.
H323 call closed. No port left for video.	The required video ports exceed the number of ports allocated to video in fixed ports.
H323 call closed. No port left for FECC.	The required data ports exceed the number of ports allocated to data in fixed ports.
H323 call closed. No control port left.	The required control ports exceed the number of ports allocated to control data in fixed ports.

Disconnection Cause	Description
H323 call closed. No port left for videocont.	The required video content ports exceed the number of ports allocated to video content in fixed ports.
H323 call closed. Small bandwidth.	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. No port left.	There are no free ports left in the IP card.
Caller not registered.	The calling endpoint isn't registered in the gatekeeper.
H323 call closed. ARQ timeout.	The endpoint sent an ARQ message to the gatekeeper, but the gatekeeper didn't respond before timeout.
H323 call closed. DRQ timeout.	The endpoint sent a DRQ message to the gatekeeper, but the gatekeeper didn't respond before timeout.
H323 call closed. Alt Gatekeeper failure.	An alternate gatekeeper failure occurred.
H323 call closed. Gatekeeper failure.	A gatekeeper failure occurred.
H323 call closed. Remote busy.	The endpoint was busy. (Applicable only to dial-out)
H323 call closed. Normal.	The call ended normally, for example, the endpoint disconnected.
H323 call closed. Remote reject.	The endpoint rejected the call.
H323 call closed. Remote unreachable.	The call remained idle for more than 30 seconds and was disconnected because the destination device didn't answer. Possible causes can be due to network problems, the gatekeeper couldn't find the endpoint's address, or the endpoint was busy or unavailable (for example, the "don't disturb" status is selected).
H323 call closed. Unknown reason.	The reason for the disconnection is unknown, for example, the endpoint disconnected without giving a reason.
H323 call closed. Faulty destination address.	Incorrect address format.
H323 call closed. Small bandwidth.	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. Gatekeeper reject ARQ.	The gatekeeper rejected the endpoint's ARQ.
H323 call closed. No port left.	There are no ports left in the IP card.
H323 call closed. Gatekeeper DRQ.	The gatekeeper sent a DRQ.
H323 call closed. No destination IP address.	For internal use.
H323 call closed. Call failed prior or during the capabilities negotiation stage.	The endpoint didn't send its capabilities to the gatekeeper.

Disconnection Cause	Description
H323 call closed. Audio channels didn't open before timeout.	The endpoint didn't open the audio channel.
H323 call closed. Remote sent bad capability.	There was a problem in the capabilities sent by the endpoint.
H323 call closed. Local capability wasn't accepted by remote.	The endpoint didn't accept the capabilities sent by the gatekeeper.
H323 failure.	Internal error occurred.
H323 call closed. Remote stop responding.	The endpoint stopped responding.
H323 call closed. Master subordinate problem.	A Person + Content cascading failure occurred.
SIP bad name.	The conference name is incompatible with SIP standards.
SIP bad status.	A general IP card error occurred.
SIP busy everywhere.	The participant's endpoints were contacted successfully, but the participant is busy and doesn't wish to take the call at this time.
SIP busy here.	The participant's endpoint was contacted successfully, but the participant is currently not willing or able to take additional calls.
SIP capabilities don't match.	The remote device capabilities aren't compatible with the conference settings.
SIP card rejected channels.	The IP card couldn't open the media channels.
SIP client error 400.	The endpoint sent a SIP Client Error 400 (Bad Request) response. The request couldn't be understood due to malformed syntax.
SIP client error 402.	The endpoint sent a SIP Client Error 402 (Payment Required) response.
SIP client error 405.	The endpoint sent a SIP Client Error 405 (Method Not Allowed) response. The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.
SIP client error 406.	The endpoint sent a SIP Client Error 406 (Not Acceptable) resources. The remote endpoint can't accept the call because it doesn't have the necessary resources. The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.
SIP client error 407.	The endpoint sent a SIP Client Error 407 (Proxy Authentication Required) response. The client must first authenticate itself with the proxy.

Disconnection Cause	Description
SIP client error 409.	The endpoint sent a SIP Client Error 409 (Conflict) response. The request couldn't be completed due to a conflict with the current state of the resource.
SIP client error 411.	The endpoint sent a SIP Client Error 411 (Length Required) response. The server refuses to accept the request without a defined Content Length.
SIP client error 413.	The endpoint sent a SIP Client Error 413 (Request Entity Too Large) response. The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
SIP client error 414.	The endpoint sent a SIP Client Error 414 (Request-URI Too Long) response. The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
SIP client error 420.	The endpoint sent a SIP Client Error 420 (Bad Extension) response. The server didn't understand the protocol extension specified in a Require header field.
SIP client error 481.	The endpoint sent a SIP Client Error 481 (Call/Transaction Doesn't Exist) response.
SIP client error 482.	The endpoint sent a SIP Client Error 482 (Loop Detected) response.
SIP client error 483.	The endpoint sent a SIP Client Error 483 (Too Many Hops) response.
SIP client error 484.	The endpoint sent a SIP Client Error 484 (Address Incomplete) response. The server received a request with a To address or Request-URI that was incomplete.
SIP client error 485.	The endpoint sent a SIP Client Error 485 (Ambiguous) response. The address provided in the request (Request-URI) was ambiguous.
SIP client error 488.	The endpoint sent a SIP Client Error 488 (Not Acceptable Here) response.
SIP forbidden.	The SIP server rejected the request. The server understood the request, but is refusing to fulfill it.
SIP global failure 603.	A SIP Global Failure 603 (Decline) response was returned. The participant's endpoint was successfully contacted, but the participant explicitly doesn't wish to or can't participate.

Disconnection Cause	Description
SIP global failure 604.	A SIP Global Failure 604 (Doesn't Exist Anywhere) response was returned. The server has authoritative information that the user indicated that in the Request-URI doesn't exist anywhere.
SIP global failure 606.	A SIP Global Failure 606 (Not Acceptable) response was returned.
SIP gone.	The requested resource is no longer available at the Server and no forwarding address is known.
SIP moved permanently.	The endpoint moved permanently. The user can no longer be found at the address in the Request-URI.
SIP moved temporarily.	The remote endpoint moved temporarily.
SIP not found.	The endpoint wasn't found. The server has definitive information that the user doesn't exist at the domain specified in the Request-URI.
SIP redirection 300.	A SIP Redirection 300 (Multiple Choices) response was returned.
SIP redirection 305.	A SIP Redirection 305 (Use Proxy) response was returned. The requested resource MUST be accessed through the proxy given by the Contact field.
SIP redirection 380.	A SIP Redirection 380 (Alternative Service) response was returned. The call wasn't successful, but alternative services are possible.
SIP remote canceled call.	The endpoint canceled the call.
SIP remote closed call.	The endpoint ended the call.
SIP remote stopped responding.	The endpoint isn't responding.
SIP remote unreachable.	The endpoint couldn't be reached.
SIP request terminated.	The endpoint terminated the request. The request was terminated by a `BYE` or `CANCEL` request.
IP request timeout.	The request was timed out.
IP server error 500.	The SIP server sent a SIP Server Error 500 (Server Internal Error) response. The server encountered an unexpected condition that prevented it from fulfilling the request.
IP server error 501.	The SIP server sent a SIP Server Error 501 (Not Implemented) response. The server doesn't support the functionality required to fulfill the request.

Disconnection Cause	Description
IP server error 502.	The SIP server sent a SIP Server Error 502 (Bad Gateway) response. The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
IP server error 503.	The SIP server sent a SIP Server Error 503 (Service Unavailable) response. The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.
IP server error 504.	The SIP server sent a SIP Server Error 504 (Server Time-out) response. The server didn't receive a timely response from an external server it accessed in attempting to process the request.
IP server error 505.	The SIP server sent a SIP Server Error 505 (Version Not Supported) response. The server doesn't support, or refuses to support, the SIP protocol version that was used in the request.
IP temporarily not available.	The participant's endpoint was contacted successfully but the participant is currently unavailable (for example, not logged in or logged in such a manner as to preclude communication with the participant).
IP remote device didn't respond in the given time frame.	The endpoint didn't respond in the given time frame.
SIP trans error TCP Invite.	A SIP Invite was sent via TCP, but the endpoint wasn't found.
SIP transport error.	Unable to initiate connection with the endpoint.
SIP unauthorized.	The request requires user authentication.
SIP unsupported media type.	The server is refusing to service the request because the message body of the request is in a format not supported by the requested resource for the requested method.

ISDN Disconnection Causes

The following table lists the ISDN Disconnection causes.

ISDN Disconnection Causes

Number	Summary	Description
1	Unallocated (unassigned number).	No route to the number exists in the ISDN network or the number wasn't found in the routing table. • Ensure that the number appears in the routing table. • Ensure that it's a valid number and that correct digits were dialed.
2	No route to specified transit network (national use).	The route specified (transit network) between the two networks doesn't exist.
3	No route to destination.	No physical route to the destination number exists although the dialed number is in the routing plan. • The PRI D-Channel is malfunctioning. • Incorrect connection of the span or WAN.
4	Send special information tone.	Return the special information tone to the calling party indicating that the called user can't be reached.
5	Misdialed trunk prefix (national use).	A trunk prefix has erroneously been included in the called user number.
6	Channel Unacceptable.	The sending entity in the call doesn't accept the channel most recently identified.
7	Call awarded and being delivered in an Established channel.	The incoming call is being connected to a channel previously established for similar calls.
8	Pre-Emption.	The call has been pre-empted.
9	Pre-Emption - Circuit reserved for reuse.	Call is being cleared in response to user request.
16	Normal Call Clearing.	Call cleared normally because user hung up.
17	User Busy.	Dialed number is busy.
18	No User Responding.	The called user hasn't answered the call.
19	No Answer from User (User Alerted).	Called user has received call alert, but hasn't responded within a prescribed period of time. Internal network timers may initiate this disconnection.
20	Subscriber Absent.	User is temporarily absent from the network - as when a mobile user logs off.

Number	Summary	Description
21	Call Rejected.	Called number is either busy or has compatibility issues. Supplementary service constraints in the network may also initiate the disconnection.
22	Number Changed.	Same as Cause 1. The diagnostic field contains the new called user number. Cause 1 is used if the network doesn't support this cause value.
26	Non-Selected User Clearing.	The incoming call hasn't been assigned to the user.
27	Destination Out-of-Order.	Messages can't be sent to the destination number because the span may not be active.
28	Invalid Number Format (address incomplete).	The Type of Number (TON) is incorrect or the number is incomplete. Network unknown and National numbers have different formats.
29	Facility Rejected.	User requested supplementary service, which can't be provided by the network.
30	Response to STATUS ENQUIRY.	A `STATUS` message has been received in response to a prior `STATUS ENQUIRY`.
31	Normal, Unspecified.	A normal, unspecified disconnection has occurred.
34	No Circuit/Channel Available.	No B-Channels are available for the call.
38	Network Out-of-Order.	Network is out-of-order because due to a major malfunction.
39	Permanent Frame Mode Connection Out-of-Service.	A permanent frame mode connection is out-of-service. This cause is part of a `STATUS` message.
40	Permanent Frame Mode Connection Operational.	A permanent frame mode connection is operational. This cause is part of a `STATUS` message.
41	Temporary Failure.	Minor network malfunction. Initiate call again.
42	Switching Equipment Congestion.	High traffic has congested the switching equipment. Cause 43 is included.
43	Access Information Discarded.	Access Information elements exceed maximum length and have been discarded. Included with Cause 42.
44	Requested Circuit/Channel not Available.	The requested circuit or channel isn't available. Alternative circuits or channels aren't acceptable.
47	Resource Unavailable, Unspecified.	The resource is unavailable. No other disconnection cause applies.
49	Quality of Service Not Available.	Quality of Service, as defined in Recommendation X.213, can't be provided.
50	Requested Facility Not Subscribed.	A supplementary service has been requested that the user isn't authorized to use.

Number	Summary	Description
53	Outgoing Calls Barred Within Closed User Group (CUG).	Outgoing calls aren't permitted for this member of the CUG.
55	Incoming Calls Barred within CUG.	Incoming calls aren't permitted for this member of the CUG.
57	Bearer Capability Not Authorized.	A bearer capability has been requested that the user isn't authorized to use.
58	Bearer Capability Not Presently Available.	A bearer capability has been requested that the user isn't presently available.
62	Inconsistency in Designated Outgoing Access Information and Subscriber Class.	Outgoing Access and Subscriber Class information is inconsistent.
63	Service or Option Not Available, Unspecified.	The service or option is unavailable. No other disconnection cause applies.
65	Bearer Capability Not Implemented.	The requested bearer capability isn't supported.
66	Channel Type Not Implemented.	The requested channel type isn't supported.
69	Requested Facility Not Implemented.	The requested supplementary service isn't supported.
70	Only Restricted Digital Information Bearer Capability is Available (national use).	Unrestricted (64kb) bearer service has been requested but isn't supported by the equipment sending this cause.
79	Service or Option Not Implemented, Unspecified.	An unsupported service or unimplemented option has been requested. No other disconnection cause applies.
81	Invalid Call Reference Value.	A message has been received which contains a call reference which is currently unassigned or not in use on the user-network interface.
82	Identified Channel Doesn't Exist.	A request has been received to use a channel which is currently inactive or does not exist.
83	A Suspended Call Exists, but This Call Identity Doesn't Exist.	A `RESUME` message cannot be executed by the network as a result of an unknown call identity.
84	Call Identity in Use.	A `SUSPEND` message has been received with a call identity sequence that is already in use.
85	No Call Suspended.	A `RESUME` message can't be executed by the network as a result of no call suspended.

Number	Summary	Description
86	Call Having the Requested Call Identity Has Been Cleared.	A `RESUME` message can't be executed by the network as a result of the call having been cleared while suspended.
87	User Not Member of CUG.	A CUG member was called by a user who isn't a member of the CUG or a CUG call was made to a non-CUG member.
88	Incompatible Destination.	User-to-user compatibility checking procedures in a point-to-point data link have determined that an incompatibility exists between Bearer capabilities.
90	Non-Existent CUG.	CUG doesn't exist.
91	Invalid Transit Network Selection (national use).	The transit network selection is of an incorrect format. No route (transit network) exists between the two networks.
95	Invalid Message, Unspecified.	Invalid message received. No other disconnection cause applies.
96	Mandatory Information Element is Missing.	A message was received with an information element missing.
97	Message Type Non-Existent or Not Implemented.	A message was received that is of a type that isn't defined or of a type that is defined but not implemented.
98	Message is Not Compatible with the Call State, or the Message Type is Non-Existent or Not Implemented.	An unexpected message or unrecognized message incompatible with the call state has been received
99	An Information Element or Parameter Doesn't Exist or is Not Implemented.	A message was received containing elements or parameters that aren't defined or of a type that is defined but not implemented.
100	Invalid Information Element Contents.	A message other than `SETUP`, `DISCONNECT`, `RELEASE`, or `RELEASE COMPLETE` has been received which has one or more mandatory information elements containing invalid content.
101	The Message is Not Compatible with the Call State.	A `STATUS` message indicating any call state except the Null state has been received while in the Null state.
102	Recovery on Timer Expired.	An error handling procedure timer has expired.
103	Parameter Non-Existent or Not Implemented - Passed On (national use).	A message was received containing parameters that aren't defined or of a type that is defined but not implemented.
110	Message with Unrecognized Parameter Discarded.	A message was discarded because it contained a parameter that wasn't recognized.

Number	Summary	Description
111	Protocol Error, Unspecified.	A protocol error has occurred. No other disconnection cause applies.
127	Interworking, Unspecified.	An interworking call has ended.

Disconnection Cause Values

The following table lists the disconnection cause values.

Disconnection Cause Values

Value	Call Disconnection Cause
0	Unknown.
1	Participant hung up.
2	Disconnected by User.
5	Resources deficiency.
6	Password failure.
20	H323 call close. No port left for audio.
21	H323 call close. No port left for video.
22	H323 call close. No port left for FECC.
23	H323 call close. No control port left.
25	H323 call close. No port left for video content.
51	A common key exchange algorithm couldn't be established between the MCU and the remote device.
53	Remote device didn't open the encryption signaling channel.
59	The remote devices' selected encryption algorithm doesn't match the local selected encryption algorithm.
141	Called party not registered.
145	Caller not registered.
152	H323 call close. ARQ timeout.
153	H323 call close. DRQ timeout.
154	H323 call close. Alt Gatekeeper failure.
191	H323 call close. Remote busy.
192	H323 call close. Normal.

Value	Call Disconnection Cause
193	H323 call close. Remote reject.
194	H323 call close. Remote unreachable.
195	H323 call close. Unknown reason.
198	H323 call close. Small bandwidth.
199	H323 call close. Gatekeeper failure.
200	H323 call close. Gatekeeper reject ARQ.
201	H323 call close. No port left.
202	H323 call close. Gatekeeper DRQ.
203	H323 call close. No destination IP value.
204	H323 call close. Remote hasn't sent capability.
205	H323 call close. Audio channels not open.
207	H323 call close. Bad remote cap.
208	H323 call close. Capabilities not accepted by remote.
209	H323 failure.
210	H323 call close. Remote stop responding.
213	H323 call close. Primary secondary problem.
251	SIP timer popped out.
252	SIP card rejected channels.
253	SIP capabilities don't match.
254	SIP remote closed call.
255	SIP remote canceled call.
256	SIP bad status.
257	SIP remote stopped responding.
258	SIP remote unreachable.
259	SIP transport error.
260	SIP bad name.
261	SIP trans error TCP invite.
300	SIP redirection 300.

Value	Call Disconnection Cause
301	SIP moved permanently.
302	SIP moved temporarily.
305	SIP redirection 305.
380	SIP redirection 380.
400	SIP client error 400.
401	SIP unauthorized.
402	SIP client error 402.
403	SIP forbidden.
404	SIP not found.
405	SIP client error 405.
406	SIP client error 406.
407	SIP client error 407.
408	SIP request timeout.
409	SIP client error 409.
410	SIP gone.
411	SIP client error 411.
413	SIP client error 413.
414	SIP client error 414.
415	SIP unsupported media type.
420	SIP client error 420.
480	SIP temporarily not available.
481	SIP client error 481.
482	SIP client error 482.
483	SIP client error 483.
484	SIP client error 484.
485	SIP client error 485.
486	SIP busy here.
487	SIP request terminated.

Value	Call Disconnection Cause
488	SIP client error 488.
500	SIP server error 500.
501	SIP server error 501.
502	SIP server error 502.
503	SIP server error 503.
504	SIP server error 504.
505	SIP server error 505.
600	SIP busy everywhere.
603	SIP global failure 603.
604	SIP global failure 604.
606	SIP global failure 606.

Event Auditor

Topics:

The Event Auditor enables administrators and auditors to analyze configuration changes and unusual or malicious activities in the RealPresence Collaboration Server system.

The Event Auditor operates in real time, recording all administration activities and login attempts from the following RealPresence Collaboration Server modules:

- Control Unit
- Shelf Manager

The Event Auditor must always be active in the system. A System Alert is displayed if it becomes inactive for any reason.

The Event Auditor tool is comprised of the Auditor Files and an Auditor File Viewer to view them.

Note: Time stamps of Audit Events are GMT.

Related Links

User Roles (Authorization Levels) and Permissions on page 257

Auditor Files

All audit events are saved to a buffer file on hard disk in real time and then written to a file on hard disk in XML in an uncompressed format.

A new current auditor event file is created when:

- The system is started.
- The size of the current auditor event file exceeds 2 MB.
- The current auditor event file's age exceeds 24 hours.

Up to 1000 auditor event files are stored per RealPresence Collaboration Server. These files are retained for at least one year and require 1.05 GB of disk space. The files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000.

A System Alert is displayed with Can't store data displayed in its Description field if:

- The system cannot store 1000 files.
- The RealPresence Collaboration Server does not have available disk space to retain files for one year.

Audit Event Files are retained by the RealPresence Collaboration Server for at least 1 year. Any attempt to delete an audit event file that is less than one year old raises a System Alert with File was removed listed in the Description field.

Using the Restore Factory Defaults of the System Restore procedure erases Audit Files.

Retrieving Auditor Files

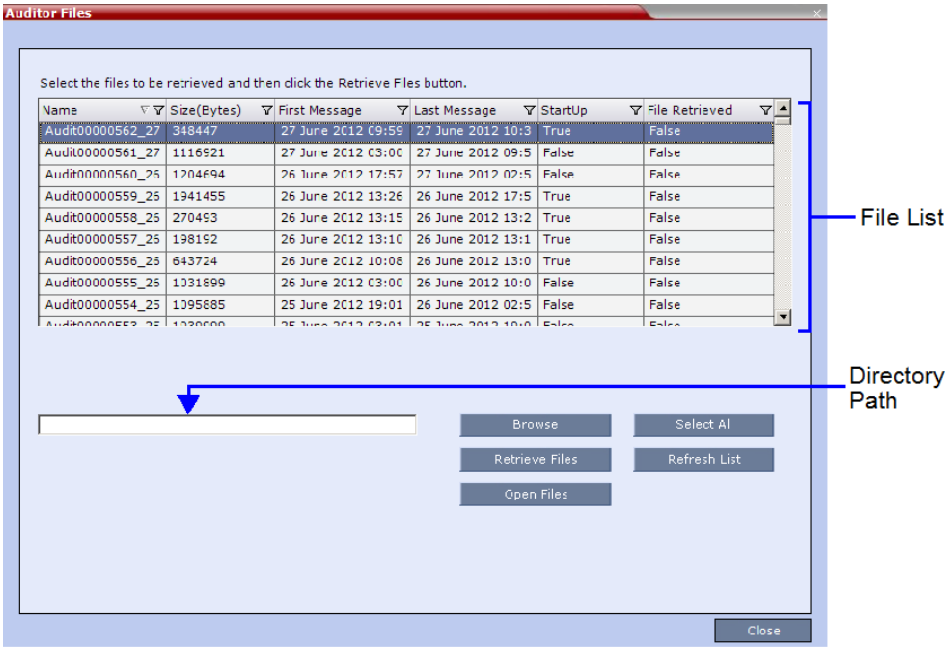
You can open the Auditor file directly from the Auditor Files list or you can retrieve the files and save them to a local workstation.

Retrieve Auditor Files in RMX Manager

You can open the **Auditor File Viewer** in RMX Manger.

Procedure

» In RMX Manager, go to **Administration** > **Tools** > **Auditor Files**.



The **Auditor Files** dialog displays a file list containing the following file information:

- Name
- Size (Bytes)
- First Message - Date and time of the first audit event in the file
- Last Message - Date and time of the last audit event in the file
- Startup:
  - True - File was created when the system was started
  - False - File was created when previous audit event file reached a size of 2 MB or was more than 24 hours old
- File Retrieved:
  - True - File was previously retrieved.
  - False - File was never previously retrieved.

The order of the **Auditor Files** dialog box field header columns can be changed and the fields can be filtered to enable searching.

Retrieve an Auditor File Stored on the Workstation

You can open a locally stored auditor file on your workstation.

Procedure

1. Click **Browse** to select the location on the workstation in which to store the files, and click **OK**.

   The folder name is displayed in the directory path field.
2. Select the file(s) to be retrieved, or click **Select All** to retrieve all the files. (Windows multiple selection techniques can be used.)
3. Click Retrieve Files.

   The selected files are copied to the selected directory on the workstation.

Viewing Auditor Files

The **Auditor File Viewer** enables auditors and administrators to view the content of and perform detailed analysis on auditor event data in a selected auditor event file.

You can view an auditor event file directly from the **Auditor Files** list or by opening the file from the **Auditor File Viewer**.

Open the Auditor File Viewer in RMX Manager

You can open the **Auditor File Viewer** in RMX Manger.

Procedure

1. In RMX Manager, go to **Administration** > **Tools** > **Auditor File Viewer**.

   If you previously double-clicked an auditor event file in the **Auditor Files** list, that file is automatically opened.

   The following fields are displayed for each event:

   Auditor Event Columns

Field	Description
Event ID	The sequence number of the event generated by the RealPresence Collaboration Server.
Date & Time	The date and time of the event taken from the RealPresence Collaboration Server's Local Time setting.
User Name	The **Username** (Login Name) of the user who triggered the event.

Field	Description
Reporting Module	The RealPresence Collaboration Server system internal module that reported the event: • MCMS • MPL • Central Signaling • MPL Simulation • RealPresence Collaboration Server Web Client • CM Switch • Shelf Management • ART • Video • Card Manager • RTM • MUX
Workstation	The name (alias) of the workstation used to send the request that triggered the event.
IP Address (Workstation)	The IP address of the workstation used to send the request that triggered the event.
Event Type	Auditor events can be triggered by: • API • HTTP • RealPresence Collaboration Server Internal Event
Event	The process, action, request or transaction that was performed or rejected. • POST:SET transactions (API) • Configuration changes via XML (API) • Login/Logout (API) • GET (HTTP) • PUT (HTTP) • MKDIR (HTTP) • RMDIR (HTTP) • Startup (RealPresence Collaboration Server Internal Event) • Shutdown (RealPresence Collaboration Server Internal Event) • Reset (RealPresence Collaboration Server Internal Event) • Enter Diagnostic Mode (RealPresence Collaboration Server Internal Event) • IP address changes via USB (RealPresence Collaboration Server Internal Event)

Field	Description
Process Completed	Status of the process, action, request or transaction returned by the system: • Yes - performed by the system. • No - rejected by the system.
Description	A text string describing the process, action, request or transaction.
Additional Information	An optional text string describing the process, action, request or transaction in additional detail.

The order of the **Auditor File Viewer** field header columns can be changed and the fields can be sorted and filtered to facilitate different analysis methods.

2. In the event list, click the events or use the keyboard's Up and Down arrow keys to display the **Request Transaction** and **Response Transaction** XML trees for each audit event.

   The transaction XML trees can be expanded and collapsed by clicking **Expand** and **Collapse** .

Open an Auditor Event File Stored on the Workstation

You can open a locally stored auditor event file on your workstation.

Procedure

1. Click **Local File** .
2. Go to the location of the audit event file and select it.
3. Click **Open**.

Audit Events

All audit events are stored in a buffer file on hard disk and then written to a file in XML in an uncompressed format.

Alerts and Faults

The following alerts and faults are recorded by the auditor:

Alerts and Faults recorded by the Auditor

Event
Attempt to exceed the maximum number of management session per user
Attempt to exceed the maximum number of management sessions per system
Central Signaling indicating Recovery status.
Failed login attempt
Failed to open Apache server configuration file.

Event
Failed to save Apache server configuration file.
Fallback version is being used.
File system scan failure.
File system space shortage.
Internal MCU reset.
Internal System configuration during startup.
Invalid date and time.
Invalid MCU Version.
IP addresses of Signaling Host and Control Unit are the same.
IP Network Service configuration modified.
IP Network Service deleted.
Login
Logout
Management Session Time Out
MCU Reset to enable Diagnostics mode.
MCU reset.
Music file error.
New activation key was loaded.
New version was installed.
NTP synchronization failure.
Polycom default User exists.
Private version is loaded.
Restoring Factory Defaults.
Secured SIP communication failed.
Session disconnected without logout
SSH is enabled.
System Configuration modified.
System is starting.

Event
System Resets.
TCP disconnection
Terminal initiated MCU reset.
The Log file system is disabled.
The software contains patch(es).
USB key used to change system configuration.
User closed the browser
User initiated MCU reset.

Transactions

The following transactions are recorded by the auditor:

Transactions recorded by the Auditor

Transaction
`TRANS_CFG:SET_CFG`
`TRANS_IP_SERVICE:DEL_IP_SERVICE`
`TRANS_IP_SERVICE:NEW_IP_SERVICE`
`TRANS_IP_SERVICE:SET_DEFAULT_H323_SERVICE`
`TRANS_IP_SERVICE:SET_DEFAULT_SIP_SERVICE`
`TRANS_IP_SERVICE:UPDATE_IP_SERVICE`
`TRANS_IP_SERVICE:UPDATE_MANAGEMENT_NETWORK`
`TRANS_ISDN_PHONE:ADD_ISDN_PHONE`
`TRANS_ISDN_PHONE:DEL_ISDN_PHONE`

Transaction
TRANS_ISDN_PHONE:UPDATE_ISDN_PHONE
TRANS_ISDN_SERVICE:DEL_ISDN_SERVICE
TRANS_ISDN_SERVICE:NEW_ISDN_SERVICE
TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE
TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE
TRANS_MCU:BEGIN_RECEIVING_VERSION
TRANS_MCU:COLLECT_INFO
TRANS_MCU:CREATE_DIRECTORY
TRANS_MCU:FINISHED_TRANSFER_VERSION
TRANS_MCU:LOGIN
TRANS_MCU:LOGOUT
TRANS_MCU:REMOVE_DIRECTORY
TRANS_MCU:REMOVE_DIRECTORY_CONTENT
TRANS_MCU:RENAME
TRANS_MCU:RESET
TRANS_MCU:SET_PORT_CONFIGURATION
TRANS_MCU:SET_RESTORE_TYPE

Transaction
TRANS_MCU:SET_TIME
TRANS_MCU:TURN_SSH
TRANS_MCU:UPDATE_KEY_CODE
TRANS_OPERATOR:CHANGE_PASSWORD
TRANS_OPERATOR:DELETE_OPERATOR
TRANS_OPERATOR:NEW_OPERATOR
TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN
TRANS_SNMP:UPDATE

Log Management

Topics:

You can determine information about logging levels and obtain the log files from RealPresence Collaboration Server.

Retrieve Logger Diagnostic Files

The Logger utility is a troubleshooting tool that continually records MCU system messages and saves them to files in the MCU hard drive.

For each time interval defined in the system, a different data file is created. The files may be retrieved from the hard drive for off-line analysis and debugging purposes.

The Logger utility is activated at the MCU startup. The Logger is disabled when the MCU is reset manually or when there is a problem with the Logger utility, e.g. errors on the hard drive where files are saved. In such cases, data cannot be retrieved.

When the MCU is reset via the RealPresence Collaboration Server, the files are saved on the MCU hard drive.

When retrieved, the log file name structure is as follows:

- Sequence number (starting with 1)
- Date and Time of first message
- Date and Time of last message
- File size
- Special information about the data, such as Startup

File name structure:

```
Log_SNxxxxxxxxxx_FMDddmmyyy_FMThhmm_LMDddmmyyyy_LMThhmm_SZxxxxxxxxxx_SUY.lo
g
```

File name format:

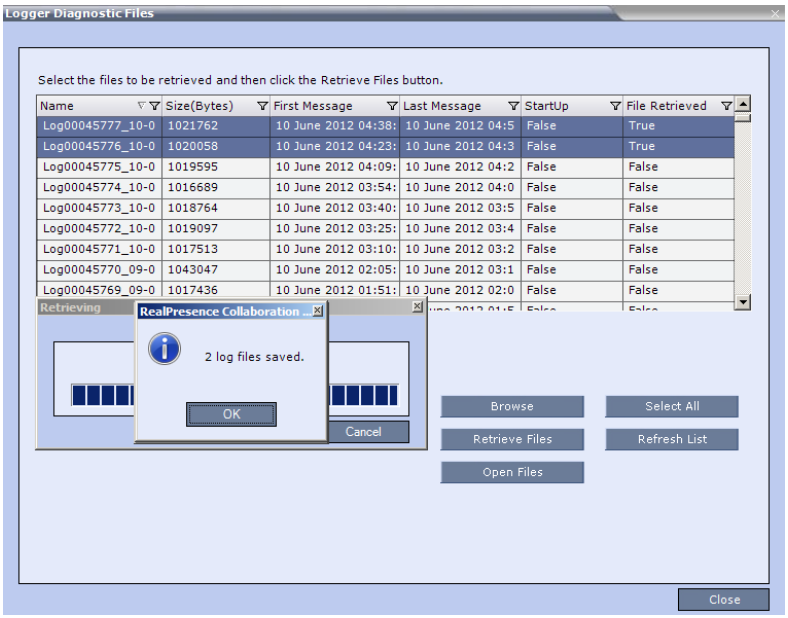
- SN = Sequence Number
- FM = First Message, date and time
- LM = Last Message, date and time
- SZ = Size
- SU = Startup (Y/N) during the log file duration

Example:

```
Log_SN0000000002_FMD06032007_FMT083933_LMD06032007_LMT084356_SZ184951_SUY.log
```

Procedure

1. In RMX Manager, go to **Administration** > **Tools** > **Logger Diagnostic Files**.
2. Select the log files to retrieve. Multiple selections of files are enabled using standard Windows conventions.
3. In the **Logger Diagnostic Files** dialog, click **Browse** to select the directory location from which to retrieve the Logger files, and click **OK**.
4. In the **Logger Diagnostic Files** dialog, click **Retrieve Files**, and once complete, click **OK**.



The log files (in *.txt format) are saved to the defined directory and a confirmation caption box is displayed indicating a successful retrieval of the log files.

5. To analyze the log files generated by the system, using Windows Explorer, browse to the directory containing the retrieved log files and use any text editor to open the retrieved *.txt files.

Collect Comprehensive System Logs

You can collect comprehensive system logs using the Information Collector.

The Information Collector attains all information from all the MCU internal entities for data analysis. The system logs the data from the following system components and stores it in a central repository.

- System log files
- CDR
- OS (core dumps, CFG - DNS, DHCP, NTP, kernal state, event logs)
- Signaling trace files (H.323 and SIP)
- Central signaling logs

- Processes internal state and statistics
- Full faults
- Apache logs
- CFG directory (without IVR)
- Cards info: hardware version, state, and status
- Software version number

Procedure

1. In RMX Manager, go to **Administration** > **Tools** > **Information Collector**.
2. In the **From Date** and **Until Date** fields, use the arrow keys to define the date range of the data files to be included in the compressed file.
3. In the **From Time** and **Until Time** fields, use the arrow keys to define the time range of the data files to be included in the compressed file.

   Note: If logs are collected to troubleshoot a specific issue, it is important to set the date and time range to include the time and date in which the issue occurred, since the default date and time ranges may be insufficient to allow for a full understanding of the problem.

   For example, if a specific issue occurred on October 1, 2018 at 12:15, the **From Date** and **Until Date** should be October 1, 2018, the **From Time** should be around 12:10, and the **Until Time** should be around 12:20.

4. Select the check boxes of the information you want to collect.
5. Browse to the directory path where you want to save the compressed file.
6. Click **Collect Information**.

   A progress indicator displays in the **Information Collector** dialog while the file is created.

   The system saves compressed file to the directory you selected in the **Information Collector** dialog. The file is named `info.tgz`.

   Note: Some browsers save the file as `info.gz` due to a browser bug. If this occurs, the file must be manually renamed to `info.tgz` before it can be viewed.

7. Click **OK**.

Forward Audit Logs to a Syslog Server

You can use RMX Manager to configure the MCU to forward audit logs, which document all administrative actions, to a syslog server.

Procedure

1. In RMX Manager, go to **Administration** > **Tools** > **Syslog Configuration** > **RMX - Syslog Configuration**.
2. In the **Configuration** tab, select the **Enable Syslog server** check box
3. Enter the **Server IP** address and **Transport Type** (UDP, TCP, or TLS).
4. Click **OK**.
5. Reset the RealPresence Collaboration Server.

Network Intrusion Detection System (NIDS)

The RealPresence Collaboration Server system uses iptables for access control.

For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the RealPresence Collaboration Server must pass the rules applicable to it.

Depending on the nature of the suspect packets, the rules may reject, drop, or limit their arrival rate (dropping the rest).

The RealPresence Collaboration Server maintains a log that includes all non-permitted access attempts blocked by the fire wall.

Unpermitted access includes:

- Access to ports which are not opened on the RealPresence Collaboration Server.
- Invalid access to open ports.

A Homologation for Brazil

Topics:

The following information describes how the RealPresence Collaboration Server meets homologation requirements for import into Brazil.

Add Required H.323 and SIP Protocol Flags

To adhere to homologation requirements for Brazil, configure the required H.323/SIP protocol settings by adding RealPresence Collaboration Server system flags.

Note: If these flags already exist in your RealPresence Collaboration Server environment, verify that they use the required values for homologation for Brazil.

Procedure

1. In RMX Manager, go to **Setup** > **System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, add the following flag and value:

   Flag Name: `DISABLE_DUMMY_REGISTRATION` **Value:** `YES` (enabled)
3. In the **CS_MODULE_PARAMETERS** tab, add the following flags and values:

   Flag Name: `SIP_TIMERS_SET_INDEX` **Value:** `1` (standard SIP)

   Flag Name: `H323_TIMERS_SET_INDEX` **Value:** `1` (standard H.323)
4. Click **Close**.