ADMINISTRATION GUIDE

8.8 | December 2018 | 3725-74900-000B1

RealPresence® Collaboration Server

1800/2000/4000/Virtual Edition

6001 America Center Drive
San Jose, CA 95002
USA

Contents

Before You Begin

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

Privacy

Privacy-related options

Option name in UI	Available settings	Location in the system
Manage call detail records (CDR)	Yes - multiple	See the Call Detail Records section in this guide.
Manage user credentials	Yes - multiple	See the User Management and User Management Flags sections in this guide.
Manage address book	Yes - multiple	See the Address Book section in this guide.
Manage data backups	Yes - multiple	See the Address Book , Enabling a CDR Backup Alarm , and Cyclic File System Flag sections in this guide.
Manage audit and log files	Auto	Audit and log files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000. Also see the Cyclic File System Flag section in this guide.

How Data Subject Rights are supported

Data Subject Right	Method of support
Right to be informed	**What customer personal data is collected?** See the Purposes for processing personal data table in this topic. **How is customer personal data is used?** See the Purposes for processing personal data table in this topic. **How long is customer personal data kept?** Any personal data made available when working with Polycom support is only retained until each specific issue is resolved and then it is purged. **Is customer personal data shared with any third parties and if so, who?** If personal data is made available when working with Polycom support, this data may be shared with contracted third-party engineering companies. **How can a data subject be notified of a data breach?** Data Subjects have a right to be notified when their data has been processed without authorization. The product administrator is able to monitor and identify when security anomalies have occurred. See the How admin can be informed of any security anomalies (including data breach) table in this topic.
Right to access (view and/or obtain a copy of all personal data for a specific data subject)	Personal data about specific participants in conferences can be viewed or downloaded via the CDR. See the Retrieve and Save a CDR for Viewing section in this guide. Personal data related to users who are Administrators, Operators and Auditors can be viewed using RMX Manager or RealPresence Resource Manager (if configured). See the User Management section in this guide.
Right to rectification (make corrections to inaccurate or incomplete personal data)	Personal data about specific participants in conferences cannot be edited or updated because the information derives from the device of origin. Personal data related to users who are Administrators, Operators and Auditors can be edited or updated using RMX Manager or RealPresence Resource Manager (if configured). See the User Management section in this guide. Polycom does not manipulate data made available during the support process, so any rectification of inaccuracies of personal data must be performed by customer directly.
Right to erasure (remove all personal data)	For details on how to erase customer personal data from the system, see the How customer personal data is deleted table in this topic. Any customer personal data made available when working with Polycom support will be erased by requesting erasure through your Polycom support representative.
Right to restrict processing (temporarily cease all processing of personal data)	Not applicable.

Data Subject Right	Method of support
Right to data portability (receive a copy of all personal data in a commonly used, machine-readable format)	CDRs can be downloaded in XML format to a USB device. See the Retrieve and Save a CDR for Viewing section in this guide. The Address Book can be exported in XML format. See the Exporting an Address Book section in this guide. Audit and log files can be downloaded in plain text format.See the Retrieve Logger Diagnostic Files section of this guide.
Right to object to processing (permanently stop all processing of personal data)	Not applicable.

Purposes for processing personal data

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
Call detail records (CDR)	All of the following for both near and far endpoints: • Name • Status • Role • IP Address/Phone • Alias Name/SIP Address • Lync/Skype user name	• Maintaining call history • Troubleshooting call errors or performance issues	• RMX Manager • RealPresence Resource Manager (if configured) • Download to USB • API Use the TRANS_CDR_LIST and TRANS_CDR_FULL APIs to retrieve CDRs. All RMX APIs are available at Polycom Support page. See the RMX API SDK for your version of the product.
User credentials	All of the following: • User name • Password • Authorization level	Login and authentication	• RMX Manager • RealPresence Resource Manager (if configured)

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
Address book	All of the following: • Name • Endpoint website • IP Address (H.323 and SIP) • Alias Name/Type (H.323 Only) • SIP Address • Endpoint Website IP Address (IP Only)	• Ease of use for dialing participant • Store frequently used information	• RMX Manager • RealPresence Resource Manager (if configured)
Audit and log files	• Admin and User credentials (excluding passwords) • All CDR details • Admin and User actions	• Admin and user activity logging • Maintain history of configuration changes • Troubleshooting system issues	• RMX Manager • RealPresence Resource Manager (if configured) • Download to USB • API APIs are used to retrieve audit and log files. Use TRANS_AUDIT_FILE_SUMMARY_LIST API for audit files and TRANS_LOG_FILE_LIST for log files. All RMX APIs are available at Polycom Support page. See the RMX API SDK for your version of the product.S

How admin can be informed of any security anomalies (including data breach)

Security anomaly type	Where to check	Recommended frequency to check
All active alarms	See the Active Alarms , Hardware Monitoring and System Flags sections in this guide.	The alarms are checked every 3 sec. If there is new alarm, the alarm list is updated with new list of alarms. Recommend log review once daily

How customer personal data is deleted

Data type	Steps to delete	Deletion method
Call detail record (CDR)	By default, CDRs are overwritten by new CDRs periodically. If required, CDR can be deleted through the command line interface (ssh) CDRs can also be deleted by performing a standard or comprehensive restore operation. See the Restore RealPresence Collaboration Server Defaults section in this guide.	To do this: **1** Enable SSH **2** Go to > /opt/mcu/output/cdr **3** rm -f * cdr Standard restore – simple delete Comprehensive restore – System hard disk file partition is formatted
User credentials	See the Delete a User section in this guide.	Simple delete
Address book	See the Deleting a Participant from the Address Book section in this guide. The Address Book is also deleted by performing a standard or comprehensive restore operation. See the Restore RealPresence Collaboration Server Defaults section in this guide.	If using the RMX Manager – simple delete Standard restore – simple delete Comprehensive restore – System hard disk file partition is formatted
Data backups	Backup are stored in Local system. Back up files can be deleted from local Windows / Linux system. The local system is the machine where the backup file is stored using RMX Manager.	Delete the backup file from specific path on the local system.
Audit and log files	Audit and log files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000. Audit and log files are also deleted by performing a standard or comprehensive restore operation. See the Restore RealPresence Collaboration Server Defaults section in this guide.	To do this: **1** Enable SSH **2** Go to > opt/mcu/mcms/Logfiles **3** Select the module > cd Logger **4** rm -f * (or the file name) Standard restore – simple delete Comprehensive restore – System hard disk file partition is formatted

Getting Help

For more information about installing, configuring, and administering Polycom products, see the Polycom Document Library.

Polycom and Partner Resources

See the following Polycom documentation for related information on this product:

- *Polycom® RealPresence® Collaboration Server Release Notes*
- Polycom® RealPresence® Collaboration Server 1800/2000/4000/Virtual Edition Getting Started Guide
- *Polycom® RealPresence® Collaboration Server Hardware Guide* for the associated appliance edition

- *Polycom® RealPresence® Collaboration Server 1800/2000/4000 Deployment Guide for Maximum Security Environments*

See the Polycom Document Library to learn more about the following RealPresence Platform products:

- Polycom® RealPresence® DMA® 7000
- Polycom® RealPresence® Resource Manager
- Polycom® RealPresence® Web Suite
- Polycom® RealPresence® Media Suite
- Polycom® RealPresence® Access Director™
- Polycom® RealPresence® Group Series

The Polycom Community

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

Product Overview

The 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.

Product Features

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

Supported Features for Conferencing

Feature Name	Description
Polycom Open Collaboration Network	The Polycom Open Collaboration Network (POCN) enables Polycom, Microsoft, and Cisco users, within their own environment, to participate in the same conference running on a RealPresence Collaboration Server. The RealPresence Collaboration Server also natively interoperates with Cisco Telepresence Systems and Polycom 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 RealPresence Collaboration Server can merge multiple conferences into a single conference. This enables 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.
Content Sharing	The 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 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 RealPresence Collaboration Server supports H.264 High Profile with video preview.

Supported Features for Conferencing (continued)

Feature Name	Description
Indicators	The 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 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.
NoiseBlock™	The RealPresence Collaboration Server automatically detects and mutes AVC endpoints that have a noisy audio channel.

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

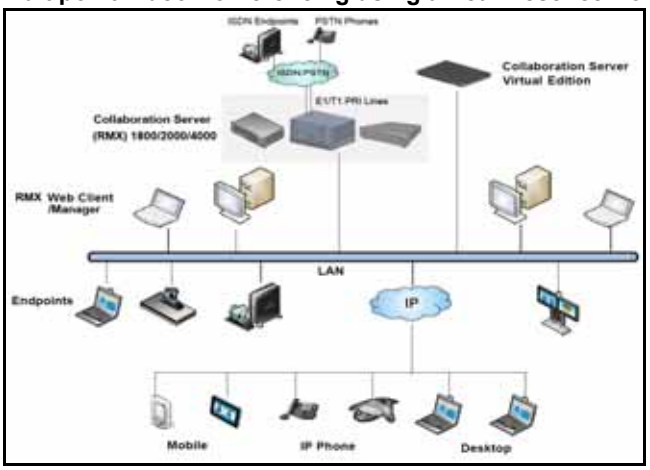
To enable ISDN-video and ISDN-voice participants to connect to the MCU, you must define an ISDN (audio/video) Network Service. You can define only two ISDN (audio/video) Network Services, of the same Span Type (E1 or T1). Each Network Service can attach spans from either or both cards.

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

The RealPresence Collaboration Server 1800 with three DSP cards supports ISDN (Audio/Video) networks. The RealPresence Collaboration Server 2000 and 4000 also support ISDN (Audio/Video) networks. For more information on ISDN (Audio/Video) support, see Defining ISDN (audio/video) Network Services.

Multipoint Conferencing Network

Multipoint Video Conferencing using a RealPresence Collaboration Server



Required Software Components

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 a user's capabilities within the system. The RealPresence Collaboration Server supports the following user authorization levels:

- Administrator
- Operator
- Administrator Read-only
- Chairperson
- Auditor

Note that conference participants are not considered "users" of the RealPresence Collaboration Server as they never access the MCU user interface. However, conference participant information can be stored in the RealPresence Collaboration Server Address Book for scheduling and management purposes.

Machine Accounts

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies, but these are not considered a user type. For more details, see Defining a Machine Account.

Administrator

A RealPresence Collaboration Server system administrator can define and delete other users and perform all system configuration and maintenance tasks.

The RealPresence Collaboration Server, by default, ships with a single pre-defined administrator account which provides initial system access. This administrator account is:

- User name: SA_PLCM_Integration
- Password: Polycom_CS

Upon initial login, the RealPresence Collaboration Server displays an active alarm indicating the existence of this SA_PLCM_Integration default user.

The RealPresence® Distributed Media Application™ (DMA®) is configured to recognize this default administrator account as well, thus allowing the RealPresence DMA system to log into the RealPresence Collaboration Server. However, for security reasons, Polycom strongly recommends immediately setting up a new administrator account on both the RealPresence Collaboration Server and the RealPresence DMA system and deleting the default administrator account.

Administrator Read-only

A user with Administrator Read-only permissions has the same viewing and monitoring permissions of an administrator. However, this user is limited to creating system backups and cannot perform any other configuration or conference related operation.

Operator

An Operator can manage Meeting Rooms, Profiles, Entry Queues, and SIP Factories, and can also view the Collaboration Server configurations, but cannot change them.

Administrator and Operator users can verify which users are defined in the system. Neither of them can view the user passwords, but an Administrator can change a password.

Chairperson

A Chairperson can only manage ongoing conferences and participants, in both single and cascading RealPresence Collaboration Server scenarios. The Chairperson does not have access to the Collaboration Server configurations and utilities.

Auditor

An **Auditor** can only view Auditor Files and audit the system.

User Interface Availability Based on User Type

The following table identifies which user interface panes, features, and functions are available to which type of RMX system user.

	Admin				Chairperson				Operator			
Tab Name	**CP**	**SVC**	**Mixed**	**VSW**	**CP**	**SVC**	**Mixed**	**VSW**	**CP**	**SVC**	**Mixed**	**VSW**
General	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gathering Settings	✓	×	×	✓	✓	×	×	✓	✓	×	×	✓
Video Quality	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Video Settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audio Settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Customized Polling	✓	×	×	✓	×	×	×	×	✓	×	×	✓
Skins	✓	×	✓	×	✓	×	✓	×	✓	×	✓	×
IVR	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recording	✓	×	✓	✓	✓	×	✓	✓	✓	×	✓	✓

Tab Name	Admin				Chairperson				Operator			
	CP	SVC	Mixed	VSW	CP	SVC	Mixed	VSW	CP	SVC	Mixed	VSW
Site Names	✓	×	✓	×	✓	×	✓	×	✓	×	✓	×
Message Overlay	✓	×	×	×	✓	×	×	×	✓	×	×	×
Network Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Navigating the System

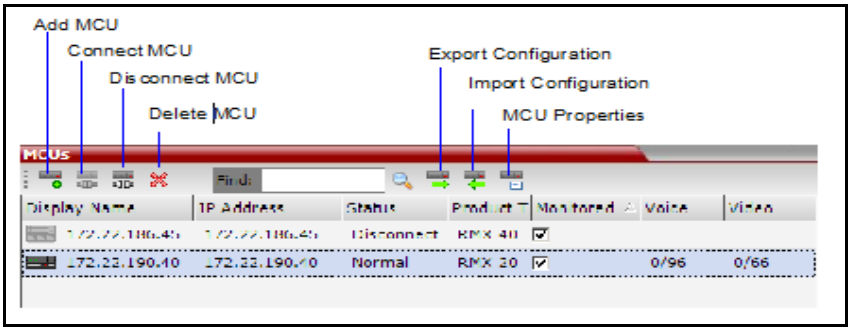
The RealPresence Collaboration Server can be managed and monitored with either the RMX Manager application on a Windows-based system or the RMX Web Client using Internet Explorer. In general, the tasks documented in this guide apply to both RMX Manager and the RMX Web Client, but we document them from the RMX Manager interface.

The RMX Manager main screen is displayed when it is connected to at least one RealPresence Collaboration Server. The RMX Manager main screen and the RMX Web Client main screen are similar except RMX Manager includes an MCU pane, as it can manage multiple MCUs. RMX Manager displays the RealPresence Collaboration Server functions based on the authorization level of the logged in user.

The MCU pane is available to all users. Only one RealPresence Collaboration Server can be selected in the MCU pane. The menu items, RMX management, address book, conference templates, and all properties that are applicable to the selected MCU are available.

The MCU Pane

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



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

MCU Menu	Description
MCU Display Name	The name of the RealPresence Collaboration Server and its icon according to its type and connection status.
IP Address	The IP address of the 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 RealPresence Collaboration Server type: **RMX 1800/2000/4000/800VE**. Before connecting to the MCU for the first time, the RealPresence Collaboration Server type is unknown and so **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

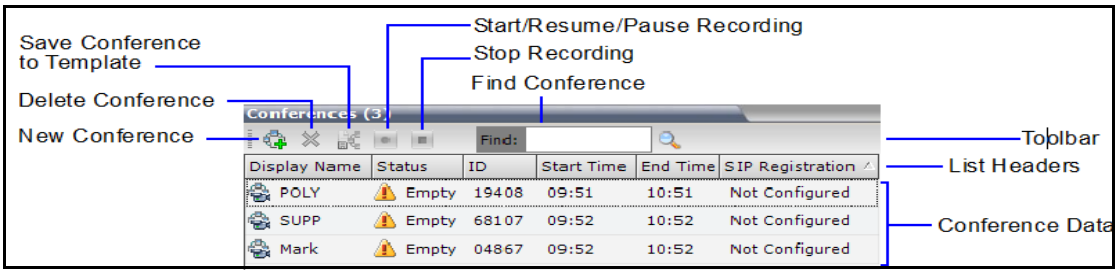
The MCU icons and states are as follows:

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

If you are 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

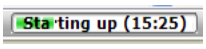
The Status Bar is available to operators and administrators to display the system alerts, participant alerts, port usage gauges, and MCU state indicator. The information included in the status bar varies with the product model.

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

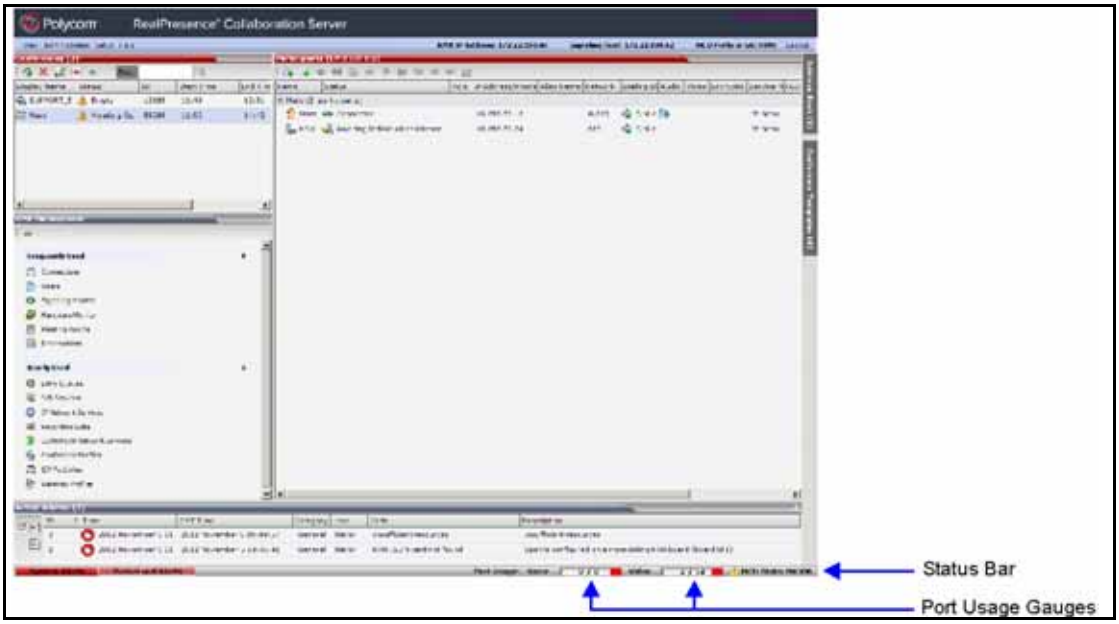
Option	Description
	The MCU is starting up. The time remaining until the system start-up is complete. The Time remaining is displayed within parentheses. The blue progress indicator bar indicates the start-up progress. 

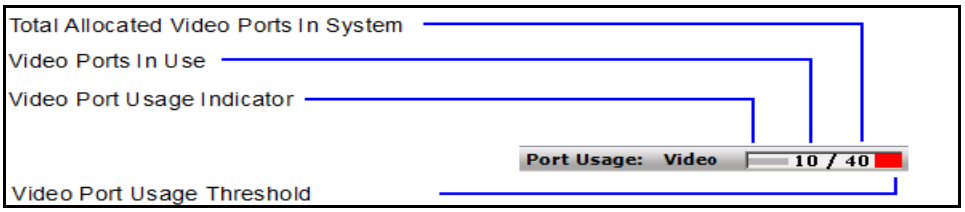
MCU State Indicator (continued)

Option	Description
MCU State: NORMAL	The MCU is functioning normally.
MCU State: MAJOR	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 RealPresence Collaboration Server 1800/2000/4000, the Port Usage Gauge displays:

- 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 RealPresence Collaboration Server, Virtual Edition, the Port Usage Gauge displays:

- 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.

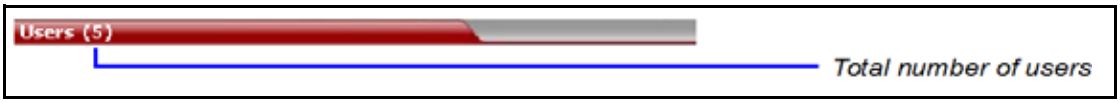
List Pane

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.

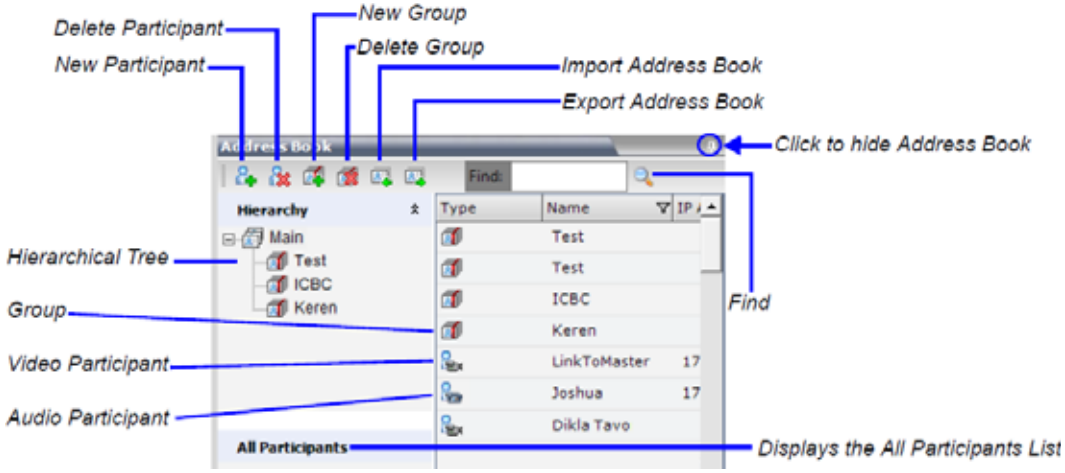
Selecting an item in the RMX Management pane lists the items currently defined.

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)
Dialing Direction	**Dial-in** – The participant dials in to the conference. **Dial-out** – The 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 is 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 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.

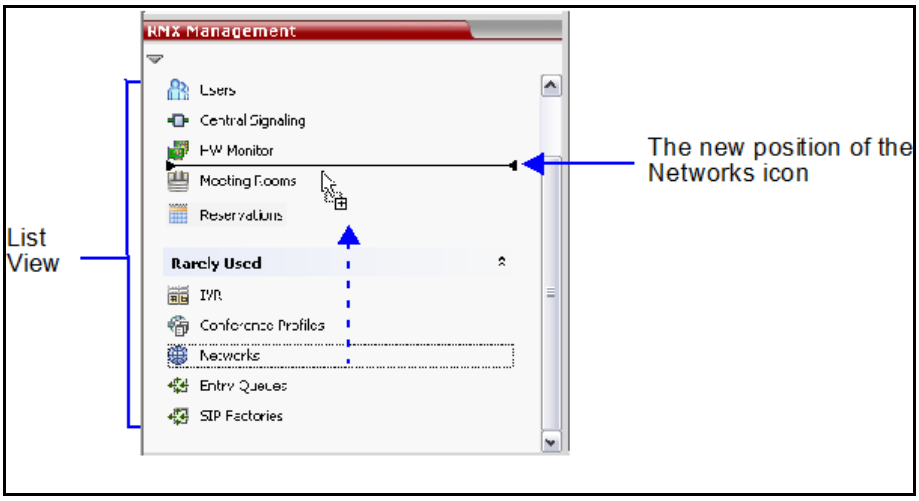
You can toggle between toolbar and list views in the RMX Management pane, and you can move items between these two sections to customize the management tasks per system user.

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 does not work in toolbar view as all items are represented by icons.

Frequently Used and Rarely Used Sections

You can expand or collapse items between the frequently used and rarely used sections. You can also move the items within and between the frequently used and rarely used sections by dragging icons of the item to the appropriate position.

An indicator line (▸——◂) appears indicating the new position of the icon.



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.

Toolbar Buttons

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 the Conference Template(s) 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. For more information see Scheduling Conferences Using the Reservation Calendar.

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.

Getting Started

This section describes the tasks that you may need to complete (based on your system design and installation) to configure the Polycom RealPresence Collaboration Server after first-time setup.

Install RMX Manager

The RealPresence Collaboration Server can be managed and monitored with either the RMX Manager application on a Windows-based system or the RMX Web Client application using Internet Explorer. For the most part, Polycom recommends using RMX Manager to configure and manage the RealPresence Collaboration Server. However, use the RMX Web Client when direct access to a single RealPresence Collaboration Server, Appliance Edition is required.

To install RMX Manager:

1. Access Polycom Support at support.polycom.com. Polycom recommends using Microsoft Internet Explorer for the download.

   You can also install RMX Manager from the RMX Web Client login page.
2. In the **Documents and Downloads** section, select **UC Infrastructure** as the **Product Type**, your model of the **RealPresence Collaboration Server** as the **Product**, and click **Go**.
3. Select the appropriate version of the **Local Web Client (RMX Manager)**.
4. When prompted, accept the **End User License Agreement** and the **Export Restrictions Agreement**.
5. When prompted, click **Open** and navigate to the `RMX_x-x-x-nnnn_LocalWebClient-RMXManager > RmxManagerInstallerMsi` folder.
6. Double-click `setup.exe` to install RMX Manager.
7. Follow the directions for the install wizard.

Connect to the MCU with RMX Manager

With RMX Manager, you can connect to one or more RealPresence Collaboration Server MCUs installed on the network.The connection process has two steps: you first add the MCU, then you connect to the MCU.

Note the following about connecting RMX Manager to an MCU:

- The first MCU connected to RMX Manager provides the authorization level of users that can connect to the other MCUs on the list.
- Each user can have a different login name and password for each of the listed MCUs.
- You must define all users in the user list of each of the listed MCUs.

Add an MCU

To add a RealPresence Collaboration Server MCU to RMX Manager, you need the MCUs IP address and a user name and password for the server--either the admin account or your own credentials.

To add an MCU:

1. In RMX Manager, click **Add MCU.**
2. Enter a unique name for the MCU and enter the **MCU IP**.
3. Enter the required port to be used for the connection. Enter 443 to establish a secure connection.
4. Enter a valid **User Name**, and **Password**.
5. Click **OK**.

Connect to an MCU

Use the RMX Web Client when direct access to a single RealPresence Collaboration Server, Appliance Edition is required.

To connect to an MCU:

1. In RMX Manager, select the MCU from the MCUs list or enter its IP address in the **Find**: field and click 
2. Click **Connect MCU**  .
3. If required, select a certificate for the MCU and click OK.
4. If you are prompted to re-enter credentials, enter the **User Name**, and **Password** again.

   When the progress indicator shows Complete, the RealPresence Collaboration Server is ready.

Configure the Time Settings

You can configure the RealPresence Collaboration Server (RMX) time manually or set it up to synchronize with an external NTP server. While using NTP Server, ensure to use version 4 which is supported and used by the RealPresence Collaboration Server while using NTP Server. This will ensure continuity, accurate scheduling, and accurate reports for all systems. Following MCU reset, a delay might occur when synchronizing with the external NTP servers.

To set the time settings:

1. In RMX Manager, go to **Setup > RMX Time**.
2. Configure these settings, as necessary.

Field	Description
GMT Date	The UK, Greenwich date.
Local Time	The MCU local time settings calculated from GMT Time and GMT Offset.

Field	Description
GMT Time	Select the Up/Down arrows to set the GMT Time.
GMT Offset	The time zone difference between Greenwich and the MCU physical location, in hours and minutes.
Retrieve Client Time	Automatically updates the GMT Date, GMT Time, and GMT Offset to match that of the workstation.
Use NTP Server	When selected, synchronizes the MCU time with up to three NTP server and disables the manual GMT Date and GMT Time setting.
Adjust Reservations Time	This option adjusts the start time of all reservations.

3 Click **OK**.

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 do not 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 are not trusted and CA-signed certificates are needed.

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.

To create a certificate signing request:

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 of
State or Province	Specifies the state or province where your organization is located.
Locality	Specifies the city where your organization is located.

CSR Information	Description
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.
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 is selected, you can modify the example values provided, to match local certificate requirements and delete those that are not applicable. • Principle Name—Specifies the user and domain name for logging in to a Windows domain (e.g., `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 RMX is configured with IPv4, then the IPv4 address will display. ▲ If RMX is configured with IPv6, then the IPv6 address will display, besides you can also enter additional IPv6 addresses. ▲ If RMX is configured with both IPv4 and IPv6, then both IP addresses will display.
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.

Installing the Certificate

You can add, edit, and remove certificates from the system.

To add the certificate to the system:

1. In RMX Manager**,** go to **Setup > RMX Secured Communication > 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.

Obtain the Display Name

Administrators and operators can configure the MCU to display participants' names (as found in the Addess 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 is not 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.

This feature is supported for IPv4 participants only.

To enable the Obtain Display Name from Address Book option:

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

Integrate with the RealPresence Resource Manager System

If your organization has the Polycom® RealPresence® Clariti solution (that is, a RealPresence Resource Manager system and a RealPresence DMA system along with one or more RealPresence Collaboration Servers), integrate your RealPresence Collaboration Server with the Polycom® RealPresence® Resource Manager system and set it us as the device (endpoint and server) application manager. The Resource Manager system can also manage users and conference participants.

To integrate the RealPresence Collaboration Server with the RealPresence Resource Manager system:

1. If not already done, add the MCU(s) to the RealPresence Resource Manager system. See the *RealPresence Resource Manager Operations Guide* for more information.
2. If your organization uses the RealPresence Resource Manager system Global Address Book for conference and endpoint management, add a user account on the RealPresence Resource Manager that the RealPresence Collaboration Server can use as its machine integration account. See the *RealPresence Resource Manager Operations Guide* for more information.
3. Write down the user name and password for the machine integration account. You will need this information for configuring the required system flags. See System Flags for more information.

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 x256 pixels
- Image area (width * height) must not be smaller than 64 pixels x 64 pixels

To add a custom logo as a conference overlay:

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. Enable the Custom Logo checkbox.
5. Select the appropriate Logo Position. The options are identical to those supported for the Layout Indication icons.
6. Click **OK** to save the profile.
7. In RMX Manager, go to **Setup > Custom Logo**
8. Browse to and select the logo image file to upload.
9. Click OK.

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

Configure Required System Flags

In general, you configure the RealPresence Collaboration Server using the user interface. However, you will likely need to configure the MCU for specific application and operational needs by adding predefined RealPresence Collaboration Server system flags and setting them to the required values.

To configure the required system flags:

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 RealPresence Resource Manager system, add 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, 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 RealPresence Resource Manager system.

Integrate with the RealPresence DMA System

If your organization has the Polycom® RealPresence® Clariti solution (that is, a RealPresence Resource Manager system and a RealPresence DMA system along with one or more RealPresence Collaboration Servers), integrate your RealPresence Collaboration Server with the Polycom® RealPresence® DMA system and set it us as the call control for the conferencing network. Configure the RealPresence DMA system as the H.323 gatekeeper and/or SIP server, endpoint registrar and virtual meeting room manager.

To integrate the RealPresence Collaboration Server with the RealPresence DMA system:

1. If not already done, add the RealPresence Collaboration Servers and the RealPresence DMA system as device instances to the RealPresence Resource Manager system. See the *RealPresence Resource Manager Operations Guide* for more information.
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 RealPresence DMA 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 RealPresence DMA system 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.

To integrate the RealPresence Collaboration Server with the HARMAN Media Suite:

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.

Recording Link Parameters

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 does not define the VRR, enter the HARMAN Media Suite E.164 that registers to RealPresence DMA system as the Alias Name. The default VRR is used for recording. If you are 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**.

Customizing the RMX Manager User Interface

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.

To switch between RMX Management Toolbar and List Views:

» 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.

To move items in the RMX Management list:

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.
   An indicator line () appears indicating the new position of the icon.

Restore Default RMX Manager User Interface

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

To restore the RMX Manager user interface to its default configuration:

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

Conference Profiles and Templates

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

IMPORTANT:

If you have a Polycom® RealPresence® DMA® system, create conference templates and manage conferencing parameters on the RealPresence DMA system and not on the RealPresence Collaboration Server.

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

Conference Profiles

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 protocol(s) supported
- Conference messaging
- Polycom Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA)
- Encryption

The following topics describe RealPresence Collaboration Server conference profiles.

View the List of Conference Profiles

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

- Factory_Video_Profile
- Factory_SVC_Video_Profile
- *Factory_Mix_Video_Profile*

To view the current list of conference profiles:

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

Add a New 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.

To add a new conference profile:

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 **CP (Continuous Presence)** is selected, all tabs are available.
   - When **SVC Only** is selected, the **General**, **Advanced**, **Video Quality**, **Video Settings**, **Audio Settings**, **IVR**, and **Network Settings** tabs are available.
   - When **CP and SVC** is available, 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 CP and SVC or SVC Only conferencing modes are selected
   - 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

   For detailed information about the conferencing parameters, see Conference Profile Parameters .
5. Click **OK** to save the new profile.

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:** Downspeeding is not supported. As a result, ISDN-video calls will consume bandwidth resources according to the line rate specified in the conference profile. For example, if the conference line rate is 512kbps, ISDN-video calls connecting at lower line rates (256kbps) still consume the bandwidth resources of 512kbps calls. As a result, if bandwidth resources are fully consumed, ISDN-video calls may be rejected before media card resources are exhausted.
Conferencing Mode	Choose one of the following: • **Continuous Presence (CP)** — (also known as AVC) This mode supports the H.264 Advanced Video Coding (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). The number of enhancement layer streams sent to a device can be tailored 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. • If all ASCII text is entered in the **Display Name**, it is used also as the **Routing Name**. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in the **Display Name**, the ID (such as Conference ID) is used 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. Those that don't support the specified line rate are connected in voice-only mode. • You can also enable H.264 high profile, which allows the conference to use Polycom's bandwidth-conserving H.264 High Profile codec.
Operator Conference	Not available when **Video Switching** is enabled. 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 cannot join.
Packet loss compensation (LPR and DBA)	Enables Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA). • LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission. In CP Conferences, LPR is enabled by default while in VSW Conferences, LPR is disabled by default. LPR can be enabled for VSW conferences but H.320 and SIP participants will not be able to connect. • DBA allocates the bandwidth needed to transmit the additional packets.
Auto Terminate	Not available when **Operator Conference** is enabled. Not recommended for **SVC Only** conferences. When enabled, the MCU automatically ends the conference when the specified termination conditions are met. 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 have been abnormally disconnected from a conference.
Exclusive Content Mode	When enabled, if a participant is broadcasting content, other participants are prevented from interrupting with their own content while 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 that when receiving calls through a firewall or session border controller (SBC), the MCU should send media stream keep-alive messages to the RTP, UDP and BFCP channels at the interval specified. The acceptable interval is within the range of 1 - 86400 seconds.

Advanced Parameters

Field/Option	Description
TIP Compatibility	Available only when **CP (Continuous Presence)** conferencing mode is selected. Enables compatibility with Cisco Telepresence Systems (CTS) and Telepresence Interoperability Protocol (TIP), either for video only or for both video and content. If **Prefer TIP** is enabled, TIP content is used for endpoints that support TIP, and non-TIP content is used with non-TIP endpoints. Requires a minimum line rate of 1024 kbps and HD resolution (720 or better). **Note:** If an option other than **None** is enabled, the **Gathering Settings** options are disabled.
MS AV MCU 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** — The cascade link between the <Product Name>RealPresence Collaboration Server system and the Skype for Business server's AVMCU is limited to SD video resolutions to conserve MCU resources. • **Video Optimized** — The cascade link between the <Product Name>RealPresence Collaboration Server system 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 when **CP (Continuous Presence)** conferencing mode is selected. When enabled, the MCU implements a Gathering Phase, which is the time period at the beginning of a conference when participants are connecting to the conference. During the Gathering Phase, a mix of live video from connected endpoints is combined with both static and variable textual information (specified here) about the conference into a slide which is displayed on all connected endpoints.
Displayed Language	Language in which the Gathering Phase page is displayed.
Dial-in Number 1	Applies to Appliance Editions only. Optional access numbers to display on the gathering phase slide.
Dial-in Number 2	
Info 1	Optional free-form text fields to display on the gathering phase slide. On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint.
Info 2	
Info 3	

Video Quality Parameters

Field	Description
People Video Definition	
Video Quality	Available only when **CP (Continuous Presence)** conferencing mode is selected. Specifies two video optimizations: • **Motion** — higher frame rate without increased resolution • **Sharpness** — higher video resolution that requires more system resources **Note:** When **Sharpness** is selected, the MCU will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps.
Maximum Resolution	Available only when **CP (Continuous Presence)** conferencing mode is selected.. Overrides the **Maximum Resolution** setting of the **Resolution Configuration** dialog box. Select one of the following options: • **Auto** - The **Maximum Resolution** remains as selected in the **Resolution Configuration** dialog box. • **CIF** • **SD** • **HD720** • **HD1080**
Video Clarity™	Applies to Appliance Editions only. Available only when **CP (Continuous Presence)** conferencing mode is selected. Not available when **Video Switching** is enabled. When enabled, a video enhancement algorithm is applied that sends clearer images with sharper edges and higher contrast back to all endpoints at the highest possible resolution supported by each endpoint. All layouts, including 1x1, are supported.
Auto Brightness	Applies to Appliance Editions only. When enabled, color changes may be observed in computer-based VGA content sent by HDX endpoints through the People video channel.
Content Video Definition	
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 when **CP (Continuous Presence)** conferencing mode is selected. Enables content sharing using AS-SIP security and the **Multiple Content Resolutions** option, which is not supported in any other content sharing mode.

Video Quality Parameters

Field	Description

Multiple Content Resolutions	Available only when **CP (Continuous Presence)** conferencing mode is selected.
	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 set to **H.264 cascade and SVC optimized**. The content resolutions available for selection depend on the content sharing mode (highest common or multiple content resolutions), line rate and content settings selected for the conference.

Send Content to Legacy Endpoints	Available only when **CP (Continuous Presence)** conferencing mode is selected. When enabled, content can be sent over the video (people) channel to H.323/SIP/ISDN-video endpoints that do not support H.239 content. Select this option when Avaya IP Softphone will be connecting to the conference.
H.264 High Profile	Applies to Appliance Editions only. Displayed only when conferencing mode is VSW (Video Switching), or the selected Content Protocol is **H.264 Cascade Optimized**. In scenarios where endpoints not supporting high profile (such as HDX) are connected to the conference, it is recommended to clear this check-box to enable them to share content.
Enable MS RDP Content	When enabled, the MCU starts conferences on Modular MCUs (MMCU) that have sufficient soft blade resources. MMCUs may be configured with an RDP translator that converts H.264 content shared from a standard endpoint 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. **Notes:** • For Polycom RealConnect calls to work, set ‘AllowMultiView’ to TRUE on the Skype for Business Front End Server. This will enable the participants to connect and receive multiple video streams. • This option can be used in place of a separate Polycom® ContentConnect™ gateway solution.

Video Settings Parameters

Field/Option	Description
Presentation Mode	Available only when **CP (Continuous Presence)** conferencing mode is selected. When enabled, the conference changes 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 when **CP and SVC** conferencing mode is selected. Not available if **Presentation Mode** or **Video Switching** is selected, or if **Telepresence Mode** is **Yes**. Forces the selected layout to all participants. Personal selection of the video layout is disabled.
Lecturer View Switching	Available only when **CP (Continuous Presence)** conferencing mode is selected. Not available if **Same layout** is selected or **Telepresence Mode** is **Yes**. When in lecture mode, enables the lecturer's view to automatically switch among participants (if the number exceeds the number of windows in the layout) while the lecturer is talking.
Telepresence Mode	Available only when **CP (Continuous Presence)** conferencing mode is selected. Supports telepresence conference rooms joining the conference: • **Auto** – A conference is automatically put into 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.
Telepresence Layout Mode	Available only when **CP (Continuous Presence)** conferencing mode is selected. Not available if **Telepresence Mode** is **No**. Specifies the layout for telepresence conferences: • **Manual** – Layout is controlled manually by a conference operator 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 speaker's site is the only one seen by others. • **Speaker Priority** – Ensures that the current speaker is always displayed in the video layout. The previous speakers are also displayed if there is room in the layout. In this mode, each endpoint in the conference reserves screens for displaying the active speaker in the largest video layout cell available.
Auto Scan Interval(s)	Available only when **CP (Continuous Presence)** conferencing mode is selected. Specifies the time interval (between 5 - 300 seconds) that **Auto Scan** uses to cycle the display of participants that are not in the conference layout in the selected cell. **Auto Scan** is often used in conjunction with **Customized Polling** which allows the cyclic display to be set to a predefined order for a predefined time period.
Auto Layout	Available only when **CP (Continuous Presence)** conferencing mode is selected. When selected, the system automatically selects the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically 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. The default Conference IVR Service is selected.
Conference Requires Chairperson	When enabled, conferences will not start until the chairperson joins. Callers who arrive early are placed on hold. If Terminate conference after chairperson leaves is also enabled, the conference will end when the last chairperson leaves. This option is ignored if a participant doesn't enter a chairperson passcode. 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 the users. **Note**: When enabled for a Polycom RealConnect™ conference, the Skype for Business presenter acts 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 to be used for conference recording.
Start Recording	Select when to start the recording: • **Immediately** – Conference recording is automatically started upon connection of the first participant. • **Upon Request** – The operator or chairperson must initiate the recording (manual).
Audio Only	When enabled, limits recording to the audio channel of the conference.

Recording Parameters - Not available when SVC Only conferencing mode is selected

Parameter	Description
Display Recording Icon	When enabled, the MCU displays a recording indicator (a red dot) to all participants to inform them that the conference is being recorded. Skype for Business users connected to the conference via Polycom RealConnect technology get notified when a Skype for Business user starts recording the meeting by displaying a recording icon within the video layout.
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 if, when, and how the endpoint display name is shown on each video participant's display. • **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** - Do not display the site names and all other fields in this tab are grayed and disabled

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 font size, color, position, and transparency 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 when **Enable Recording** is enabled on the **Recording** tab. When enabled, the MCU displays a recording indicator (a red dot) to all participants to inform them that the conference is being recorded. Skype for Business users connected to the conference via Polycom RealConnect technology get notified when a Skype for Business user starts recording the meeting by displaying a recording icon within the video layout.
Audio Participants	When enabled, displays the count of audio participants on each video participant's display. The count can be displayed on the 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, the network quality reading is displayed on each video participant's display.
Custom Logo	When enabled and a

Conference Templates

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

A *conference template does the following*:

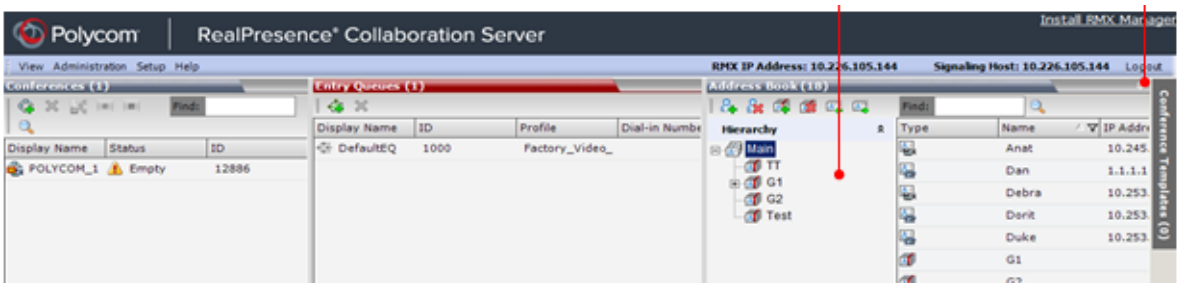
- Saves the conference profile
- Saves all participant parameters including the Personal Layout and Video Forcing settings
- Simplifies telepresence conference setup where precise participant layout and video forcing settings are crucial

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.

View the List of Conference Templates

A RealPresence Collaboration Server does not have default conference templates because they require information that is not standard.

On first access, the list of conference templates appears in the main RMX Manager pane. If the list is hidden, double-click the **Conference Template** tab on the right.



Add a New Conference Template

Create conference templates to start and replicate successful conferences. Conference templates:

- 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.

To add a new conference template:

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:
   - **a** Click **Add from Address Book**, select the required groups and participants, and click **Add** or
   - **b** Click **New** and 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.

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 cannot 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.

Additional Conference Profile and Conference Template Tasks

You can edit, delete, export, and import conference profiles and conference templates as described in the following sections.

Edit a Conference Profile

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

To edit a conference profile:

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 the required profile parameter(s) and click **OK**.

   For detailed information about the conferencing parameters, see Conference Profile Parameters .

Delete a Conference Profile

You can delete profiles from the MCU; however, a conference profile cannot be deleted if it is 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.

To delete a conference profile:

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 will 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.

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

To export a conference profile:

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:
     i. In the **Conference Profiles** list, select the required conference profiles.
     ii. 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 will likely want all of the same profiles available on all MCUs, so conferences can successfully cascade over multiple MCUs.

To import a conference profile:

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 will not be imported when:
   - A conference profile with that name already exists
   - The conference profile requires an IVR service that is not present on the MCU .

Edit a Conference Template

You cannot edit a conference template.

Delete a Conference Template

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

To delete a conference template:

1. In RMX Manager, click **Conference Templates**.
2. In the **Conference Templates** list, select the template(s) 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.

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

To export a conference template:

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,
     i. In the **Conference Templates** list, select the required conference template(s).
     ii. Right-click and select **Export Selected Conference Templates**.
3. **Browse** to the location to which to save the exported file(s).
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.

To import a conference template:

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` file(s)

5 Select the file(s) to import and click OK.

The imported conference template(s) and profile are added to their respective lists.

Save an Ongoing Conference as a Template

You can save any ongoing conference as a template; however, consider these notes:

- 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 are not saved in conference templates.
- Conference templates saved from an ongoing conference do not include Message Overlay text messages.

To save an ongoing conference as a template:

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

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.

IMPORTANT:

If you have a Polycom® RealPresence® DMA® system, create conference templates and manage conferencing parameters on the RealPresence DMA system and not on the MCU.

The RealPresence DMA 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 that allow the conference chairperson to control the recording process from the endpoint. However, you can associate change these default settings if desired.

To enable recording via the Conference Profile:

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 are using the HARMAN Media Suite, enter its IP address and 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 are associating this recording link to a VRR on the HARMAN Media Suite, if the Alias Type is set to H.323 ID, enter the 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##5555Define 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). E-mail 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. For more information about these parameters, see Recording Parameters - Not available when SVC Only conferencing mode is selected .

12 Click **OK**.

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.

To change the position of the conference indicators:

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**.

Indicators for Microsoft Skype for Business Users

Microsoft Skype for Business and Lync users see the same conference indicators other Polycom RealConnect conference participants do provided the video stream sent to the their endpoint is compatible. However, the indications are not embedded in the video sent to the link, so as to preserve the Skype for Business or Lync user experience.

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.

To enable multiple resolutions (set content transcoding) on Cisco TIP endpoints:

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
4. Now enable **Multiple Content Resolutions**.
5. Select the appropriate content resolution and frame rate from the drop-down menu for the **TIP Encoder**.
6. Click **OK**.

Binary Floor Control Protocol (BFCP) Support for TIP endpoints

Support for Cisco Telepresence Interoperability Protocol (TIP) version 8, now allows TIP endpoints to receive high-resolution content using Binary Floor Control Protocol (BFCP).

BFCP provides better coordinated access to conferencing resources.

For more information, see Content Sharing Using BFCP Protocol for TIP Participants in *RealPresence® Collaboration Server Technical Reference Guide*.

Legacy Content for TIP Endpoints

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.

Enable NoiseBlock™

The RealPresence Collaboration Server uses NoiseBlock,™ a heuristic algorithm, to monitor and lessen the audio of AVC endpoints with high levels of non-speech background noise. This helps prevent those endpoints from mistakenly become the active speaker, 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 affects only AVC-based and audio only endpoints (non-SAC endpoints). It does not affect SVC-based endpoints.

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

Typically, the NoiseBlock feature is enabled by default based on the interaction of two configuration elements:

- The ENABLE_SELECTIVE_MIXING flag value (enabled by default) and
- The Auto mute noisy endpoints setting (enabled by default)

Note that NoiseBlock does not guarantee exact identification of non-speech 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 prior to 8.1, the Auto mute noisy endpoints option is not 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 change the value to YES/NO. MCU reset is not required when changing the system flag value.
- If your conferencing environment includes Polycom DMA, the conferences started from the DMA do not include the NoiseBlock parameter as it is not part of the DMA 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 is enabled in the conference.

Conference Management

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

IMPORTANT:
If your environment includes a Polycom® RealPresence® Resource Manager, 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 what operations are available to perform on active conferences.

Viewing Scheduled Conferences

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

To view scheduled conferences in the Reservation Calendar:

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

Scheduling a Conference

On the RealPresence Collaboration Server, you schedule a conference by making a reservation. The reservation reserves the required resources for the number of participants at the time and duration you specify. Resources are reserved for participants at the highest video resolution supported by the line rate specified in the conference profile associated with the reservation and up to the maximum system video resolution specified for the system.

To schedule a conference:

1. In RMX Manager, go to **RMX Management > Rarely Used** > **Reservations**.
2. In the **Reservation Calendar**, 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 can then be modified. The maximum field length for the Display Name is approximately: • 80 ASCII characters • 40 European or Latin text characters • 25 Asian text characters Do not use comma or semi-colon characters 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 with which the MCU registers the conference with network devices such as gatekeepers and SIP servers. If left blank, the MCU automatically generates a Routing Name. Because this name must be ASCII characters, the MCU defines the name as follows: • If ASCII characters are entered as the Display Name, it is 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. Polycom recommends you allow the MCU to assign the Routing Name automatically
Profile	Choose the pre-defined conference profile that best identifies the conferencing mode, line rate, media settings and general settings suitable for your conferencing environment. For a detailed description of Conference Profiles, see Conference Profiles and Templates .
ID	Unique ID number for the conference on the MCU. If left blank, the MCU automatically assigns an ID number once the conference starts. Polycom recommends you allow the MCU to assign the Routing Name automatically. Communicate this conference ID to dial-in participants to enable them to dial in to the conference. Note: If setting the Conference ID to the digits that are used for MCU prefix in Gatekeeper (for example gatekeeper prefix is set to 10 and the conference ID is 1001), the system will not be able to dial to the destination conference as the prefix digits are truncated from the conference ID, preventing the system from locating it.
Conference Password	Password that participants must enter to join the conference. If left blank, participants are not required to enter a password to join the conference. This password is valid only in conferences that are configured to prompt for a conference password. By default, this password is 4 numeric characters. The administrator can modify requirements for this field. For more information, see System Flags . The MCU can be configured to automatically generate this password when this field is left blank. For more information, see System Flags .

General Conference Parameters

Field	Description
Chairperson Password	Password that the chairperson must enter to join the conference with chairperson responsibilities. If left blank, chairperson functionality is not enabled for the conference. This password is valid only in conferences that are configured to prompt for a chairperson password. By default, this password is 4 numeric characters. The administrator can modify requirements for this field. For more information, see System Flags . The MCU can be configured to automatically generate this password when this field is left blank. For more information, see System Flags .
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 / RMX1800: 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 / RMX1800: 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 a number is specified, it should be large enough to accommodate the participants specified in the **Reserve Resources for Video/Voice 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	Choose the pre-defined network service that best suites your conferencing environment. Identifies the pre-defined Network Service.
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. Again, 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 To make the conference recurring, click **Schedule** and enter the required scheduling and recurrence information.

6 Click **Participants** and add participants from the **Address Book** or click **New** and enter the required information for new participants.

7 If required, chose a participant as a lecturer and as needed enable **Dial Out Manually**, so the MCU can dial out to the lecturer.

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 cannot replace that participant with the dial-in participant that is connected to the conference.

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

9 To add optional conference information, click **Information** and enter the required text into the Info1, Info2, Info3, or Billing Info text boxes.

10 Click **OK** to schedule the conference.

Unless otherwise specified, the system automatically assigns the conference an ID when the conference starts.

11 Communicate the conference ID to conference dial-in participants.

Starting an Ad Hoc Conference

Ad hoc conferences are those created and started immediately.

To create and start an ad hoc conference:

1 In the **Conferences** section of RMX Manager, click **New Conference** ( ).

2 Select and edit the conference parameters you wish to define. For more information about the conferencing parameters, see General Conference Parameters .

3 Click **Participants** and add participants from the **Address Book** or click **New** and enter the required information for new participants.

4 If required, chose a participant as a lecturer and as needed enable **Dial Out Manually**, so the MCU can dial out to the lecturer.

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 cannot 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.

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

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

IMPORTANT:
If your organization uses another conference management application such as the Polycom® RealPresence® Resource Manager, Polycom recommends that you create and schedule conferences using that applications and not the MCU.

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

General Conference Management Tasks

An RMX administrator or operator may be required to perform these general conference management tasks on an active conference.

Viewing the List of Active Conferences

You can view the list of active conferences in the main Conferences List section of RMX Manager.

Viewing 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.

To view the properties of an active conference:

1. In the RMX Manager **Conferences List**, select the active conference of interest.
2. Right-click and select **Conference Properties**.
   For information about the conference parameters identified, see General Conference Parameters .

Locking a Conference

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

To lock a conference:

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

Unlocking a Conference

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

To unlock a locked conference:

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

   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.

Participant Management Tasks

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

Viewing the List, State and Properties of Participants

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

To view the list and state of active conference participants:

1. In the RMX Manager **Conferences List**, select the active conference of interest.

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

Column	Icon/Description	
Name	Displays the name and type (icon) of the participant:	
		Audio Participant – Connected via IP phone or ISDN (audio/video).
		Video Participant – Connected with audio and video channels.

Column	Icon/Description	
Status	Displays the connection status (text and icon) of the participant. If there is no problem with the participant's connection no indication is displayed.	
		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 is not yet complete; the video channel has not been connected.
		Faulty **Connection** – The participant is connected, but problems occurred in the connection, such as synchronization loss.
		Secondary Connection – The endpoint's video channel cannot be connected 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-based connection) – 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 does not 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/system operator can indicate that they want to be unmuted by entering the appropriate DTMF code (default 99). The icon is displayed for 30 seconds.
IP Address/Phone	The IP participant's IP address or the ISDN (audio/video) participant's phone number.	
Alias Name/ SIP Address	The participant's Alias Name or SIP URI. The alias of a Polycom® RealPresence® Media Suite if the participant is functioning as a recording link.	
Network	The participant's network connection type – H.323, or SIP or ISDN (audio/video).	
Dialing Direction		Dial-in – The participant dialed the conference.
		Dial-out – The MCU dialed the participant.
Audio	Displays the status of the participant's audio channel. If the participant's audio is connected and the channel is neither muted nor blocked, no indication is displayed.	
		**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 User 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.

Column	Icon/Description	
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 neither suspended nor secondary, no indication is displayed.	
		**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 is not supported with ISDN-video.
Content Token		Participant is the holder of 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 of interest.

3 Right-click and select **Participant Properties**.

Adding Participants 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.

To add a participant or group to an active conference:

1 In the RMX Manager **Conferences List**, select the active conference of interest.

2 Click **Participants** and then:

a Click **Add from Address Book**, select the required groups and participants, and click **Add**

OR

b Click **New** and 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.

Moving Participants Between Conferences

An 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).

An RMX administrator or operator cannot move participants from Lost Packet Recovery (LPR)-enabled, Video Switching, or Telepresence conferences. Moving participants between encrypted and non-encrypted 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 will be disconnected from the original conference, and then the MCU automatically dials out to connect them to the destination conference.
- Participants in cascaded conferences links 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.

To move a participant from one conference to another:

1. In the RMX Manager **Conferences List**, select the active conference of interest.
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 the participant(s) 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 options returns the participant back the original conference.

  This option is not available if the participant was moved from an Entry Queue to an active conference.

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

Sending a Message to Participants During a Conference

Using the Message Overlay feature, an RMX administrator or operator can send messages to a single conference participant, a number of selected participants, or all conference participants. The 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 is not available:

- 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.

To send messages to conference participants:

1 In the RMX Manager **Conferences List**, select the active conference of interest.
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, again select the conference of interest.
5 Right click and select **Conference Properties**.
6 Go to **Message Overlay** and check the **Enable** option.
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.

Restricting Content Sharing

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 is shared in a conference.

Enable this restriction by setting the RESTRICT_CONTENT_BROADCAST_TO_LECTURER system flag to ON. For more information about setting this system flag, see System Flags .

Designating a Participant 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 is resumed automatically when the lecturer resumes talking.

To designate a participant the lecturer during the ongoing conference:

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**.

Muting 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 are not muted until the lecturer joins the conference.

Muted participants can only be unmuted by:

- A RealPresence Collaboration Server administrator or operator or

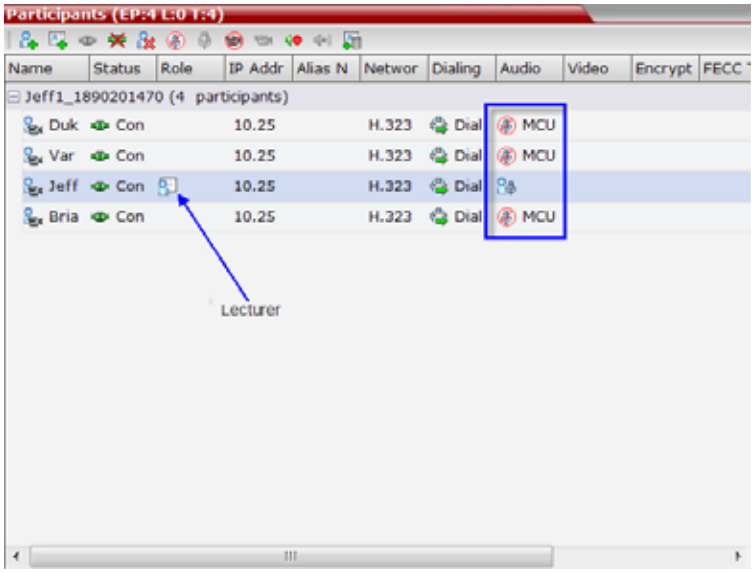
- The participant entering the DTMF code to activate the **Mute All Except Me** option. To do this, the participant must be authorized to do so in the IVR Services properties). In this case, the lecturer's audio is muted and the authorized participant's audio is unmuted until you reactive the Mute Participants Except Lecturer option again.

When the **Mute Participants Except Lecturer** option is enabled, the mute indicator on the participant video endpoint display are not visible because the mute participants was initiated by the MCU. You may wish to inform participants that their audio is muted by using the Message Overlay functions. For more information on this function, see Sending a Message to Participants During a Conference .

To mute all participants other than the lecturer during the ongoing conference:

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 is not 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 MCU** icon is displayed in the Participants pane.



Previewing 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 does not 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 does not include shared content being sent by the participant
- Video preview is supported in cascaded conferences
- Video preview is disabled in encrypted conferences
- Video preview is not displayed when the participant's video is suspended

To preview the participant video:

1. In the RMX Manager **Conferences List**, select the active conference of interest.
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** - To display the video sent from the participant to the conference.
   - **View Participant Received Video** - To display the video sent from the conference to the participant.

   The **Video Preview** window opens.

Enabling Auto Scan

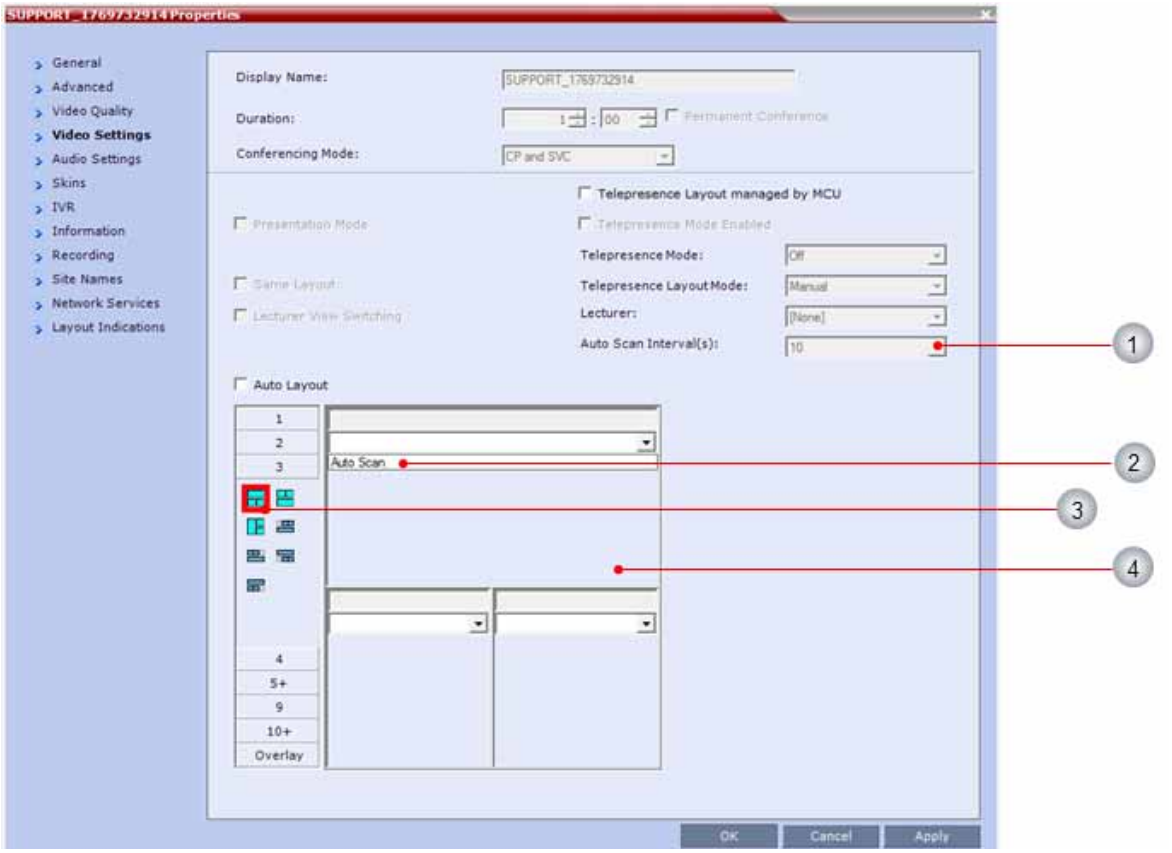
When the number of participants in a conference is greater than the number of cells in the conference layout, you can display those extra participants within a single designated cell in the conference layout. Auto Scan only takes effect when the number of participants is larger than the number of cells in the conference layout. RealPresence Collaboration Server supports Auto Scan in AVC CP conferences only

To enable Auto Scan:

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 **Video Settings**.

The **Video Settings** dialog is displayed.



Reference Number	Description
1	Auto Scan interval
2	**Auto Scan option**
3	**Selected video layout**
4	Selected video layout cell

3 If **Auto Layout** is enabled, 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**.

Enabling Customized Polling

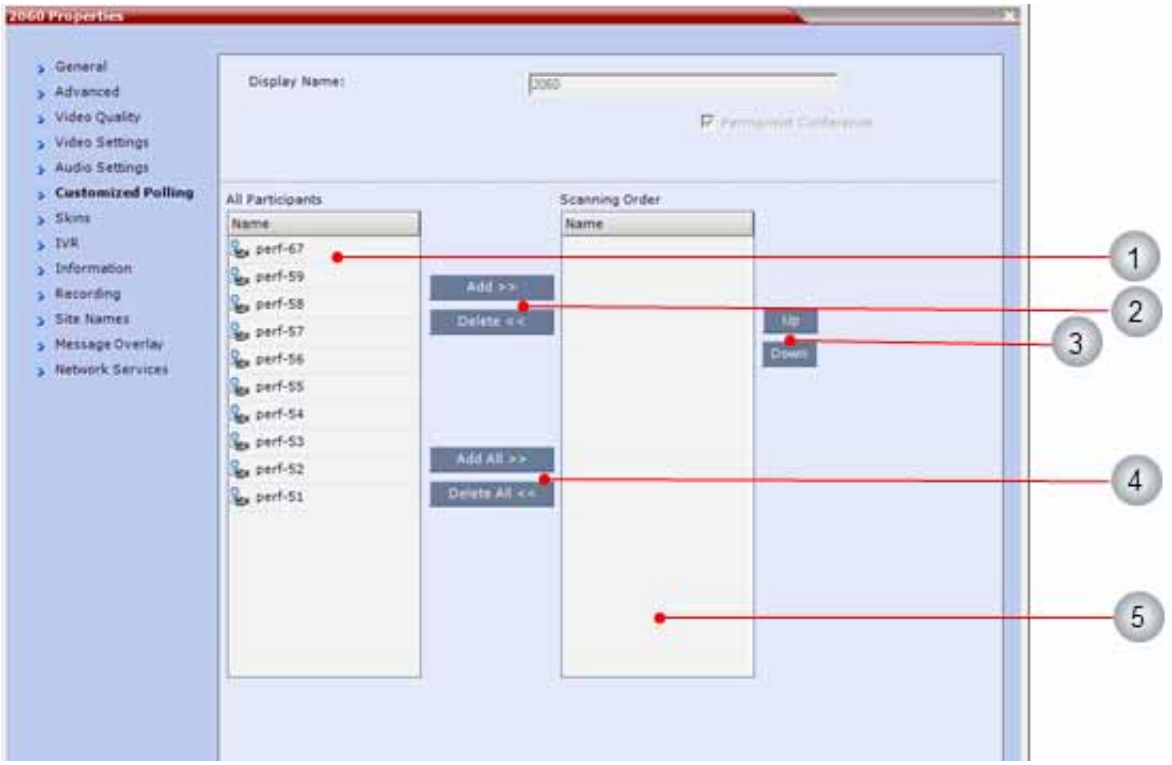
Customized Polling allows you to define an Auto Scan order and an Auto Scan time interval. Customized Polling only takes effect when the number of participants is larger than the number of cells in the layout.

Note the following:

- RealPresence Collaboration Server supports Auto Scan and Customized Polling in AVC CP conferences only
- If Customized Polling is not defined, the RealPresence Collaboration Server will Auto Scan based on the order in which participants connected to the conference.

To define the scanning order in the Customized Polling tab:

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**.

Canceling a Message Overlay

You can cancel the messages being sent to conference participants whether the message is part of the conference profile or not.

To cancel the Message Overlay:

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** checkbox.

Adding 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.

To add a participant in an active conference to the Address Book:

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

Viewing the List of Participants Awaiting Help

The Participant Alerts section at the bottom of RMX Manager flashes when participants are awaiting help. Double-click on the Participant Alert title to view the list of participants awaiting help.

Content Sharing Management Tasks

An RMX administrator or operator may be required to perform these tasks to manage content sharing into an active conference.

Giving Exclusive Content Sharing Ownership

When not in Exclusive Content Mode, all conference participants with capable devices can share content with the conference. As an RMX administrator or operator, you can give a participant the exclusive right to share content.

To give token ownership:

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 is 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.

Canceling Exclusive Content Sharing Ownership

An 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.

To cancel token ownership:

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**.

Abort a Content Sharing Session

An RMX administrator or operator can immediately abort a content sharing session.

To abort a content session:

1. In the **Conferences** list of RMX Manager, select the active conference of interest.
2. Right-click and select **Abort H.239 Session**.

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. For more information on enabling recording via the conference profile see .

If you edit the conference profile that is being used for active conferences to enable recording, that change will apply to the active conference, but it will also apply to all other active conferences and future conferences using that profile, which may not be desirable.

If an active conference is using the

Cascading Conferences

Note: Content Applicability

- Cascading information applies to AVC-enabled Conferencing (CP, VSW, and mixed CP and SVC).
- Cascading Conferences are not supported by Collaboration Server (RMX) 1800 with no DSP cards, and Collaboration Server 1800, Entry Level.

Cascading allows administrators to connect one conference directly to one or several conferences, depending on the topology, creating one large conference. The conferences can run on the same MCU or different MCUs.

There are many reasons for cascading conferences, the most common are:

- Connecting two conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, like different communication protocols, such as, serial connections, ISDN-video, etc.

Conferences are cascaded when a link is created between two conferences, running on two different MCUs.

Cascading Link Properties

Cascade links are treated as endpoints in CP conferences. They are allocated resources as any other endpoint according to Default Minimum Threshold Line Rates per Resolution and Resolution Configuration for CP Conferences

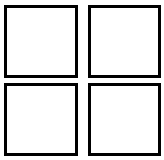
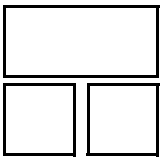
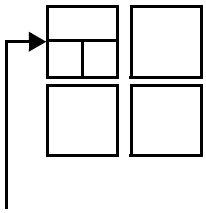
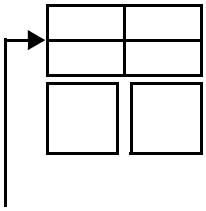
They transmit audio, video and content between conferences as well as DTMF codes input from other endpoints in the conference.

Setting the Video Layout in Cascading conferences

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

Video Layouts in Cascaded Conferences

	Conference A	Conference B
Without cascading		
During cascading	 Video layout of conference B within window of conference A	 Video layout of conference A within window of conference B

Guidelines

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

- The same version installed on all MCUs participating the cascading topology.
- The same license installed on all MCUs participating the cascading topology.
- Identical Conference Parameters defined in the Profile of the conferences participating in the cascading topology:
  - Conference line rates
  - Content rate
  - Encryption settings
- DTMF codes defined using identical numeric codes in the IVR services assigned to the cascading conferences
- DTMF forwarding suppressed
- Video layout of the link is set to 1x1 by the appropriate system flag.

  Cascaded links in 1x1 video layout use SD resolution.
- When the Mute Participants Except Lecturer option is enabled in the Conference Profile, all participants (including the link participants) except the lecturer are muted.
- Gathering phase is not supported in Cascading Conferences.

Flags Controlling Cascade Layouts

- Setting the FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION System Flag to **YES** (default) automatically forces the cascading link to Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.

  Set this flag to **NO** when cascading between an Collaboration Server and an MCU/MGC functioning as a Gateway, if the participant layouts on the MCU/MGC are not to be forced to 1X1.

- Setting the **AVOID_VIDEO_LOOP_BACK_IN_CASCADE** System Flag to **YES** (default) prevents the speaker's image from being sent back through the participant link from the cascaded conference. This can occur in cascaded conferences with conference layouts other than 1x1. It results in the speaker's own video image being displayed in the speaker's video layout.

  This option is supported with:

  ➢ In IP (H.323, SIP) and ISDN-video environments.

  This option is supported with Basic Cascading of Continuous Presence and Video Switched conferences. If a Master MCU has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.

  ➢ Video resolution will be according to the Resolution Configuration, or VSW profile.

For more details on defining system flags, see Modifying System Flags.

DTMF Forwarding

When two conferences are connected over an IP link, DTMF codes from one conference are not forwarded to the second conference. The following operations with the exception, and are available throughout the conference, with their DTMF codes forwarded (i.e. they will apply to both conferences):

- Terminate conference.
- Mute all but me.
- Unmute all but me.
- Secure conference.
- Unsecure conference.

Note: DTMF Codes Forwarding

During cascading between a gateway and a conference all DTMF codes are forwarded from the gateway to the conference and vice versa.

Play Tone Upon Cascading Link Connection

The Collaboration Server can be configured to play a tone when a cascading link between conferences is established. The tone is played in both conferences.

This tone is not played when the cascading link disconnects from the conferences.

The tone used to notify that the cascading link connection has been established cannot be customized.

The option to play a tone when the cascading link is established is enabled by setting the System Flag CASCADE_LINK_PLAY_TONE_ON_CONNECTION to YES.

Default value: NO.

The tone volume is controlled by the same flag as the IVR messages and tones: IVR_MESSAGE_VOLUME.

Possible Cascading Topologies

The following cascading topologies are available for setting cascading conferences:

- Basic Cascading - only two conferences are connected (usually running on two different Collaboration Servers). The cascaded MCUs reside on the same network.
- Star Cascading - one or several conferences are connected to one master conference. Conferences are usually running on separate MCUs. The cascaded MCUs reside on the same network.
- MIH (Multi-Hierarchy) Cascading (in non-virtual MCUs) - several conferences are connected to each other in Master-Slave relationship. The cascaded MCUs can reside on different networks.

System configuration and feature availability change according to the selected cascading topology.

Note: Sharing Content in Cascaded Conferences

For properly sharing content in cascaded conferences, predefined dial in and out link participants must be defined with Master/Slave settings in the conferences.

When Cascading between the Collaboration Server and third party MCUs, the participant defined in the Collaboration Server conference must be defined as Master.

When cascading between the Collaboration Server and a Codian MCU, set the system flag ENABLE_CODIAN_CASCADE to YES to ensure that the Collaboration Server is defined as a Master in cascading conferences at all times.

Basic Cascading

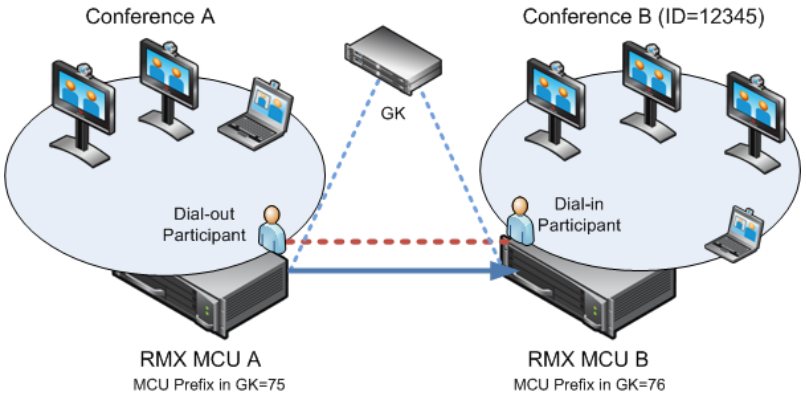
In this topology, a link is created between two conferences, usually running on two different MCUs. The MCUs are usually installed at different locations (states/countries) to save long distance charges by connecting each participant to their local MCU, while only the link between the two conferences is billed as long distance call.

- This is the only topology that enables both IP and ISDN-video cascading links.
- Cascading between Collaboration Server Virtual Edition and Collaboration Servers (RMX) 2000/1800/4000 is supported.
- When linking two conferences using an IP cascading link:
  - The destination MCU can be indicated by:
    - IP address
    - H.323 Alias
  - If IP cascading link is used to connect the two conferences, both MCUs must be located in the same network.
- One MCU can be used as a gateway.
- The configuration can include two Collaboration Servers or one Collaboration Server and one MGC.
- Multiple Cascade Links enabling Cascading between MCUs hosting conferences that include Immersive Telepresence Rooms (ITP), such as Polycom's OTX and RPX Room Systems, can be defined. For more information see Creating Multiple Cascade Links Between Telepresence Conferences.

Basic Cascading Using IP Cascaded Link

In this topology, both MCUs can be registered with the same gatekeeper or the IP addresses of both MCUs can be used for the cascading link. Content can be sent across the Cascading Link.

Basic Cascading Topology - IP Cascading Link



For example, MCU B is registered with the gatekeeper using 76 as the MCU prefix.

The connection between the two conferences is created when a dial out IP participant is defined (added) to conference A whose dial out number is the dial-in number of the conference or Entry Queue running on MCU B.

Dialing Directly to a Conference

Dial out IP participant in conference A dials out to the conference running on MCU B entering the number in the 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**.

Dialing to an Entry Queue

When dialing to an Entry Queue, the dial out participant dials the MCU B prefix or IP address of MCU B and the Entry Queue ID in the 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**.

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.

At this point, 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**.

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.

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.

Automatic Identification of the Cascading Link

In both dialing methods, the system automatically identifies that the dial in participant is an MCU, creates a Cascading Link, and displays the link icon for the participant ( ). The master-slave relationship is randomly defined by the MCUs during the negotiation process of the connection phase.

Basic Cascading Using ISDN-video Cascaded Link

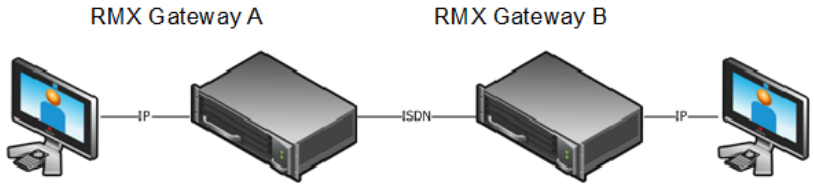
ISDN-video connection can be used to link between two MCUs or MCU and gateway and create a cascading conference. Content can be sent across the ISDN-video Cascading Link.

Network Topologies Enabling Content Sharing Over ISDN-video Cascaded Links

ISDN-video Cascaded links that support content sharing can be created between two gateways, gateway-to-MCU or between two MCUs in the following network topologies:

- Gateway to Gateway

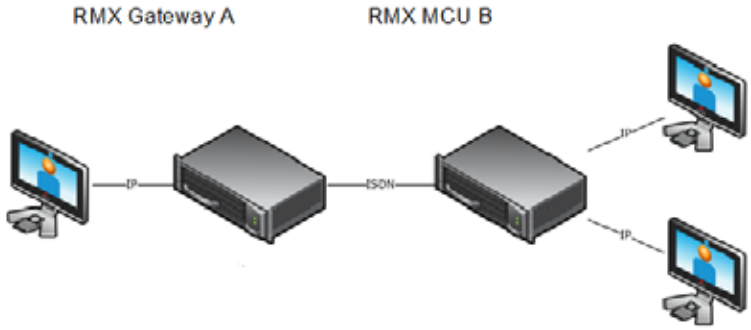
Gateway to Gateway Topology



In this topology, an IP participant calls another IP participant over an ISDN-video link between two gateways.

- Gateway to MCU

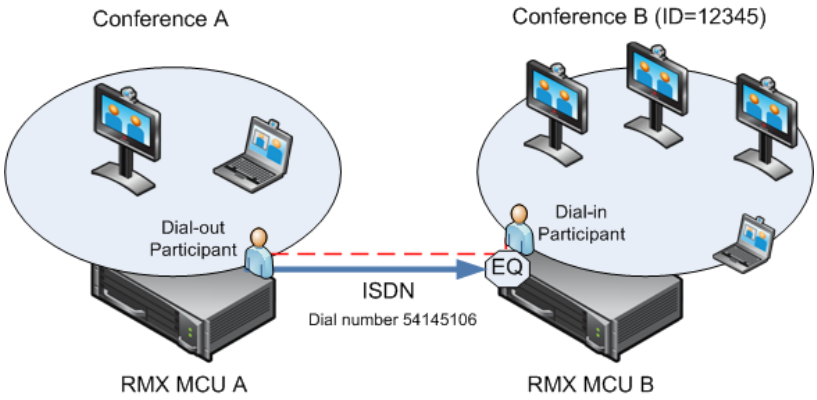
Gateway to MCU/ MCU to Gateway Topology



In this topology, an IP participant calls a conference running on an MCU via a gateway and over an ISDN-video link.

- MCU to MCU

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.

Guidelines for ISDN-video Cascaded Links

- Content is restricted, in the sense that when another endpoint wants to send content, the first endpoint must stop sending content before the second endpoint can initiate or send content.
- Endpoints that do not support H.239 can receive the Content using the Send Content to Legacy Endpoints option.
- A participant joining a conference with active Content, cannot view it. Content sharing should be restarted.
- Cascaded MCUs/Gateways must be registered with the same Gatekeeper or neighboring Gatekeepers. MCUs and endpoints must also be registered with Gatekeepers.
- Gateway/MCU calls require definition of IVR Services. For more information see System Configuration.

Note: Content Protocol over ISDN-video Cascaded link
The content sharing protocol is H.263 when sent over ISDN-video Cascading link.

Gateway to Gateway Calls via ISDN-video Cascading Link

When H.323 participants connects to another IP participants via a Gateway to Gateway call over an ISDN-video link, the dialing string includes the following components:

[GW A prefix in GK] - The prefix with which the Collaboration Server (gateway) is registered to the gatekeeper.

[GW Profile ID] - The ID of the Gateway Profile defined on Gateway A to be used for routing the call to the Gateway B.

[GW Profile ISDN (audio/video) number] - The dial-in number assigned to the Gateway Profile defined on Gateway B, including the required country and area codes.

Information required that is not part of the dialing string:

[Destination number] - The destination number as alias, IPv4 address or ISDN (audio/video) number of participant B.

The dialing string format:

H.323 Participants connecting to another IP participant via a Gateway to Gateway call over an ISDN-video link enter a dial string using the format:

<GW A Prefix in GK><Gateway Profile_ID on GW A>*<Destination ISDN-video Dial-in number assigned to the Gateway Session Profile GW B>*<Destination Number, participant>

For example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN-video Dial-in Number assigned to the Gateway Session Profile GW B	4444103
IP Participant Alias	3456

H.323 participant dials: 229999*4444103, and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes

SIP Participants connecting to another IP participant via a Gateway to Gateway call over an ISDN-video link enter a dial string using the format:

<Gateway Profile_ID on GW A>@<Central Signaling IP GW A>*<Destination ISDN-video Dial-in number assigned to the Gateway Session Profile GW B>*<Destination Number, participant>

For example:

If Central Signaling IP address of Gateway A is 172.22.177.89, SIP participant dials: 9999@172.22.177.89* 4444103 and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes.

Gateway to MCU Calls via ISDN-video Cascading Link

When H.323 participants connects to a conference/Meeting Room via a Gateway to MCU call over an ISDN-video link, the dialing string includes the following components:

[GW A prefix in GK] - The prefix with which Gateway A is registered to the gatekeeper.

[GW Profile ID on GW A] - The ID of the Gateway Profile on GW A to be used for routing the call to the Meeting Room/conference running on MCU B.

[Conference/Meeting Room/Entry Queue ISDN (audio/video) number] - The dial-in number assigned to the Entry Queue/Meeting Room/Conference defined on MCU B, including the required country and area codes.

Information required that is not part of the dialing string:

[Destination Conference ID] - Only if using the Entry Queue on MCU B for routing calls or creating new ad hoc conferences. The ID of the destination conference on MCU B.

The dialing string format:

`<GW A Prefix in GK><Gateway Profile_ID on GW A>*<ISDN-video Number assigned to the Meeting Room/Conference/Entry Queue>`

For Example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN-video Dial-in Number assigned to the Entry Queue/MR/conference	4444100
H.323 participant dials	229999*4444100

SIP participant dials (if Central Signaling IP address of Gateway A is 172.22.177.89) `9999@172.22.177.89 IP* 4444100`

If dialing an Entry Queue, when prompted for the Destination number enters `3456` followed by the pound key (`#`) using DTMF codes to create a new conference or join an ongoing conference with that ID.

MCU to MCU Calls via ISDN-video Cascading Link

A dial out ISDN-video participant is defined (added) to conference A running on MCU 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.

When the participant, who is a dial-in participant in conference B, 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 (or if connecting to a conference directly, the participant is requested to enter the conference password).

At this point 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.

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.

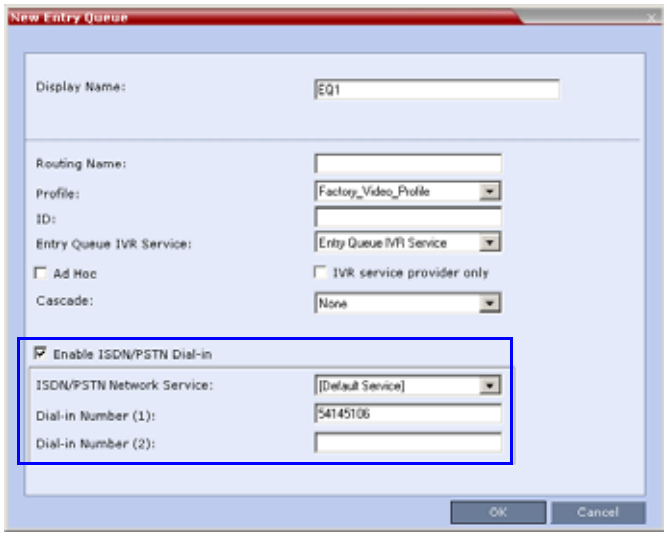
Once the DTMF codes are entered and the IVR session is completed, the participant is connected to the conference and the connection between the conferences is established. The system automatically identifies the calling participant as an MCU and the connection is identified as a cascading link and the cascading link icon is displayed for the participant ().

Collaboration Server Configuration Enabling ISDN-video Cascading Links

To enable Gateway-to-Gateway, Gateway-to-MCU and MCU-to-MCU calls over ISDN-video Cascading links, the following configurations are required:

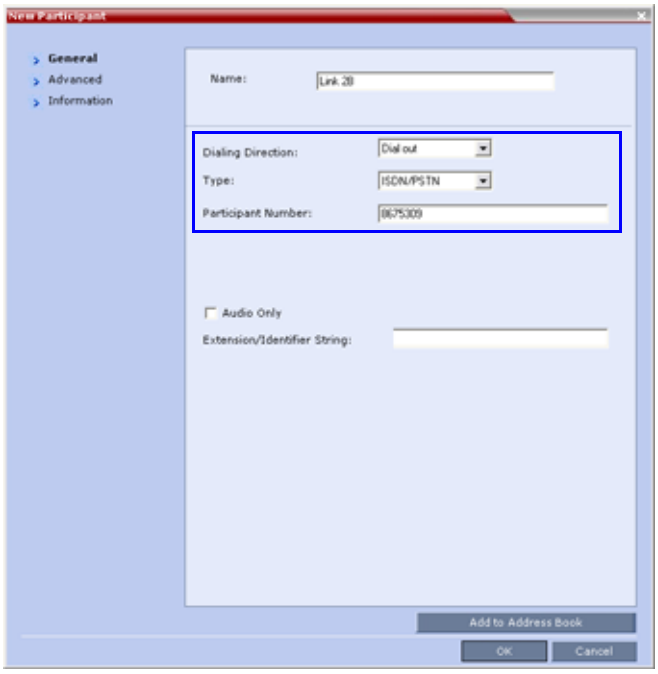
- Modifying the IP Network Service to include the MCU Prefix in the Gatekeeper (in the Gatekeepers dialog box). For more details, see Modifying the Default IP Network Service.

- ISDN-video Network Service is configured in both MCUs. For more details, **Modifying an ISDN (audio/video) Network Service**.
- Configuring a Gateway Profile and assigning dial-in ISDN (audio/video) numbers. For details, see Defining the Gateway Profile.
- Configure the Entry Queue or conference (for direct dial-in) as enabled for ISDN-video connection and a dial-in number is assigned (for example 54145106).



- Defining the dial-in ISDN-video participant in MCU B and Dial-out ISDN-video participant in MCU A (for MCU-to-MCU cascading conferences).

  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.

Conference Profile Definition

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	LPR
128	?			
128		?		
128	?			?
128	?		?	?
256	?			
256		?		
256	?			?
256	?		?	?
384	?			
384		?		
384	?			?

Recommended Conference Profile Options Setting

Line Rate	Motion	Sharpness	Encryption	LPR
384	?		?	?
512	?			
512		?		
512	?			?
512	?		?	?
768	?			
768		?		
768	?			?
768	?		?	?

Note: Line Rate Recommendation

Since the remote participant settings are unknown, it is recommended that the gateway or endpoint be configured to support a higher line rate (for example, 768 Kbps) to allow flexibility during endpoint capability negotiations.

MCU Interoperability Table

The following table lists the different MCU and Gateway configurations that are supported or implemented when routing Cascaded ISDN-video calls.

MCU Interoperability Table

Source	Destination	Scenario	Version(s)
Collaboration Server Gateway	Collaboration Server MCU	User calls via a Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 or later
Collaboration Server Gateway	Collaboration Server Gateway	User calls via a Gateway to a Remote User behind Gateway (user to user)	Collaboration Server v. 7.1 or later
Collaboration Server MCU	Collaboration Server MCU	A dial out participants calls to a remote conference (conference to conference)	Collaboration Server v. 7.1 or later
Collaboration Server MCU	Collaboration Server Gateway	A dial out participants calls to a remote User behind a Gateway (Conference to User)	Collaboration Server v. 7.1 or later
Endpoint	Collaboration Server Gateway	User calls directly to a remote user behind a Gateway (User to User)	Collaboration Server v. 7.1
Collaboration Server MCU	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	Collaboration Server v. 7.1 Latest Codian version

MCU Interoperability Table

Source	Destination	Scenario	Version(s)
Collaboration Server Gateway	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	Collaboration Server v. 7.1 Latest Codian version
Codian Gateway	Collaboration Server MCU	User calls via a Codian Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 Latest Codian version
Codian Gateway	Collaboration Server Gateway	User calls via a Codian Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Codian version
Collaboration Server MCU	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Collaboration Server Gateway	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Radvision Gateway	Collaboration Server MCU	User calls via a Radvision Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 Latest Radvision version
Radvision Gateway	Collaboration Server Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Endpoint	Collaboration Server Gateway	User calls directly to a DMA controlled environment	Collaboration Server v. 7.1
Collaboration Server MCU	Collaboration Server Gateway	A dial out participants calls to a remote conference on a DMA controlled environment	Collaboration Server v. 7.1

Notes:

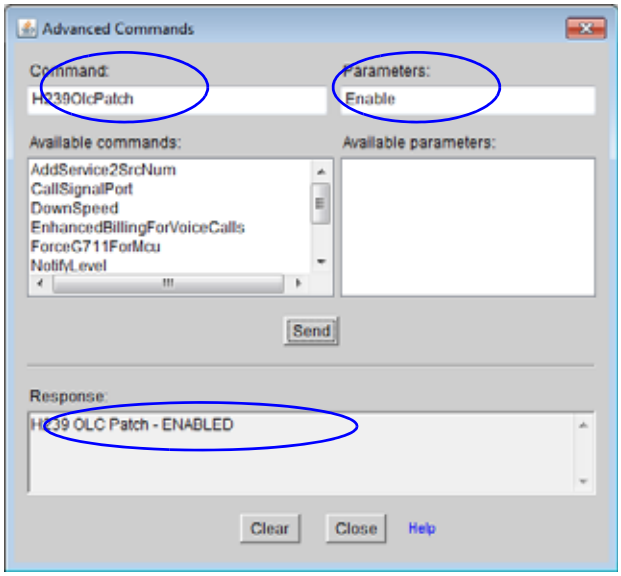
- On the Codian gateway Content is not supported with line rates of 128Kbps and below.
- To send Content from a participant over Radvision Gateway to a conference/participant, the GWP20 patch must be installed in the RadVision gateway:

  On the Radvision gateway, open the GWP20 User Interface.

  Select **Settings** > **Advanced Commands**.

  In the **Command** box, enter **H239OlcPatch**.

  In the **Parameters** box, enter **Enable** and click **Send**.



Suppression of DTMF Forwarding

Forwarding of the DTMF codes from one conference to another over an ISDN-video cascading link is not automatically suppressed as with IP cascading link, and it can be limited to basic operations while suppressing all other operations by the system flag DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS.

System Flag Settings

The **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS** flag determines the time period (in seconds) in which MCU A forwards DTMF inputs from conference A participants to MCU B. During that time, the forwarding MCU does not apply the DTMF command to itself.

Once the timer expires, most of the DTMF codes (excluding five operations as for IP links) entered in conference A are not be forwarded to conference B, and are applied within the MCU receiving the DTMF code. This is done to prevent an operation requested by a participant individually (for example, mute my line) to be applied to all the participants in conference B.

Flag range (in seconds): 0 - 360000

This flag is defined on MCU A (the calling MCU).

If a flag is not listed in the System Flags list it must be added to the system.cfg file before it can be modified. For more details on defining system flags, see Modifying System Flags.

Star Cascading Topology

In the Star topology (as well as in the Basic topology), the MCUs are usually installed at different locations (states/countries) and participants connect to their local MCU to facilitate the connection and save long distance call costs. Star Topology Cascading requires that all cascaded MCUs reside on the same network.

Note: H.323 Cascaded Link Requirement

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, the MCUs are networked together using two modes:

- Master-Slave Cascading
- Cascading via Entry Queue

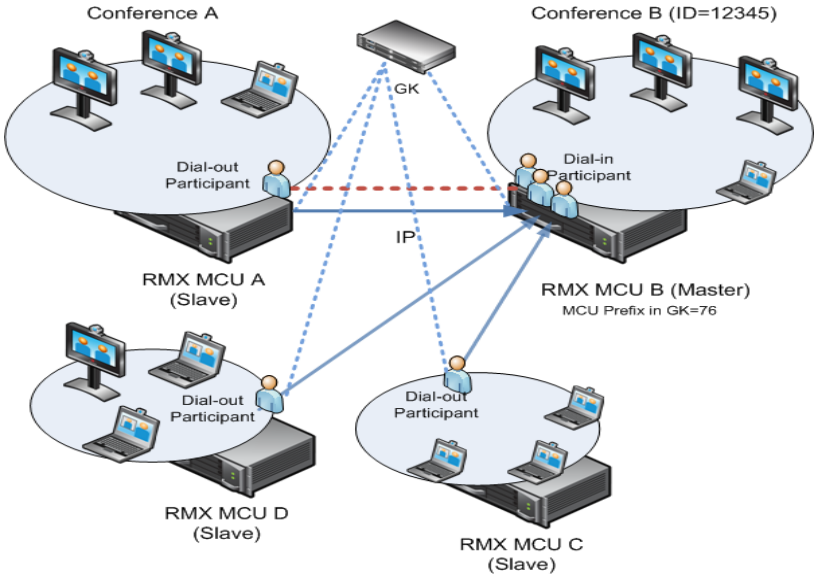
Master-Slave Cascading

It is similar to MIH (Multi Hierarchy) cascading, with only two levels: one Master MCU on level 1 and several Slave MCUs on level 2.

The cascading hierarchy topology can extend to four levels (MIH Cascade - a Sample 3-Level Cascading Configuration) and should be deployed according to the following guidelines:

- If an Collaboration Server is deployed on level 1:
  - Collaboration Server systems can be used on level 2
  - MGC with version 9.0.4 can be used in level 2, if Collaboration Server version 7.0.2 and higher, is deployed in level 1.
- If an MGC is deployed on level 1:
  - MGC or Collaboration Server can be used on level 2.

Master-Slave Star Cascading Topology



- When creating a cascading link between two Collaboration Servers:
  - The Collaboration Servers operate in CP (Continuous Presence) mode.
- When creating a cascading link between MGCs and Collaboration Servers:
  - The MGCs can only operate in VSW mode.

The following table summarizes Video Session Modes line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

MIH Cascading – Video Session Mode and Line Rate

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	Collaboration Server	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	HDX
Level 2	Collaboration Server			
Level 1	Collaboration Server	CP - CIF	768Kb/s, 2Mb/s	VSX
Level 2	Collaboration Server			
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s	HDX, VSX
Level 2	Collaboration Server	CP - CIF 264		
Level 1	MGC	VSW - HD	1.5Mb/s	HDX
Level 2	Collaboration Server	VSW - HD		

To establish the links between two Collaboration Servers requires the following procedures be performed:

- Establish the Master-Slave relationships between the cascaded conferences by defining the dialing direction.
- Create the Master and Slave conferences, defining the appropriate line rate.

- Create a cascade-enabled Dial-out Participant link in the Master conference
- Create a cascade-enabled Dial-in Participant link in the Slave conference.

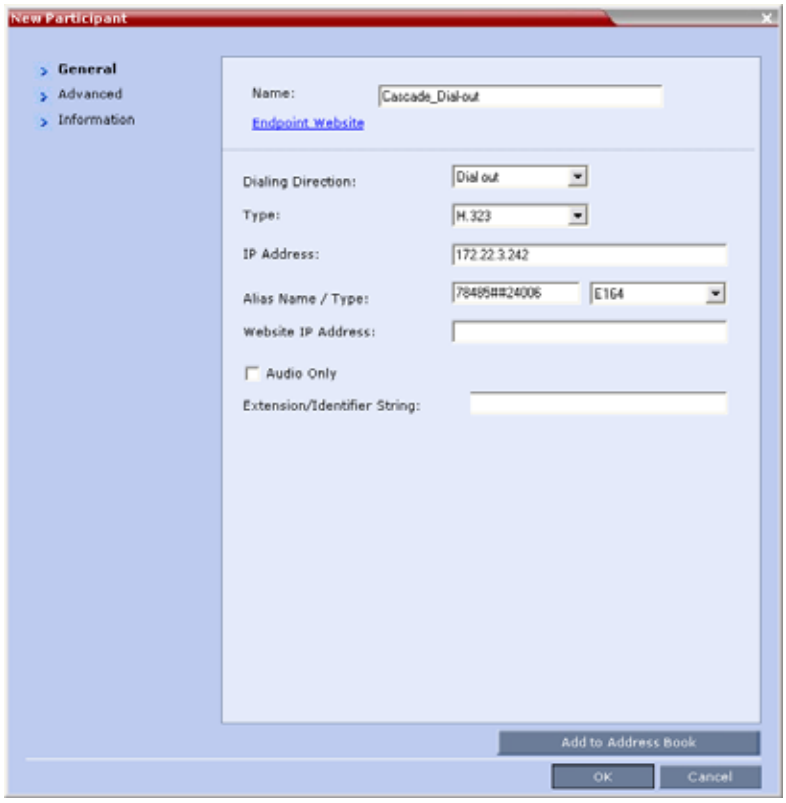
Cascade Enabled Participant Link

The connection between two cascaded conferences is established by a cascade enabled dial-out and dial-in participants, acting as a cascades link.

The dialing direction determines whether the dial-out participant is defined in the conference running on the Master MCU or the Slave MCU. For example, if the dialing direction is from the Master conference on level 1 to the Slave conference on level 2, the dial-out participant is defined in the Master conference on level 1 and a dial-in participant is defined in the Slave 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.

New Participant - General



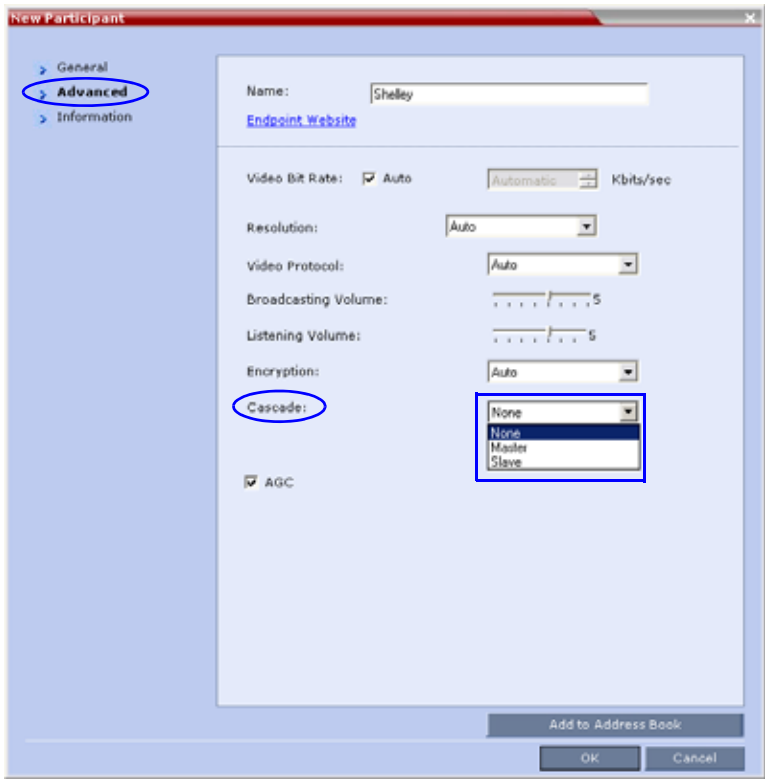
New Participant – Dial-out Cascade Link

Field	Description
Name	Enter the participant's name. This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.

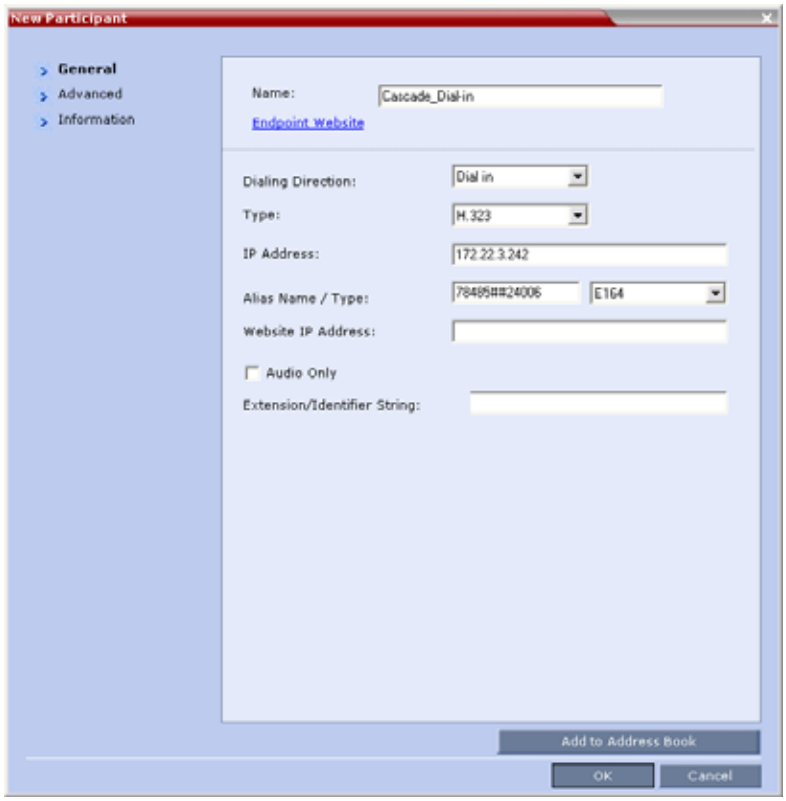
New Participant – Dial-out Cascade Link

Field	Description
Dialing Direction	Select **Dial-out**.
Type	Select **H.323**.
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 are using the target MCU IP address, enter the Conference ID of the target conference. For example: 24006 If a gatekeeper is used, 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: **925**24006 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 do not want to include the password in the dial string, set the **ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD** flag to **YES**. For more information see Modifying System Flags.
Alias Type	Select **E.164** (digits 0-9, *, #).

Advanced tab



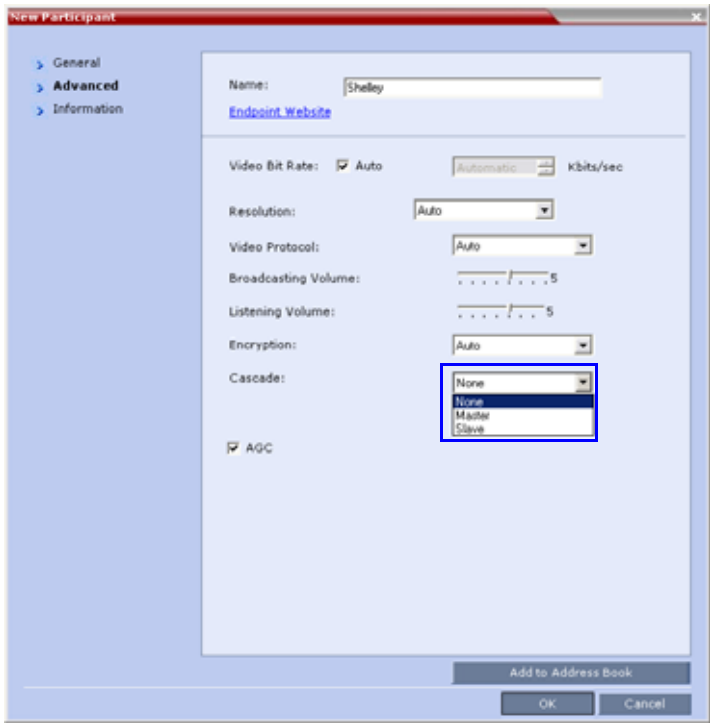
New Participant - General



New Participant – Dial-in Cascade Link

Field	Description
Display Name	Enter the participant's name. This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.
Dialing Direction	Select **Dial-in**.
Type	Select **H.323**.
IP Address	If a gatekeeper is used: This field is left empty. If a gatekeeper is not used: Enter the IP address of the Signaling Host of the MCU running the other conference.
Alias Name	**If a gatekeeper is used:** Enter the name of the other (second) conference. **If a gatekeeper is not used:** Enter the ID of the MCU running the other (second) conference.
Alias Type	If a gatekeeper is used: H.323 ID If a gatekeeper is not used: Select **E.164** (digits 0-9, *, #).

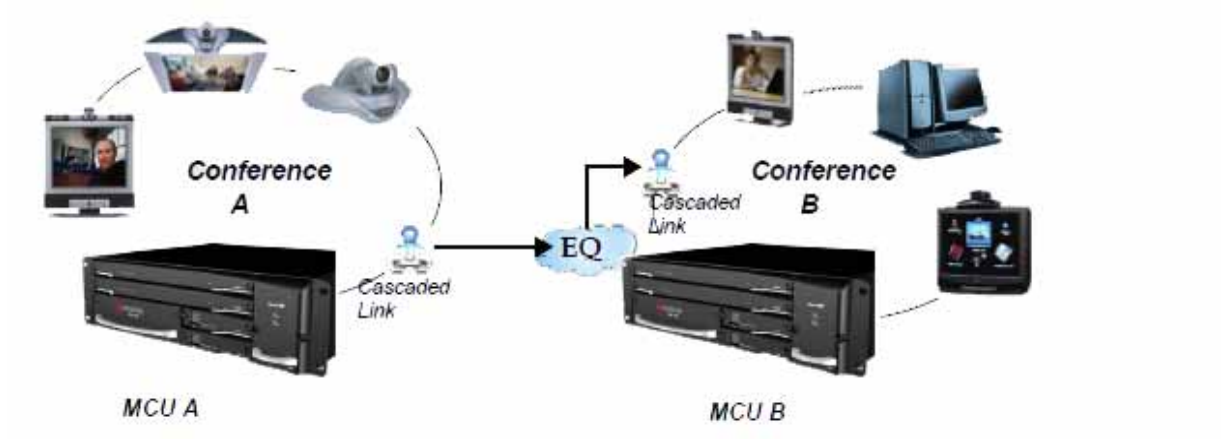
Advanced



Cascading via Entry Queue

The link between the two conferences is created when a participant that is defined as a dial-out cascaded link in one conference (Conference A) connects to the second conference (Conference B) via a special cascaded Entry Queue (EQ). 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.

Cascaded Conferences - Star Topology



Though the process of cascading conferences mentioned in this section refers to conferences running on two different Collaboration Server units, it is possible to cascade conferences running between Collaboration Server units and other MCUs.

The following features are not supported by the cascaded link and therefore are not supported in the combined conference:

- DTMF codes are enabled in cascaded conference, but only in their local conference. The operations executed via DTMF codes are not forwarded between linked conferences.
- FECC (Far End Camera Control will only apply to conferences running in their local MCU).

Enabling Cascading

Cascading two conferences requires that the following procedures are implemented:

- Creating the cascade-enabled Entry Queue

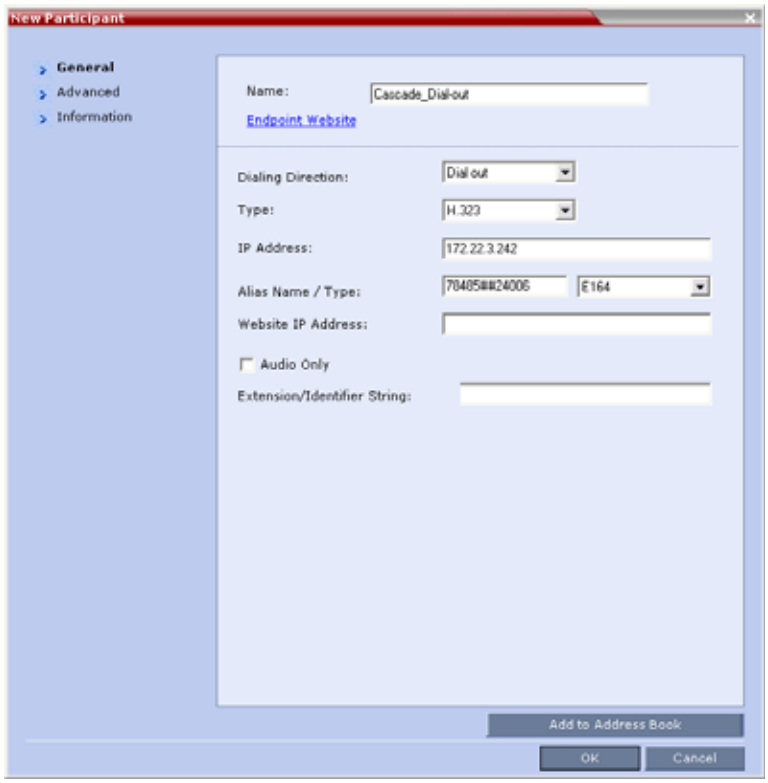
  A cascade-enabled Entry Queue must be created in the MCU hosting the destination conference (Conference B). The cascade-enabled Entry Queue is used to establish the dial-in link between the destination conference and the linked conference and bypassing standard Entry Queue, IVR prompt and video slide display.
- Creating a cascade-enabled Dial-out link

  The creation of 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.
- (Optional) Enabling the cascaded linked participant to connect to the linked conference (Conference A) without entering the conference password. This can be done by modifying the default settings of the relevant system flag.

Creating the Dial-out Cascaded Link

The dial-out link (participant) is created or added in the linked conference (Conference A). The dial-out string defined for the participant is the dialing string required to connect to the destination conference (Conference B) Entry Queue defined on the MCU hosting the destination cascaded conference. The dial-out participant can be defined in the Address Book and added to the conference whenever using the same cascade-enabled Entry Queue and a destination conference (with the same ID and Password).

New Participant - General



There are two methods to define the dialing string:

- Using the MCU's IP Address and the Alias string - Method A.

  Method A

  In this method no gatekeeper is used.

  In the **IP Address** field, enter the IP address of the **Signaling Host** of the MCU hosting the destination conference (in the example, MCU B).

  In the **Alias Name/Type** field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference (MCU B) as follows:

  `<EQ ID>#<Destination Conference ID>#<Password>` (Password is optional).

For Example: 78485#24006#1234

Cascade-enabled EQ ID | Destination Confer | Password (optional)

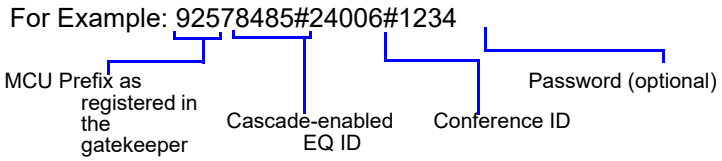
- Using only the Alias string (requires a gatekeeper) - Method B.

  Method B

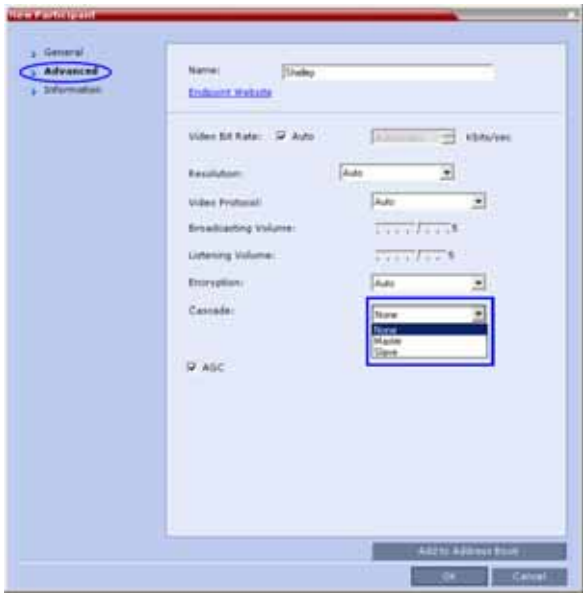
  In this method a gatekeeper is used:

  In the **Alias Name** field, enter the Prefix of MCU B, EQ ID, Destination Conference ID, and Password, as follows:

  `<MCU Prefix EQ ID>#<Conference ID>#<Password>` (Password is optional)



Advanced tab



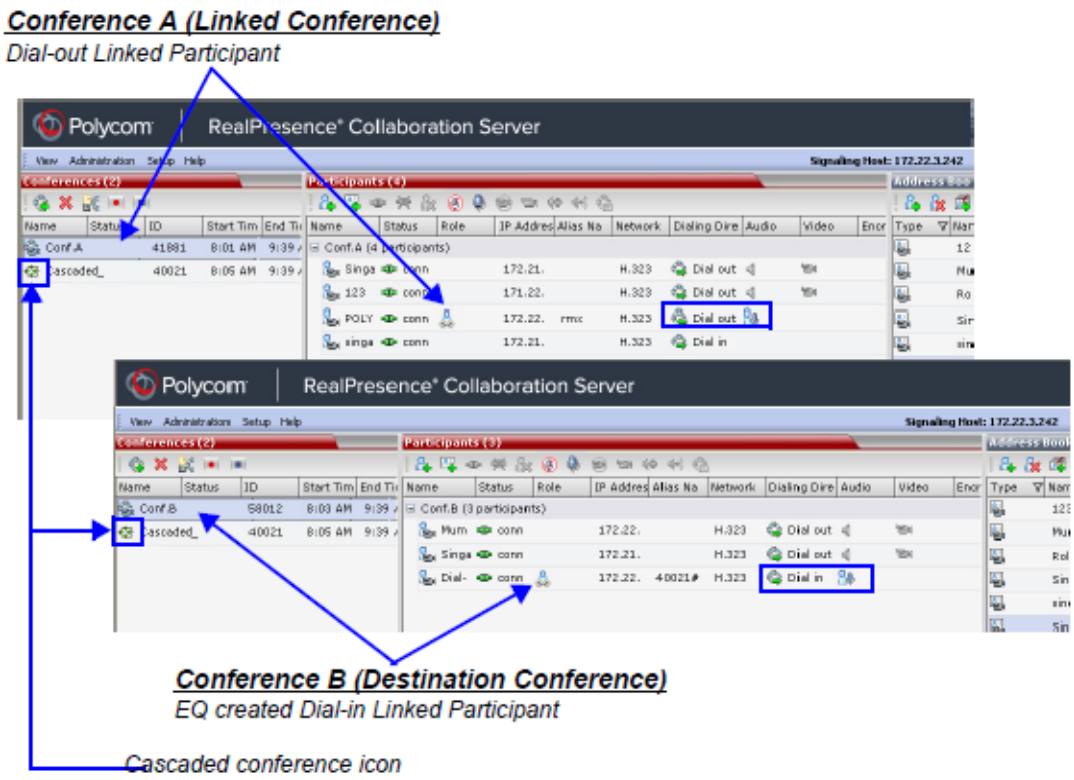
- Slave, if the participant is defined in a conference running on a Slave MCU and will connect to the Master MCU (in the center of the topology).
- Master, if the participant is defined in a conference running on the Master MCU (in the center of the topology) dialing from the Master MCU to the Slave MCU.

Monitoring Star Cascaded Conferences

To monitor both conferences at the same time, two instances of the RMX Web Clients must be opened (one for each MCU) by entering the IP Address of each MCU. If both conferences are running on the same MCU, only one RMX Web Client window is required.

When conferences are cascaded, the Participant List pane of each of the two conferences displays a linked 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 will 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 is displayed for a short duration.



H.239-enabled MIH Topology

Note: Cascading Topology Applicability for Platform
MIH cascading topology is not applicable for Collaboration Server Virtual Edition.

H.239 Multi-Hierarchy (MIH) cascading is available to Collaboration Server users enabling them to run very large conferences on different MCUs in multiple levels of Master-Slave relationships using an H.323 connection.

Multi-Hierarchy (MIH) Cascading is implemented where the cascaded MCUs reside on different networks, whereas Star Topology Cascading requires that all cascaded MCUs reside on the same network.

MIH Cascading allows:

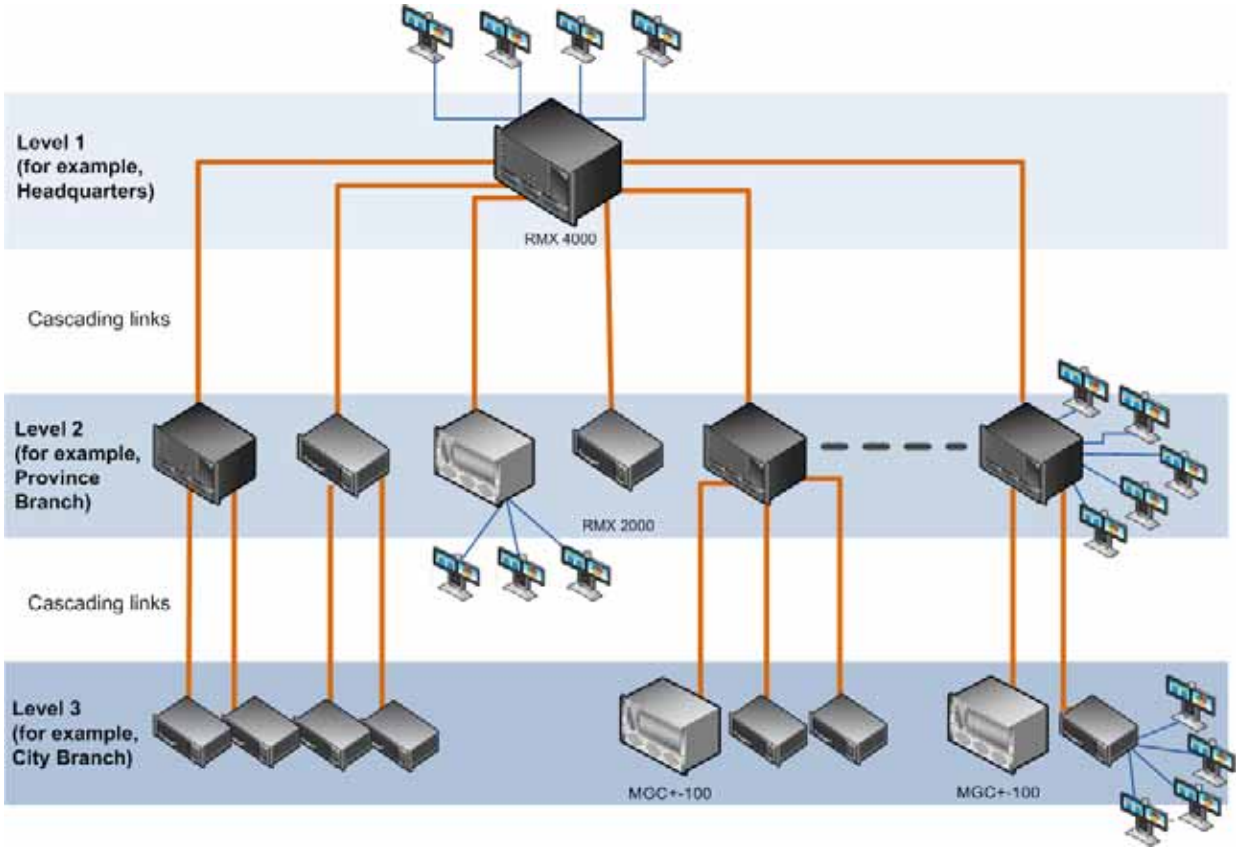
- Opening and using a content channel (H.239) during conferences.
- Full management of extremely large, distributed conferences.
- Connecting conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections, ISDN-video, etc.
- Significant call cost savings to be realized by having participants call local MCUs which in turn call remote MCUs, long distance.

Note: H.323 Cascading Link Requirement
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 (as shown below), where the most common configuration includes up to three levels.

MIH Cascade - a Sample 3-Level Cascading Configuration



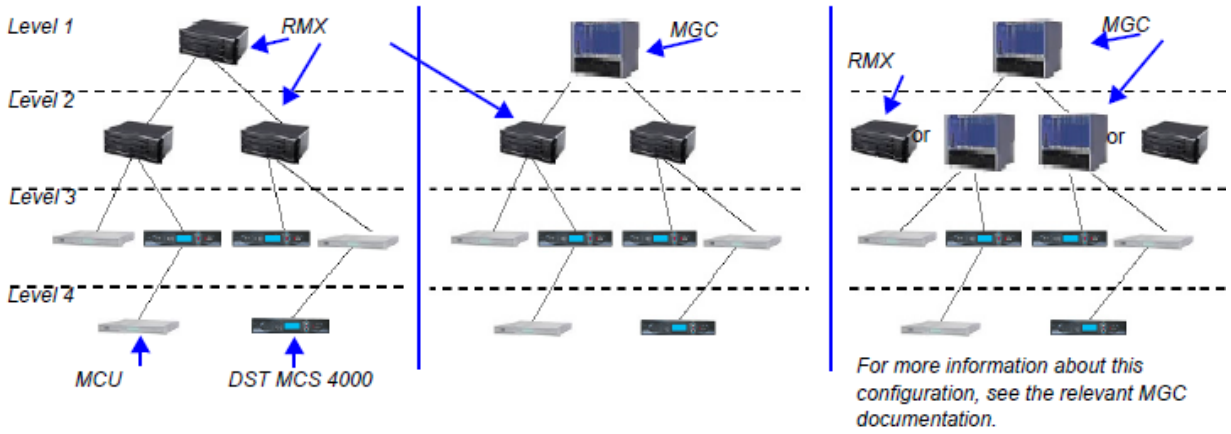
Cascading Topologies

The cascading hierarchy topology should be deployed according to the following guidelines:

- If an RMX is deployed on level 1 (recommended deployment):
  - Any RMX can be used on level 2, 3 and 4 (recommended deployment),
  - MGC version 9.0.4 can be used on level 2 and level 3,
  - DST MCS 4000 and other MCUs can be deployed on levels 3 and 4.
- If an MGC is deployed on level 1:
  - MGC or RMX can be used on level 2.

  - DST MCS 4000 and other MCUs can be deployed on levels 3 and 4.
- DST MCS 4000 MCUs connect as endpoints to the RMXs or MGCs on higher levels.

MIH Cascade Levels

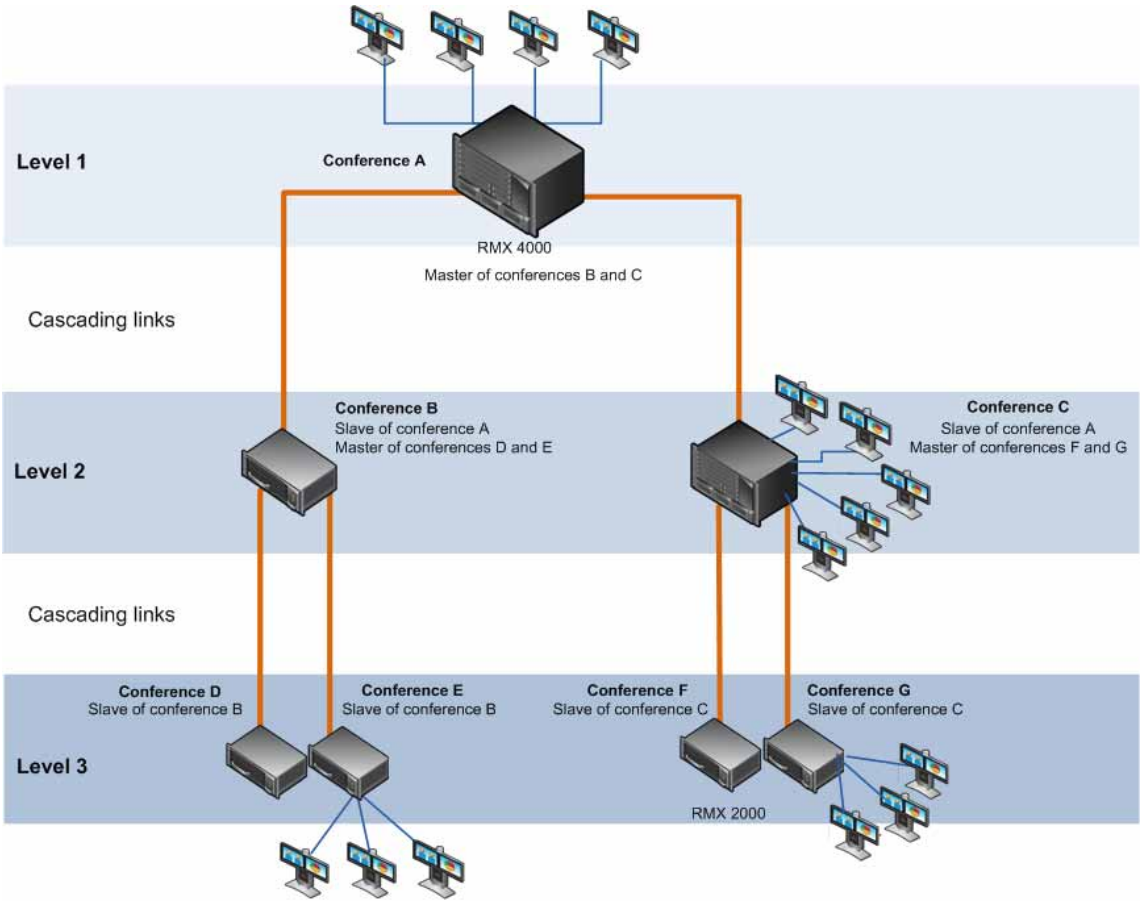


MIH Cascading Guidelines in CP Licensing

Master - Slave Conferences

- It is recommended to have RMX systems at all levels to leverage the high quality video and content offered by the RMX.
- In MIH Cascading conferences, although there are multiple levels of Master and Slave relationships between conferences, the conference that runs on the MCU on level 1 of the hierarchy must be the Master for the entire cascading session. When an MGC is part of the cascading topology, it can be configured at any level if MGC Version 9.0.4 is installed, otherwise, it must be set as Level 1 MCU.
- Conferences running on MCUs on levels 2 and 3 and can be both Masters and Slaves 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 3-level hierarchy configuration) are Slave conferences.
- When the DST MCS 4000 is on level 3 and acting as slave to level 2, the RMX on level 2 must dial out to it in order for the DST MCS 4000 to be identified as slave. The link between the two MCU (dial out participant) is defined as a standard participant and not as a cascading link.

MIH Cascading – Master-Slave 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 RMXs:
  - The RMXs operate in CP (Continuous Presence) mode.
  - DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between MGCs and RMXs:
  - If there are no MGCs on level 2, the MGCs can operate in either in CP or VSW (Video Switching) mode.
  - If there are MGCs on level 2, the MGCs can only operate in VSW mode.
  - MGC does not support H.264 High Profile, therefore when MGC is part of the Cascading topology, do not select High Profile on the RMX system.
  - DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.

- When creating a cascading link between two MGCs the MGCs must be configured to operate in VSW mode.

  For more details about the MGC to MGC connection, see *MGC Manager User's Guide, Volume II, Chapter 1, Ad Hoc Auto Cascading and Cascading Links*.
- To enable the connection of the links between cascaded conferences, they must run at the same line rate.
- To enable Content sharing between the Collaboration Server and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation.

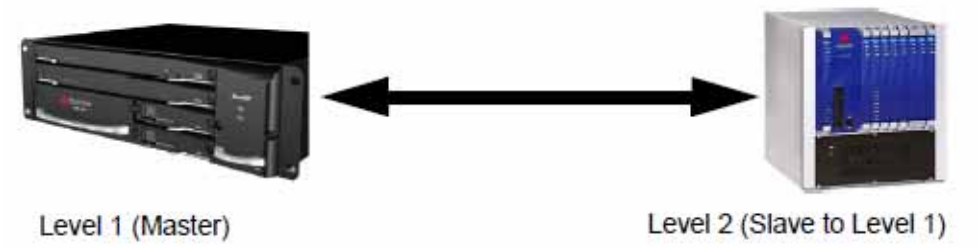
The following table summarizes Video Session Modes line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

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		
Level 1	RMX	CP - CIF	768Kb/s, 2Mb/s
Level 2	RMX		
Level 1	RMX	CP	768Kb/s, 2Mb/s
Level 2	MGC	CP or VSW	
Level 1	MGC	CP - CIF 263	768 kb/s, 2Mb/s
Level 2	RMX	CP - CIF 264	
Level 1	MGC	VSW - HD	1.5Mb/s
Level 2	RMX	VSW HD	
Level 2	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	RMX		
Level 2	MGC	VSW*	384 kbps, 768 kbps
Level 3	MGC		
Level 2	RMX	CP/VSW -HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	MCS 4000		
Level 2	RMX	CP - CIF	768kb/s, 2Mb/s
Level 3	MCS 4000		

* When MGC is on Level 3, Content cannot be shared between Level 2 and Level 3.

MGC to Collaboration Server Cascading



If MGC is running version 9.0.4, and Collaboration Server is running version 7.0.2 and higher, the Collaboration Server can be set as Master on level 1 and MGC as Slave on level 2.

MGC running versions other than 9.0.4 is always on level 1 and must be set as the Master MCU.

If the cascading topology includes additional MGCs as well as Collaboration Servers it is recommended to define Video Switching conferences for all the cascading conferences running on the MGC in the topology.

Two methods can be used to create the Cascading links between conferences running on the Collaboration Server and MGC:

- Method I - Establish the links by defining a dial-in and a dial-out participant in the Slave and Master conference (where the Master conference is created on the MCU on Level 1 and the Slave conference is created on the MCU on Level 2).
- Method II - Using a Cascading Entry Queue on either the MGC or the Collaboration Server depending on the dialing direction and the MCU Level. This is recommended when the Collaboration Server is on Level 1.

Method I

Depending on the dialing direction, the following procedures must be performed:

Set up Procedures according to the Dialing Direction

Dialing Direction	Collaboration Server - Level 1	MGC - Level 2
MGC to Collaboration Server	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-in participant (Cascaded Link) with the calling number from the MGC. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference. Set the Cascading option as Master.	Define the dial-out participant (Cascaded Link) to the conference running on the Collaboration Server. Set the dial-out alias to be the prefix of the MCU and the name of the master conference running on the Collaboration Server.

Set up Procedures according to the Dialing Direction

Dialing Direction	Collaboration Server - Level 1	MGC - Level 2
Collaboration Server to MGC	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link). Set the dial-out alias to be the prefix of the MGC and the name of the slave conference running on the MGC. Set the Cascading option as Master.	Define the dial-in participant (Cascaded Link) to the conference running on the Collaboration Server. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference.

For details on the participant definition on the Collaboration Server, see Cascade Enabled Participant Link.

For a detailed description of the participant definition in the MGC, see the *MGC Manager User's Guide, Volume II, Chapter 1, Cascading Conferences*.

Note: Content Sharing between MGC and Collaboration Server
To enable Content sharing between the Collaboration Server and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation.

Method II

Depending on the dialing direction, the following procedures must be performed:

Set up Procedures according to the Dialing Direction

Dialing Direction	MGC Level 1	RealPresence Collaboration Server (RMX) 1800/2000/4000 Level 2
MGC to Collaboration Server	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
		Define the cascade-enabled Entry Queue, setting it as **Slave**.
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link) to the conference running on the Collaboration Server.	

Set up Procedures according to the Dialing Direction

Dialing Direction	MGC Level 1	RealPresence Collaboration Server (RMX) 1800/2000/4000 Level 2
Collaboration Server to MGC	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
	Define the cascade-enabled Entry Queue.	
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
		Define the dial-out participant (Cascaded Link) to the conference running on the MGC, setting the participant Cascade parameter to **Slave**.

User Management

This section provides an introduction to the user management options, functionality, and operations associated with the RealPresence Collaboration Server. It includes these topics:

- User Roles and Permissions
- Managing Users

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.

This 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.
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.
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 Files and audit the system.

Managing Users

Only users assigned the administrator role can manage RealPresence Collaboration Server users. Some of these management tasks include:

- View the List of Current Users
- Add a User
- Edit a User
- Delete a User
- Enable a User
- Disable a User
- Rename a User
- Add a Machine Account

These tasks are documented in the following sections.

View the List of Current Users

The **Users** pane lists the currently defined users in the system.

To view the user list:

» In the RMX ***Management*** pane, click **(Users)**.

The displayed User list includes these columns:

Column	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.

To add a user:

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.

To edit a user's account information:

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:
The last remaining Administrator in the **Users** list cannot be deleted.

To delete a user's account:

1 In the RMX ***Management*** pane, click **(Users)**.
2 In the **Users** list, select the user, and click **Delete** ( ).
3 In the ***confirmation*** dialog, select **Yes** to confirm the deletion.

Change a User's Password

Administrators can change their own passwords and other users' passwords. Operators can change their own passwords.

To change a user's password:

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.

To disable a user:

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.

To enable a user:

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.

To rename a user:

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.

To add a machine account:

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.

To view the current MCU Connections:

» 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.

Address Book

Use the RealPresence Collaboration Server (RMX) Address Book to store information about conference participants and quickly and efficiently include Address Book participants in conferences.

IMPORTANT:

If you have a Polycom® RealPresence® Resource Manager system, integrate your RealPresence Collaboration Server with it and manage users and conference participants in the RealPresence Resource Manager system rather than the MCU.

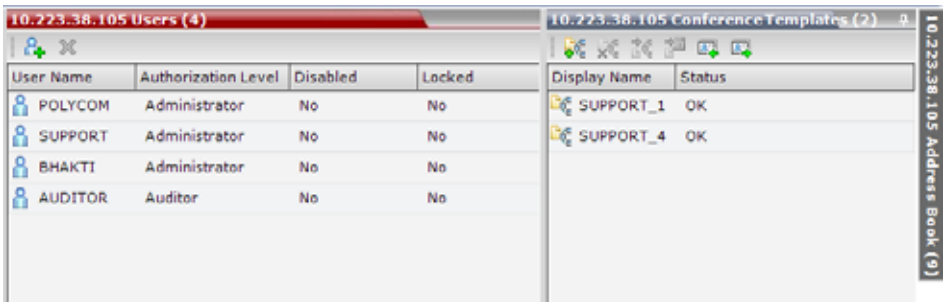
The RealPresence Resource Manager system allows you to manage all registered endpoints be they associated with LDAP users or local Global Address Book (GAB) users. RMX can be integrated with the RealPresence Resource Manager Global Address Book.

Integration with the Global Address Book is not supported by RealPresence Collaboration Server (RMX) 1800 with no DSP cards.

To fetch the Address Book from a RealPresence Resource Manager system over a secure connection, you must use RMX Manager.

Viewing the Address Book

On first access, the RMX **Address Book** appears in the main **RMX Manager** pane. If it is hidden, double-click the **Address Book** tab on the right to unhide it.



Adding a Group to the Address Book

To add a group to the Address Book:

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**.
3. To add an existing participant to the group:
   a. Select the participant from the participant list.
   b. Right click and select **Copy Participant**.
   c. Select the group from the group list.
   d. Right click and select **Paste Participant** or **Paste Participant as New**.
   e. If you selected the **Paste Participant as New** option, select and enter the properties you wish to define.
      - ♦ General Participant Properties
      - ♦ Advanced Participant Properties
   f. Click **OK**.
4. To add a new participant to the group:
   a. Select the group from the list.
   b. Right click and select New Participant.
   c. Enter the New Participant information required. For more information, see
   d. Click OK.

Adding a New Participant to the Address Book

Adding participants to the Address Book can be performed by the following methods:

- Directly in the Address Book.
- Moving or saving a participant from an ongoing conference to the Address Book.

To add a new participant directly to the Address Book:

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.
   - ➢ General Participant Properties
   - ➢ Advanced Participant Properties
4. To add general information about the participant, such as e-mail address or company name, click **Information** and enter the necessary details in the **Info 1-4** fields.
5. Click **OK**.

Participant Properties

The following tables list the conference parameters 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. The maximum field length for the Display Name is: • 80 ASCII characters. • 40 European and Latin text characters • 25 Asian text characters Do not use comma or semi-colon characters in this field. This name may be displayed in the video layout.
Endpoint Website	Hyperlink that connects to the internal website of the participant's endpoint, which allows 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 participant enter either the endpoint IP address or the endpoint Alias. • For SIP participant enter either the endpoint IP address or the endpoint SIP address. For Collaboration Servers registered to a gatekeeper, the MCU can be configured to dial and receive calls to and from H.323 endpoints using the IP address in the event that the Gatekeeper is not functioning.

General Participant Properties

Field	Description
Alias Name/Type (H.323 Only)	Select the type of Alias for the endpoint (based on communication protocol) and then enter the endpoint's alias: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Notes:** • 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. • This field is used to enter the Entry Queue ID, target Conference ID and Conference Password when defining a cascaded link. • Use of the E.164 Number is dependent on the setting of the REMOVE_IP_IF_NUMBER_EXISTS System Flag.
SIP Address/Type (SIP Only)	Select the format of the SIP address and then enter the endpoint's SIP Address. : • **SIP URI** - Uses the format of an E-mail address, typically containing a user name and a host name: sip:[user]@[host]. For example, sip:dan@polycom.com. **Note:** If the SIP Address field contains an IPv6 address, it must be surrounded by square brackets, for example, [::1]. • **TEL URI** - Used when the endpoint does not specify the domain that should interpret a telephone number that has been input by the user. Rather, each domain through which the request passes would be given that opportunity. For example, a user in an airport might log in and send requests through an outbound proxy in the airport. If the users enters "411" (this is the phone number for local directory assistance in the United States), this number needs to be interpreted and processed by the outbound proxy in the airport, and not by the user's home domain. In this case, tel: 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 Collaboration Server. If the field is blank it can be manually completed by the system administrator. The field can be modified while the endpoint is connected

General Participant Properties

Field	Description
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. 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** - enter the required string using the digits 0-9 and the characters * and #. The maximum number of characters that can be entered is identical to the H.323 alias length. If the information required to access the device/conference is composed of several strings, for example, the conference ID and the conference password, this information can be entered as one string, where pauses [p] are added between the strings for the required delays, as follows: **[p]…[p][string][p]…[p] [string]...** For example: p23pp*34p4566# The Collaboration Server automatically sends this information upon connection to the destination device/conference. The information is sent by the Collaboration Server as DTMF code to the destination device/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:** This check box cannot be cleared 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	Select the video compression standard that will be forced by the MCU 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	To adjust the volume the participant broadcasts to the conference or the volume the participant hears the conference, move the slider; each unit represents an increase or decrease of 3 dB (decibel). The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5.

Advanced Participant Properties

Field	Description
Encryption	Select whether the endpoint uses encryption for its connection to the conference. ***Auto*** (default setting) indicates that the endpoint will connect according to the conference encryption setting.
AGC	AGC (Auto Gain Control) 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. Notes: • To be enable AGC, set the value of the **ENABLE_AGC** System Flag in *system.cfg* to **YES**. The flag's default value is NO. • If the System Flag does not exist in the system, it must be manually added to the System Configuration. For information see System Flags . • Enabling AGC may result in amplification of background noise.
Cascaded **(IP Only)**	If this participant is used as a link between conferences select: • **Slave**, if the participant is defined in a conference running on a Slave MCU. • **Master**, if the participant is defined in a conference running on the Master MCU. It 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 MCU's. For more information, see Basic Cascading .

Adding 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.

In SVC-based conferences, only dial-in participants can be added from the address book.

Note: Multiple selection
Multiple selection of group levels is not available.

To add a participant or group to a new conference or an ongoing conference:

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

Editing a Participant's Address Book Information

When required, you can edit a participant's Address Book information or properties.

To edit a participant ‘s Address Book information:

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.
   - General Participant Properties
   - Advanced Participant Properties
5. Click **OK**.

Deleting a Participant from the Address Book

To delete participants from the Address Book:

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. Click **Delete Participant** ( ) or right-click and select **Delete Participant**.

   A confirmation message is displayed depending on the participant’s assignment to groups in the address book:
   - When the participant belongs to only one group: click **Yes** to permanently delete the participant from the address book.
   - When the participant belongs to multiple groups, a message is displayed requesting whether to delete the participant from the Address Book or from the current selected group.
5. Select **Current group** to delete the participant from the selected group or **Address Book** to permanently delete the participant from all groups in the address book.
6. Click **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 are not available when selecting multiple participants.

A participant can belong to multiple groups; however, there is 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.

Filtering 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:

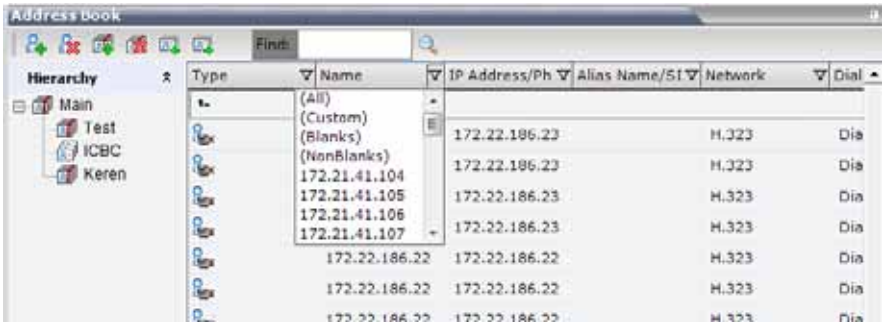
- A predefined pattern
- Customized pattern

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

To filter the Address Book:

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 column(s) by which to filter.
7. To clear a filter, click **Filter** (▽) for the column from which filtering is to be removed and select **All**.

Exporting an Address Book

If your environment includes multiple MCUs, you will likely want all MCUs to use the same Address Book. The RealPresence Collaboration Server allows you to export the Address Book from one MCU as a single proprietary formatted XML file and import it to other MCUs.

To export an Address Book:

1. In RMX Manager, click **Address Book**.
2. Click **Export Address Book** ( ) and **Browse** to the location to which to save the exported file.
3. In the **File Name** field, enter a name for the exported file. If no name is assigned to the exported Address Book, the default file name is EMA.DataObjects.OfflineTemplates.AddressbookContent_.xml
4. Click **Save** and then click **OK**.

Importing an Address Book

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

- Creates a new multi-level 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 were not 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).

To Import an Address Book:

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

   Note: Imported participants
   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**.

Operator Conference and Assistance

Note: Chapter Applicability to CP Only Conferencing Mode
Operator conferences and participant move are supported in AVC CP Conferencing Mode only.

An Operator conference is a special conference that enables the 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.

In attended mode, the 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 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.

Operator Conference Guidelines

- 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
- Once running, the 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. For move guidelines, see Move Guidelines.
- 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.

Defining Components Prerequisite for Operator Assistance

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.

To define a Conference IVR Service with Operator Assistance Options:

1 In the **RMX Management** pane, expand the **Rarely Used** list and select **IVR Services**.

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. For more information, see Conference IVR Service Properties - Global Parameters.

5 Open the **Welcome** tab.

6 Define the system behavior when the participant enters the Conference IVR queue. For more information, see Defining a New Conference IVR Service.

7 Open the **Conference Chairperson** tab.

8 If required, enable the chairperson functionality and select the various voice messages and options for the chairperson connection. For more information, see New Conference IVR Service Properties - Conference Chairperson Options and Messages.

9 Open the **Conference Password** tab.

10 If required, enable the request for conference password before moving the participant from the conference IVR queue to the conference and set the MCU behavior for password request for Dial-in and Dial-out participant connections. For more information, see New Conference IVR Service Properties - Conference Password Parameters.

11 Select the various audio messages to play in each scenario. For more information, see For more information, see New Conference IVR Service Properties - Conference Password Parameters.

12 Open the **General** tab.

13 Select the messages to play during the conference. For more information, see Conference IVR Service Properties - General Voice Messages.

14 Open the **Roll Call/Notifications** tab.

15 Enable the Roll Call feature and assign the appropriate audio file to each message type. For more information, see Conference IVR Service Properties - Roll Call Messages.

16 Open the **Video Services** tab.

17 Define the **Video Services** parameters. For more information, see New Conference IVR Service Properties - Video Services Parameters.

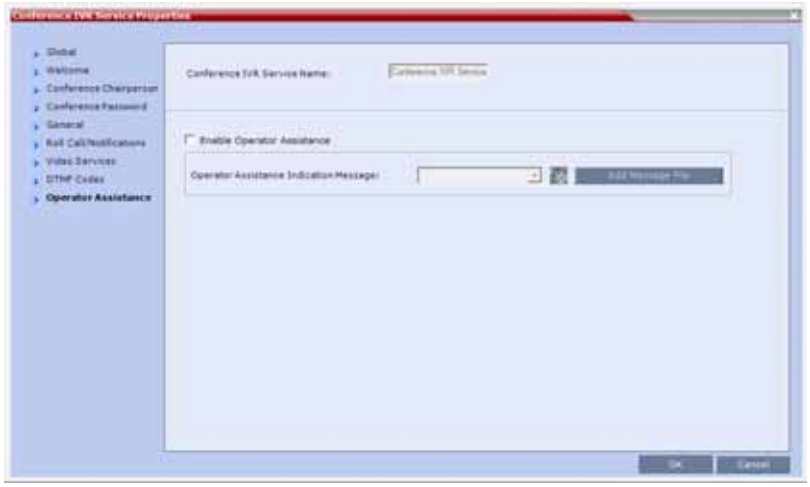
18 Open the **DTMF Codes** tab.

The default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson are listed. For the full list of the available DTMF codes, see New Conference IVR Service Properties - DTMF Codes.

19 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.

20 Open the **Operator Assistance** tab.



21 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.

22 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: Audio files
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 Collaboration Server.

23 Click **OK** to complete the IVR Service definition.

The new Conference IVR Service is added to the **IVR Services** list.

To define an Entry Queue IVR Service with Operator Assistance Options:

1 In the RMX Management pane, select **IVR Services**.
2 In the IVR Services list, click the **New Entry Queue IVR Service** but**ton**.
3 Define the Entry Queue Service **Name**.
4 Define the Entry Queue IVR Service Global parameters. For more information, see Conference IVR Service Properties - 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. For more information, see Entry Queue IVR Service Properties - Conference ID.
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.

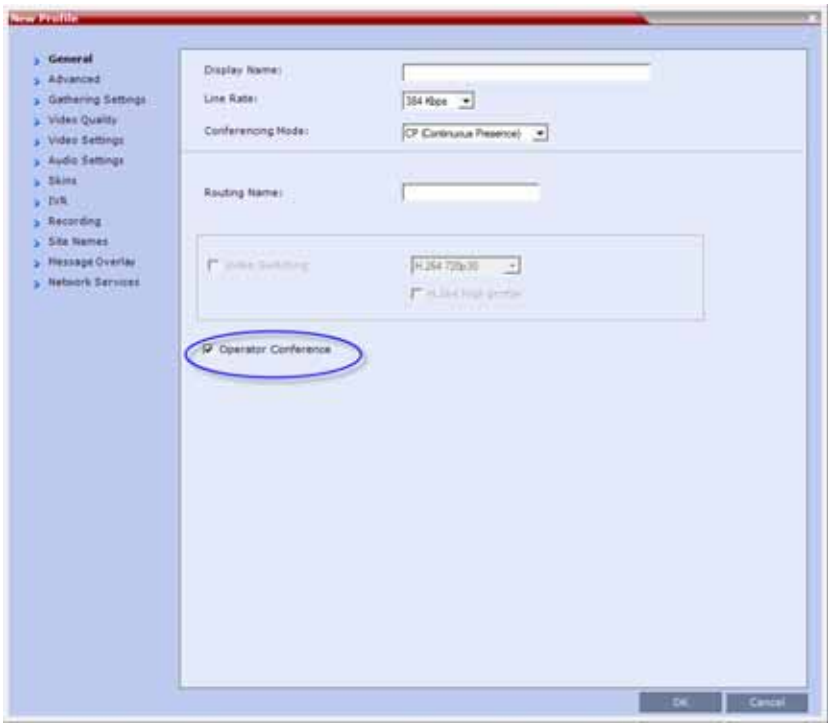
12 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.
13 In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

Note: Audio files
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 Collaboration Server.

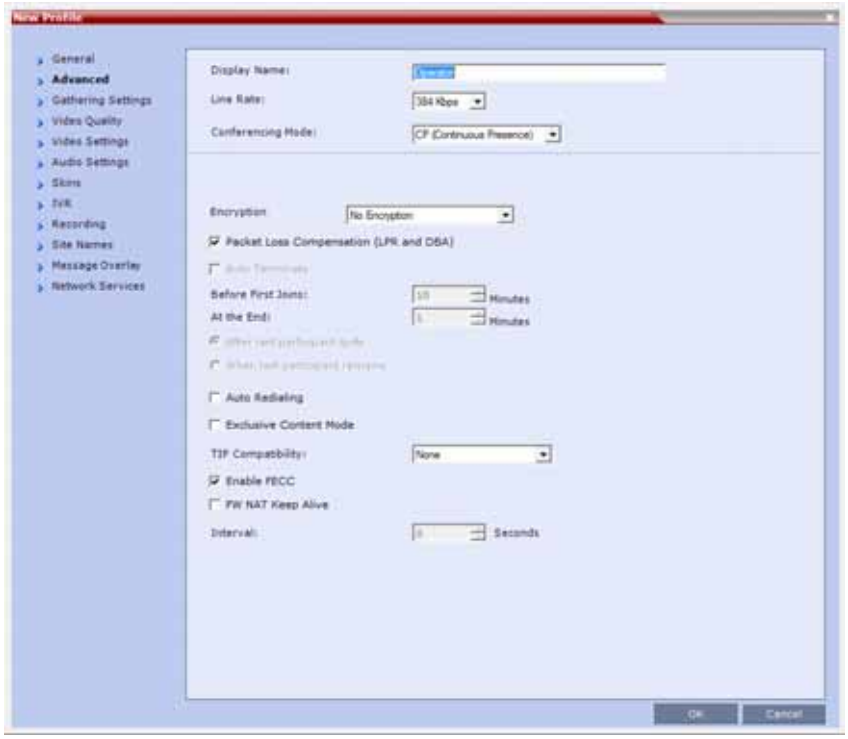
14 Click **OK** to complete the Entry Queue IVR Service definition.
The new Entry Queue IVR Service is added to the **IVR Services** list.

To define a Conference Profile for an Operator Conference:

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.
For more details, see New AVC CP Profile - General Parameters.
4 Select the **Operator Conference** check box.



5 Open the **Advanced** tab.



6 Define the **Profile - Advanced** parameters. For more details, see New AVC CP Profile - Advanced Parameters.

   Note that when Operator Conference is selected, the **Auto Terminate** selection is automatically cleared and disabled and the Operator conference cannot automatically end unless it is terminated by the Collaboration Server User.

7 Open the **Video Quality** tab.

8 Define the Video Quality parameters. For more details, see New AVC CP Profile - Video Quality Parameters.

9 Open the **Video Settings** tab.

10 Define the video display mode and layout. For more details, see New AVC CP Profile - Video Settings Parameters.

11 Define the remaining Profile parameters. For more details, see Defining AVC CP Conferencing Profiles.

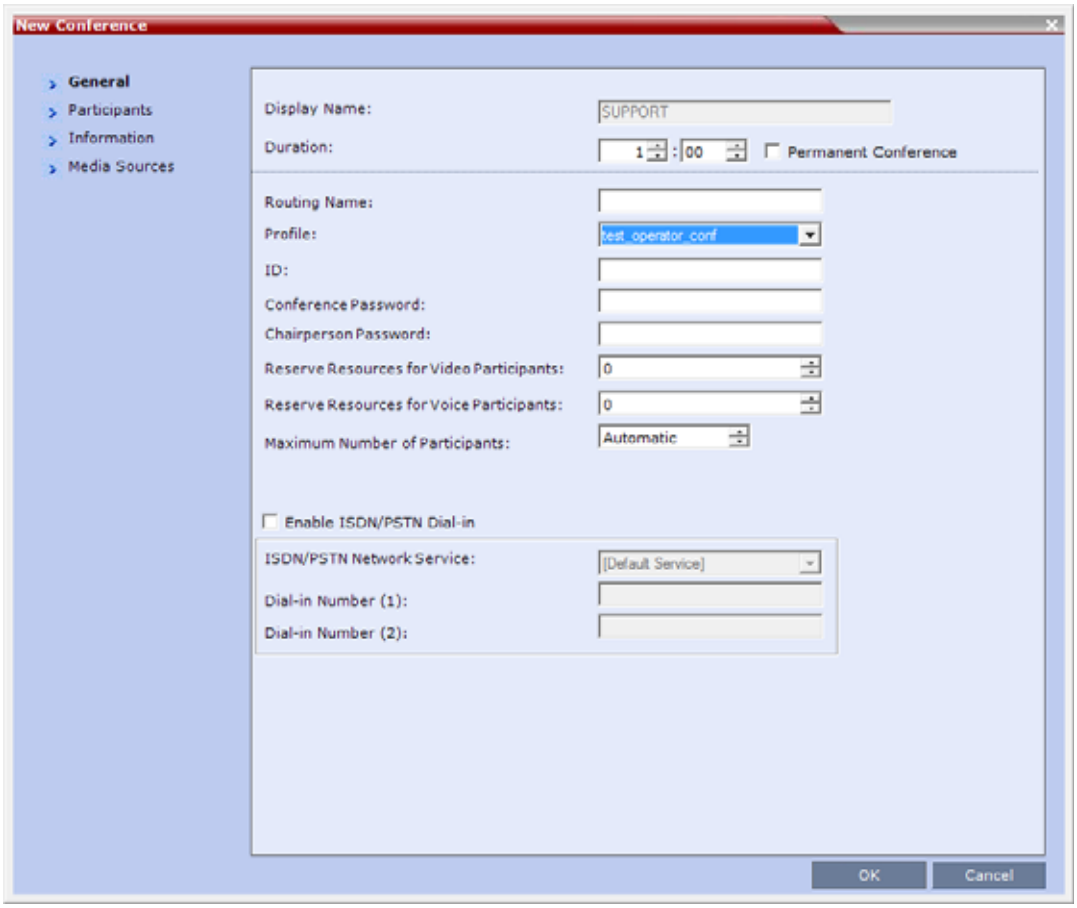
12 Click **OK** to complete the Profile definition.

   A new Profile is created and added to the Conference Profiles list.

To start a conference from the Conference pane:

1 In the **Conferences** pane, click **New Conference**.

2 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 Collaboration Server User Login Name. This name cannot be modified.

Only one Operator conference can be created for each User Login name.

3 Define the following parameters:

New Conference – General Options

Field	Description
Duration	Define the duration of the conference in hours using the format HH:MM (default 01:00). Notes: • 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.

New Conference – General Options

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 is 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 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 is 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 is not supported with Collaboration Server 1800.
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 is 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 is not supported with 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). Maximum number of participants that can connect to an Operator conference:

New Conference – General Options

Field	Description
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 enable 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.

4 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 Collaboration Server User to connect to the Operator conference and to other conference to assist participants.

For more information see Participants Tab.

5 To insert general information, open the **Information** tab.

The **Information** dialog opens.

6 Enter the required information. For more information, see Information Tab.

7 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.

Saving an Operator Conference to a Template

The Operator conference that is ongoing can be saved as a template.

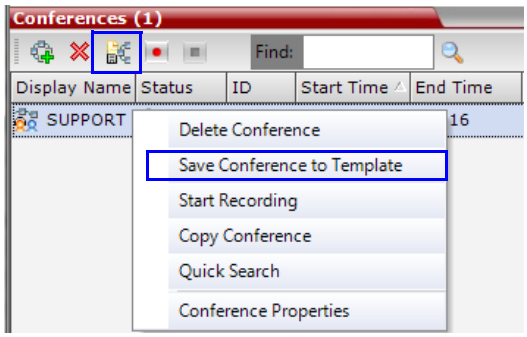
To save an ongoing Operator conference as a template:

1 In the Conferences list, select the Operator conference you want to save as a Template.

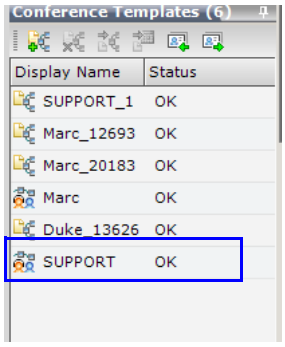
2 Click Save Conference to Template.

or

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 Collaboration Server User). The Template is displayed with the Operator Conference icon.



Starting an Operator Conference from a Template

An ongoing Operator conference can be started from an Operator Template saved in the **Conference Templates** list.

To start an ongoing Operator conference from an Operator Template:

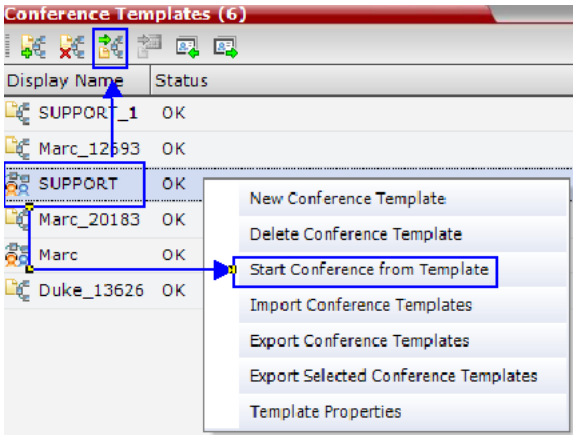
1 In the **Conference Templates** list, select the Operator Template to start as an ongoing Operator conference.

Note: Login Name
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 cannot start another Operator conference with the same login name.

2 Click Start Conference from Template.

or

Right-click and select **Start Conference from Template**.



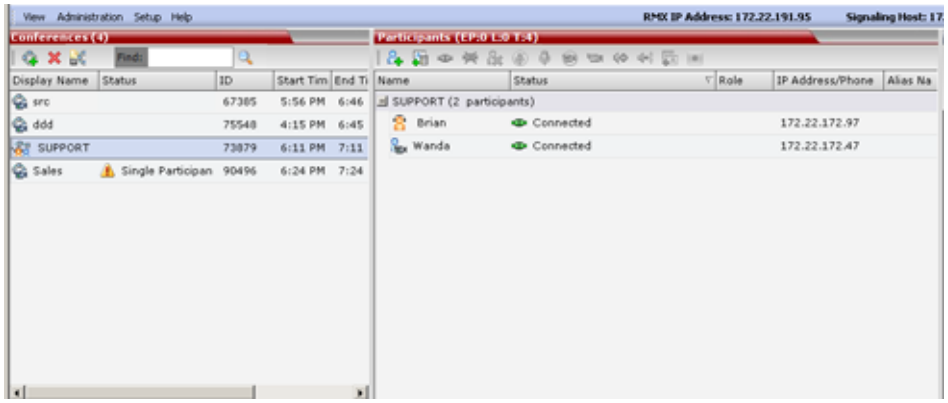
The conference is started.

The name of the ongoing conference in the **Conferences** list is taken from the Conference Template Display Name.

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.



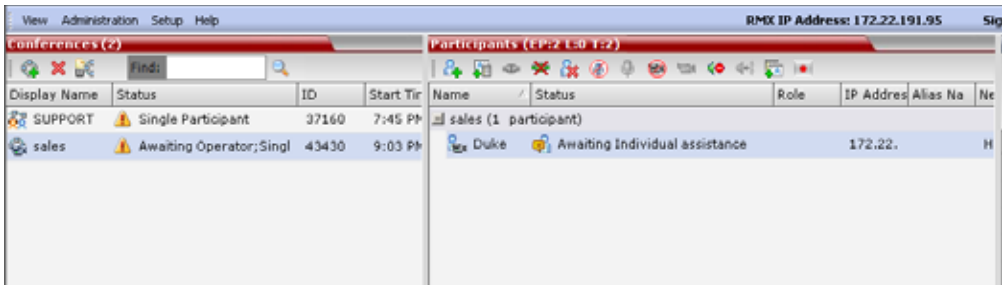
You can view the properties of the Operator conference by double-clicking the conference entry in the Conferences list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see Participant Level Monitoring.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request **Individual Assistance** (default DTMF code ***0**) or **Conference Assistance** (default DTMF code **00**).

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).

When requiring or requesting operator assistance, the Collaboration Server management application displays the following:



- The participant's connection Status changes, reflecting the help request. For more information, see Participants List Status Column Icons and Indications.
- The conference status changes and it is 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.

The following icons and statuses are displayed in the **Participant Status** column:

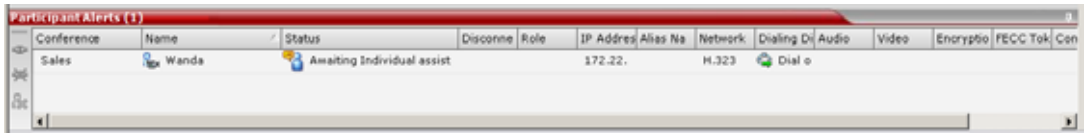
Participants List Status Column Icons and Indications

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.

When the Operator moves the participant to the Operator conference for individual assistance the participant Status indications are cleared.

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 are awaiting assistance.

The participants are automatically removed from the **Participant Alerts** list when moved to any conference (including the Operator conference).

Audible Alarm for Notifying on Required Assistance

An audible alarm can be activated and played when participants request Operator Assistance.

For more details on Audible alarms and their configuration, see Audible Alarms.

Administration and Utilities

This section describes the tasks that you may need to administer and maintain the Polycom RealPresence Collaboration Server.

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.

Viewing 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.

To view the System Alerts list:

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.

Active Alarms Pane Columns

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 (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**.

Viewing 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.

To view the Participants Alerts list:

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. For more information, see Participant Level Monitoring.

2. To resolve participant issues that created the Participant Alerts, the administrator can either **Connect** , **Disconnect** or **Delete** a participant.

Note: Delay Following Restart

Following MCU reset, a delay may occur when synchronizing with the external NTP 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 RealPresence Resource Manager, and Polycom RealPresence DMA System

Forcing 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 Collaboration Server and, if applicable, the Collaboration Server will connect it using one CIF resource, even if a higher resolution can be used.

To force CIF resources:

1. In RMX Manager, go to **System Configuration**.
2. Add a new flag by the name: FORCE_CIF_PORT_ALLOCATION. For information on adding system flags, see Add a System Flag.
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.

To cancel forcing of CIF resource:

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.

Viewing 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 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 *

Resource Capacity Allocation Per Port Type

Port Type	Non-Mixed Conferences	Mixed CP and SVC Conferences
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.

To view the Resource Report:

» In RMX Manager, go to **Administration > Resource Report**.

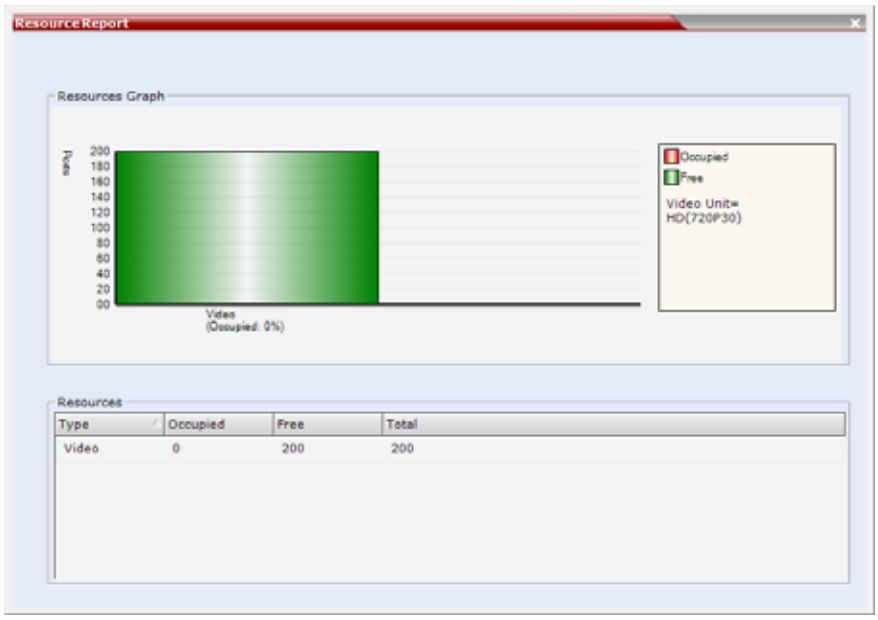
For each resource type, the Resource Report includes the following columns:

Resource Report Fields Parameters

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.

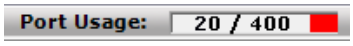
Resource Reports for Collaboration Servers 1800/2000/4000

Collaboration Servers 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.



Setting the Port Usage Threshold

The 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 Collaboration Server:

- The total number of *Video* ports in the system.
- The number of *Video* ports in use.
- The *High Port Usage* threshold.

To set the Port Usage Threshold:

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.

To view the System Information properties box:

- In RMX Manager, go to **Administration > System Information**.

  The following information is displayed:

System Information

Field	Description
Card Configuration Mode *(Collaboration Servers 2000/4000)*	The MCU configuration as derived from the installed media cards: • MPMRx - Currently only MPMRx cards are supported.
RMX Version	The Collaboration Server Software Version.
Serial Number	The Serial Number of the 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 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.

To enable the SNMP option:

1 In RMX Manager, go to **Setup > SNMP**.

The **RMX SNMP Properties - Agent** dialog is displayed.

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.

The **Retrieve MIB Files** dialog is displayed.

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.

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:

SNMPv3 - Traps

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.

SNMPv3 - Traps

Field	Description		
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**.	
	Privacy Protocol	Enter the privacy protocol: **DES** or **AES**.	
	Engine ID	Enter an Engine ID to be used for both the Agent and the Trap. Default: Empty	

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:

SNMPv3 - Traps

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.	
Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	1, 2

SNMPv3 - Traps

Field	Description	Version
User Name	Enter the name of the user who is to have access to the trap.	3
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	
Security Level	Select a ***Security Level*** from the drop-down menu. Range: **No Auth, No Priv**; **Auth, No Priv**; **Auth, Priv** Default: **Auth, Priv**	
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.	
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.	
Privacy Password		

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.

a 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		
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.		
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.		
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.		
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**		
Authentication Protocol	Select the authentication protocol Range: **MD5**, **SHA** Default: **MD5**	These fields are enabled if **Authentication** is selected in the **Security Level** field.	
Authentication Password	Enter an Authentication Password. Range: 8 - 48 characters Default: Empty		
Privacy Protocol	Select a Privacy Protocol. Range: **DES**, **AES** Default: **DES**	These fields are enabled if **Privacy** is selected in the **Security Level** field.	
Privacy Password	Enter a Privacy Password. Range: 8 - 48 characters Default: Empty		
Engine ID	Enter an Engine ID to be used for both the Agent and the Trap. Default: Empty		

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 from Unlisted Terminals

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**.

Hot Backup

Hot Backup implements a high availability and rapid recovery solution.

Two Collaboration Server's are configured in a Master/Slave relationship: the Master MCU is active while the Slave acts as a passive, fully redundant Hot Backup of the Master MCU.

All conferencing activities and configuration changes that do not require a System Reset are mirrored on the Slave MCU five seconds after they occur on the Master MCU.

In the event of failure of the Master MCU, the Slave MCU transparently becomes active and assumes the activities and functions with the backed up settings of the failed Master MCU.

In **AVC-based conferencing,** 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.

In **SVC-based conferencing**, since dial-out is unavailable, SVC-enabled endpoints will have to manually reconnect to the conference.

The following entities are automatically backed up and updated on the Slave 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 Master and Slave MCUs must have the same software version installed.
- The Users list and Passwords must be the same on both the Master and Slave MCUs.
- There must be connectivity between the Master and Slave MCUs, either on the same network or on different networks connected through routers.
- In the event of failure of the Master MCU the Slave MCU assumes the role of the Master MCU. The Master/Slave relationship is reversed: the Slave, now active, remains the Master and the previous Master MCU, when restarted, assumes the role of Slave MCU.
- No changes to the Slave MCU are permitted while it is functioning as the Hot Backup. Therefore no ongoing conferences or reservations can be added manually to the Slave MCU.
- If Hot Backup is disabled, all ongoing conferences and Reservations backed up on the Slave 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 Master Collaboration Server are not backed up in the Slave Collaboration Server.
- Master and Slave initial roles can be reversed only after all ongoing conferences and Reservations are deleted.
- Changes to the Master MCU that require a System Reset can only be made after Hot Backup is disabled.
- Collaboration Server 2000/4000 only: Video/Voice Port Configurations on the Master MCU are not synchronized with the Slave MCU. You must manually set the Video/Voice Port Configurations on both the Master and Slave MCUs to the same level.

Enabling Hot Backup

To enable Hot Backup:

1 In RMX Manager, go to **Setup > Hot Backup**.

The **Hot Backup** dialog is displayed.

2 Complete or modify the following fields:

Hot Backup

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 **Master MCU** or **Slave MCU** from the drop-down menu.
Paired MCU IP Address	Enter the Control Unit IP Address of the: • Slave MCU (if this MCU is the Master) • Master MCU (if this MCU is the Slave)

Hot Backup

Field	Description
Synchronization Status	The status of the synchronization between the Master and Slave MCUs in the Hot Backup configuration is indicated as: • OK - Hot Backup is functioning normally, and the Master and Slave MCUs are synchronized. • Attempting - Hot Backup is attempting to synchronize the Master and Slave MCUs. • Fail - A failure occurred while trying to synchronize the paired MCUs. • None - Hot Backup has not been enabled.

3 Click **OK**.

Configuring the Hot Backup Triggers

Hot Backup is initiated by the slave MCU on detection of no response from the master MCU on a Keep Alive operation. The Hot Backup triggers initiates the Hot Backup swap from Master to Slave when the selected conditions on the Master MCU occur.

The guidelines for configuring Hot Backup Triggers are:

- Hot Backup triggers should be configured on both the Master and Slave MCUs.
- Hot Backup triggers are not synchronized between the Master and Slave MCUs.

The Hot Backup triggers are configured in the **Hot Backup** dialog for the Master MCU when the Hot Backup feature is enabled.

To add the Hot Backup triggers to the Hot Backup configuration:

1 In RMX Manager, go to **Setup > Hot Backup**.

2 In the **Hot Backup** dialog, expand the **Trigger Hot Backup Triggers**.

A dialog opens with a list of event triggers displayed.

3 Select the appropriate **Hot Backup Triggers** check boxes:

Hot Backup Triggers

Hot Backup Trigger	Description
Lost connection with management port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection to the management port is lost on the Master MCU. This trigger is always set.
Lost connection with media port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active media port is lost on the Master MCU.

Hot Backup Triggers

Hot Backup Trigger	Description
Lost connection with signalling port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active signaling port is inactive for a duration of 30 seconds on the Master 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 Master to the Slave MCU when the connection with an ISDN (audio/video) card is disconnected on the Master MCU.

4 Alternatively, click **Trigger Failover Manually** when you want to trigger the Hot Backup manually and activate the Slave 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**.

Modifying the Master MCU Configuration

Modifications to the configuration of the Master MCU that require a System Reset cannot be performed while Hot Backup is enabled.

To modify the Master MCU configuration:

1 In RMX Manager, go to **Setup > Hot Backup**.

2 Disable the Hot Backup on the Master and Slave MCUs.

3 Modify the Master MCUs configuration.

4 Reset the Master MCU.

5 When the reset is **complete**, enable Hot Backup on the Master and Slave MCUs.

6 If required, reset the Slave MCU.

Audible Alarms

In addition to the visual cues used to detect events occurring on the 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.

The Audible Alarm played when Operator Assistance is requested, is enabled and selected using **Setup > Audible Alarm > User Customization**.

When an Audible Alarm is activated, the *.wav file selected in the **User Customization** is played, and is repeated according to the number of repetitions defined in the User Customization.

If more than one Collaboration Server is monitored in the RMX Manager, the Audible Alarm must be enabled separately for each 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 from either the RMX Web Client or RMX Manager, 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	?	?
Download Audible Alarm File	?	?
Stop Repeating Alarms	?	?

Configuring Audible Alarms

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.

To customize the Audio Alert:

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.
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.

Audible Alarm - User Customization Options

Option	Description
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**.

Replacing the Audible Alarm File

Each 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.

To replace the Audio file on the Collaboration Server Client or RMX Manager:

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 **Collaboration Server File** to play the file currently saved on the 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 Collaboration Servers are configured in the RMX Manager, the file must be downloaded to each of the required MCUs separately.

Customizing the Multilingual Setting

Each supported language is represented by a country flag in the Welcome Screen 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.

To customize the Multilingual Setting:

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 into for the customization to take effect**.**

Banner Display and Customization

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 be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

To customize the Multilingual Setting:

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

Software Management

The Software Management menu is used to backup and restore the Collaboration Server's configuration files and to download MCU software. Software Management operations include:

- Configuration files backup
- Configuration files restoring
- 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.

Backup Configuration Files

Backup and Restore Guidelines are:

- Direct access to the 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 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
- Collaboration Server Web Client user setting - fonts, windows
- Collaboration Server Web Client global settings – notes, address book, language
- Private keys and certificates (TLS)
- Conference participant settings
- Operation DB (administrator list)

To backup configuration files:

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 during Backup
Changes made during Collaboration Server system backup are not registered.

Restore Configuration Files

To restore configuration files:

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

To download MCU software files:

1 In RMX Manager, go to **Administration** > **Software Management** > **Software Download**.
2 Browse to the ***Install Path***, and click **Install**.

Ping the Collaboration Server

The Ping administration tool enables the 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.

To Ping a network entity from the Collaboration Server:

1 In RMX Manager, go to **Administration > Tools > Ping**.

2 Modify or complete the following fields:

Ping Parameters

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 Collaboration Server entity. The Answer is either OK or FAILED.

Configure Notification Settings

The Collaboration Server can display notifications when:

- A new 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 Collaboration Server user upon connection.

To configure the notifications:

1 In RMX Manager, go to**Setup** > **Notification Settings**.

The following notification options are displayed.

Notification Settings Parameters

Field	Description
New Connection	Notification of a new user/administrator connecting to the 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**.

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 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.log
```

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.
```

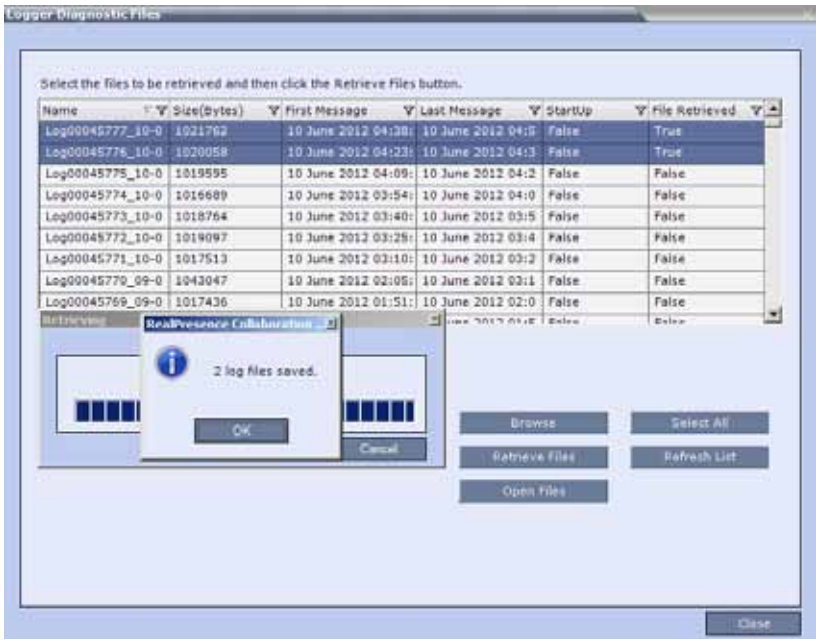
To retrieve the Logger Files:

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.

Information Collector

Standard Security Mode

The Information Collector comprehensively attains all information from all the MCU internal entities for data analysis. That data, stored in a central repository, is logged from the following system components:

- System Log Files
- CDR
- OS (Core dumps, CFG - DNS, DHCP, NTP, kernal state, event logs
- Signaling Trace files (H.323 & SIP)
- Central Signaling logs
- Processes internal state and statistics
- Full faults
- Apache logs
- CFG directory (without IVR)
- Cards info: HW version, state and status
- SW version number

- System Log Files
- CDR
- Processes internal state and statistics
- Full faults

- OS (Core dumps, CFG - DNS, DHCP, NTP, kernal state, event logs
- Signaling Trace files (H.323 & SIP)
- Central Signaling logs
- Apache logs
- CFG directory (without IVR)
- SW version number

The data collected is saved into a single compressed file containing all the information from each system component in its relative format (.txt, .xml, etc.). If the disk malfunctions, the file is written to the RAM (involves only a small amount of information where the RAM size is 1/2 a gigabyte). The zipped file (info.tgz) can be opened with the following applications: WinRAR and WinZip. The entire zipped file is then sent to Polycom's Network Systems Division for analysis and troubleshooting.

Ultra Secure Mode

The Information Collector logs information from the Collaboration Server's Network Intrusion Detection System (NIDS), saving it into a compressed disk file. (If the disk malfunctions, the file is written to RAM.) The zipped file (info.tgz) can be opened with either WinRAR or WinZip. The entire zipped file can be sent to Polycom for analysis.

Network Intrusion Detection System (NIDS)

The 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 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 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 Collaboration Server.
- Invalid access to open ports.

Using the Information Collector

When the Information Collector is used the following steps are performed:

1. **Creating** the Information Collector file.
2. **Saving** the Information Collector file.
3. **Viewing** the information in the Information Collector file.

To create the compressed file:

1. In RMX Manager, go to**Administration > Tools > Information Collector**.
   The **Information Collector** dialog is displayed.

Information Collector - Standard Security Mode

Information Collector - Ultra Secure Mode

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: Setting Date and Time Range during Troubleshooting

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, 2013 at 12:15, the From Date and Until Date should be October 1, 2013, 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 to be collected.

5 **Browse** to navigate to the directory path where the compressed file is to be saved.

6 Click **Collect Information**.

A progress indicator is displayed in the **Information Collector** dialog while the file is created.

7 To save the compressed file:

a The compressed file is automatically saved in the directory selected in the ***Information Collector*** dialog. The file is named **info.tgz**.

b Click **OK**.

8 To view the compressed file:

The compressed file is saved in .tgz format and can be viewed with any utility that can open files of that format, for example WinRAR® 3.80.

a Navigate to the directory on the workstation in which the file was saved.

b Double click the **info.tgz** file to view the downloaded information.

Note: Renaming Compressed File

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.

Auditor

An Auditor is a user who can view Auditor and CDR files for system auditing purposes.

Note: Auditor Access

The Auditor user can connect to the Collaboration Server only via the RMX Web Client.

The Event Auditor enables administrators and auditors to analyze configuration changes and unusual or malicious activities in the Collaboration Server system.

Auditor operates in real time, recording all administration activities and login attempts from the following Collaboration Server modules:

- Control Unit
- Shelf Manager

For a full list of monitored activities, see Audit Events.

The Auditor must always be active in the system. A System Alert is displayed if it becomes inactive for any reason.

The Auditor tool is comprised of the Auditor Files and an Auditor File Viewer to view them.

Note: Auditor Time Stamps
Time stamps of Audit Events are GMT.

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 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 Collaboration Server does not have available disk space to retain files for one year

Audit Event Files are retained by the 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.

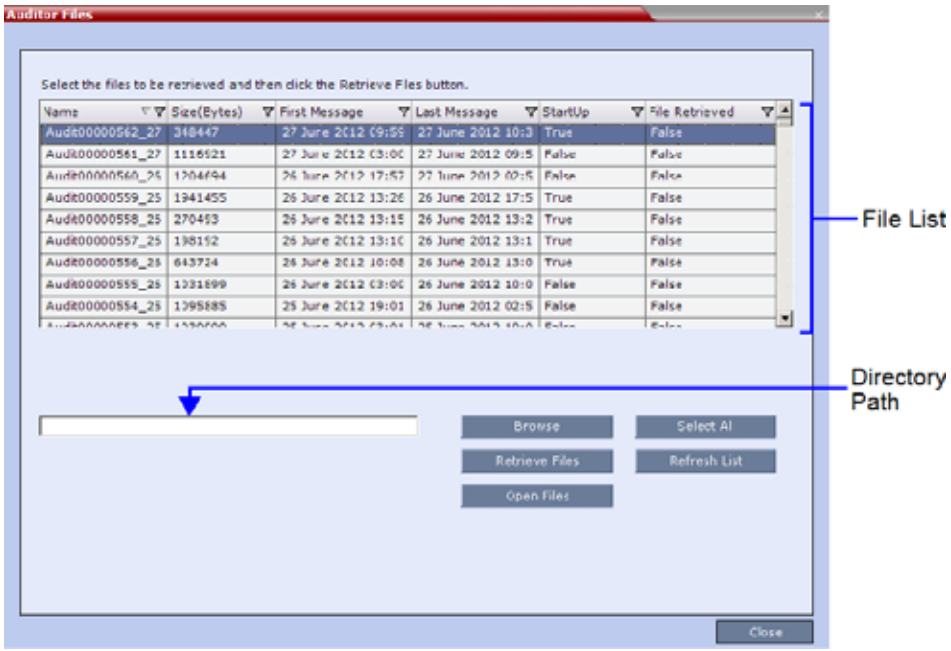
Using the Restore Factory Defaults of the System Restore procedure erases Audit Files.

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.

To access Auditor Files:

1 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.

For more information, see Auditor File Viewer.

To retrieve files for storage on a workstation:

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.

To open the file in the Auditor File Viewer:

» Double-click the file.

Auditor File Viewer

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.

To open the Auditor File Viewer from the Administration Menu:

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 Collaboration Server.
Date & Time	The date and time of the event taken from the Collaboration Server's Local Time setting.
User Name	The **Username** (Login Name) of the user who triggered the event.
Reporting Module	The Collaboration Server system internal module that reported the event: • MCMS • MPL • Central Signaling • MPL Simulation • 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 • Collaboration Server Internal Event

Auditor Event Columns

Field	Description
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 (Collaboration Server Internal Event) • Shutdown (Collaboration Server Internal Event) • Reset (Collaboration Server Internal Event) • Enter Diagnostic Mode (Collaboration Server Internal Event) • IP address changes via USB (Collaboration Server Internal Event)
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** (⊟).

To open an auditor event file stored on the workstation:

1 Click **Local File** ( ).

2 Navigate to the location of the audit event file.

3 Select the audit event file to be opened.

4 Click **Open**.

The selected file is opened in the **Auditor Viewer.**

Audit Events

Alerts and Faults

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.
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.

Alerts and Faults recorded by the Auditor

Event
Private version is loaded.
Restoring Factory Defaults.
Secured SIP communication failed.
Session disconnected without logout
SSH is enabled.
System Configuration modified.
System is starting.
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

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
TRANS_ISDN_PHONE:UPDATE_ISDN_PHONE

Transactions recorded by the Auditor

Transaction
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
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

ActiveX Bypass

At sites that, for security reasons, do not permit Microsoft® ActiveX® to be installed, the MSI (Windows Installer File) utility can be used to install .NET Framework and .NET Security Settings components on workstations throughout the network.

All workstation that connect to Collaboration Server systems must have both.NET Framework and .NET Security Settings running locally. These components are used for communication with the Collaboration Server and can only be installed on workstations by users with administrator privileges.

The MSI utility requires the IP addresses of all the Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation is to connect to.

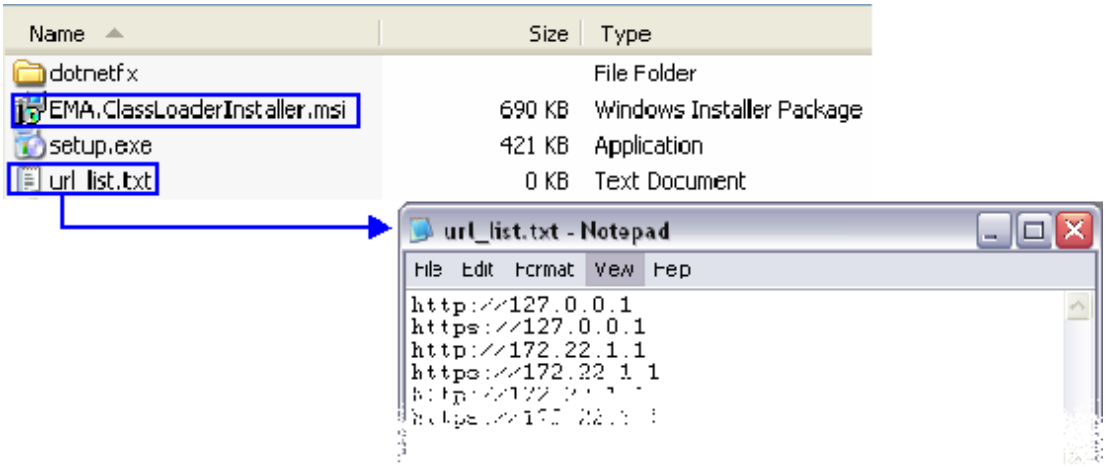
If the IP address of the any of the target Collaboration Servers is changed, the ActiveX components must be reinstalled.

Installing ActiveX

To install ActiveX components on all workstations in the network:

1. Download the MSI file **EMA.ClassLoaderInstaller.msi** from the Polycom Resource Center.
2. The MSI file contains installation scripts for both .NET Framework and .NET Security Settings.
3. Create a text file to be used during the installation, containing the IP addresses of all the Collaboration Servers (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.



4. Install the ActiveX components on all workstations on the network that connect to 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.

Collaboration Server Reset

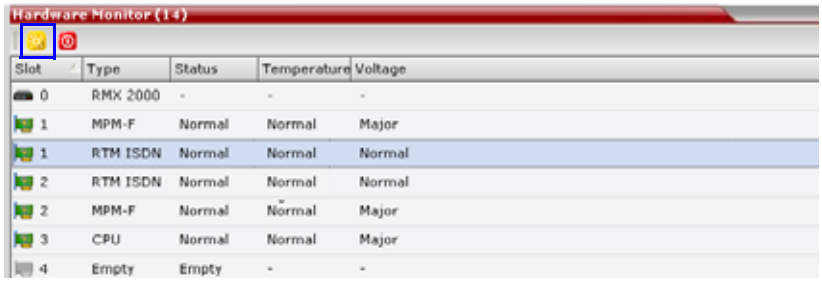
There are separate procedures for resetting Collaboration Servers 2000/4000/1800 and Collaboration Server Virtual Edition.

Reset the Collaboration Servers 2000/4000/1800

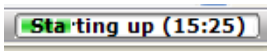
System Reset saves system configuration changes and restarts the system with the latest settings.

To reset the RMX:

1. In RMX Manager, go to the **RMX Management** pane and select **Hardware Monitor**.
2. Click **Reset** ( ).



When the Collaboration Server system is reset, during Collaboration Server startup the **Progress Bar** appears at the bottom of the 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: SIP Endpoints Connection during System Reset

Reset of the Collaboration Server from the Hardware Monitor, may not disconnect SIP endpoints previously connected even though the conference ends.

Collaboration Server Virtual Edition Reset

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.

To restart the Collaboration Server when deployed using:

- VMWare - See VMWare documentation on Resetting Virtual Machines.
- Hyper-V - See Hyper-V documentation on Resetting Virtual Machines.

Please note that, the System Reset option doesn't actually reboot the Virtual Machine, it only restarts the MCU service.

Entry Queues, Ad Hoc Conferences and SIP Factories

Note: Virtual Platform Guideline

When using Polycom® RealPresence® Platform, virtual Entry Queues and ad-hoc conferences should be defined in the RealPresence Resource Manager and virtual Meeting Rooms in the RealPresence DMA system. They should not be defined directly in the RealPresence Collaboration Server.

Entry Queues

An Entry Queue (EQ) is a special routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter. The Entry Queue remains in a passive state when there are no callers in the queue (in between connections) and is automatically activated once a caller dials its dial-in number.

Participants can be moved from the Entry Queue and the destination conference if both conferencing entities are set to the same conferencing parameters: Conferencing Mode, Line rate and video parameters. For example, participants can be moved from SVC Only Entry Queue to SVC Only conference, or from a mixed CP and SVC Entry Queue to a mix CP and SVC conference, from CP only Entry Queue to CP only conference.

The parameters (bit rate and video properties) with which the participants connect to the Entry Queue and later to their destination conference are defined in the Conference Profile that is assigned to the Entry Queue. For example, if the Profile Bit Rate is set to 384kbps, all endpoints connect to the Entry Queue and later to their destination conference using this bit rate even if they are capable of connecting at higher bit rates.

An Entry Queue IVR Service must be assigned to the Entry Queue to enable the voice prompts guiding the participants through the connection process. The Entry Queue IVR Service also includes a video slide that is displayed to the participants while staying in the Entry Queue (during their connection process).

Different Entry Queues can be created to accommodate different conferencing modes, conferencing parameters (by assigning different Profiles) and prompts in different languages (by assigning different Entry Queue IVR Services).

For more information, see IVR Services List.

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, 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. For more information about Ad Hoc conferencing, see Ad Hoc Conferencing.

An Entry Queue can be designated as Transit Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred. For more information, see Transit Entry Queue.

To enable ISDN (audio/video) participants to dial in to the Entry Queue, an ISDN (audio/video) dial-in number must be assigned to the Entry Queue. Up to two dial-in numbers can be assigned to each Entry Queue. The dial-in numbers must be allocated 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. The dial-in number must be communicated to the ISDN-video or ISDN-voice dial-in participants.

The Entry Queue can also be used as part of the Gateway to DMA solution for connecting Audio only ISDN-voice, ISDN-video, SIP and H.323 endpoints to DMA system.

For more information, see Gateway to Polycom® RealPresence Distributed Media Application™ (DMA™) System.

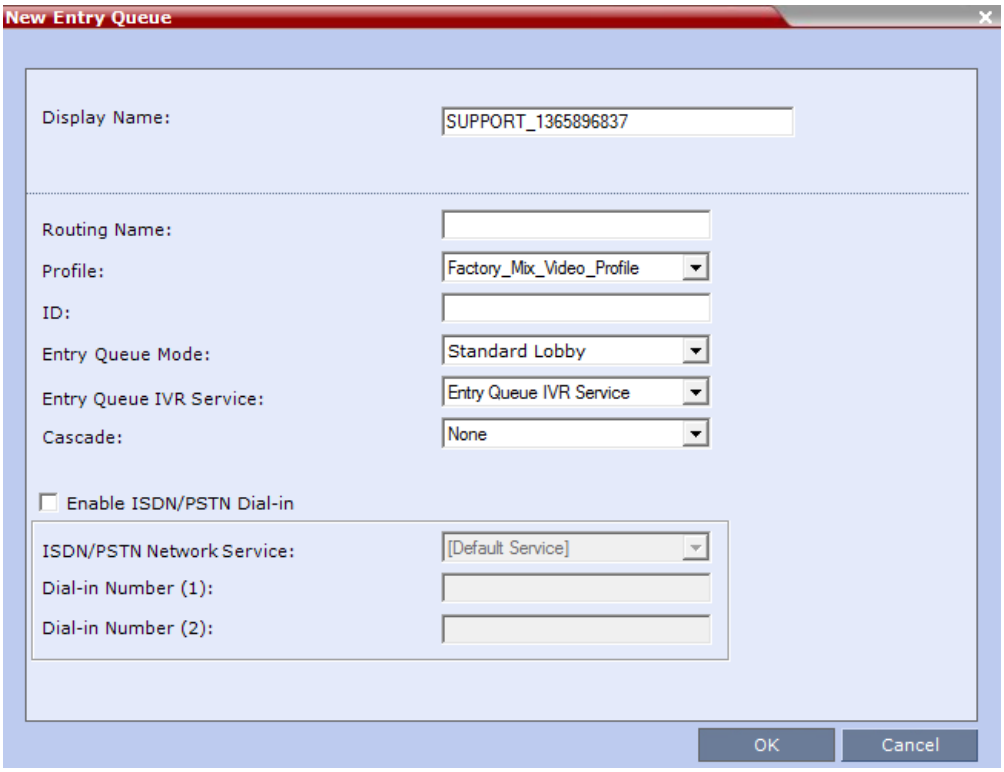
Default Entry Queue properties

The system is shipped with a default Entry Queue whose properties are shown in the following table.

Default Entry Queue Properties

Parameter	Value
Display Name	DefaultEQ The user can change the name if required.
Routing Name	DefaultEQ The default Routing Name cannot be changed.
ID	1000
Profile name	• In HW MCUs - Factory_Video_Profile, with 384 Kbps Bit Rate. • In VE MCUs - Factory_Mixd_CP_SVC_Video_Profile, with 1920Kbps Bit Rate
Entry Queue Service	Entry Queue IVR Service. This is 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. Up to two dial-in numbers can be assigned.

New Entry Queue



Entry Queue Definitions Parameters

Option	Description
Display Name	The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Manager. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the **Display Name** field that can be modified using Unicode encoding. • 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. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.

Entry Queue Definitions Parameters

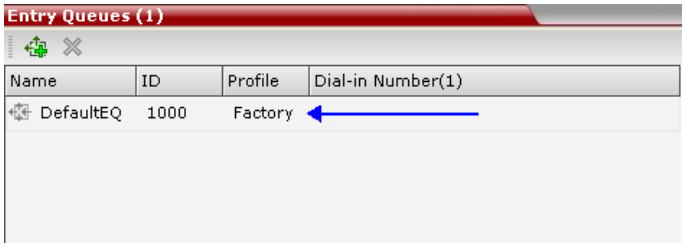
Option	Description
Routing Name	Enter a name using ASCII text only. If no Routing Name is entered, the system automatically assigns a new name as follows: • If an all ASCII text is entered in **Display Name**, it is used also as the **Routing Name.** • If any combination of Unicode and ASCII text (or full Unicode text) is entered in **Display Name**, the ID (such as Conference ID) is used as the Routing Name.
Profile	Select the Profile to be used by the Entry Queue. The default Profile is selected by default. This Profile determines the Bit Rate and the video properties with which participants connect to the Entry Queue and destination conference. To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue. In Ad Hoc conferencing, it 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 do not manually assign the ID, the MCU assigns one after the completion of the definition. The ID String Length is defined by the flag **NUMERIC_CONF_ID_LEN** in the System Configuration.
Entry Queue Mode	Select the mode for the Entry Queue
	Standard Lobby (default) - When selected, the Entry Queue is used as a routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to 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, the current Entry Queue is designated as a special Entry Queue for providing IVR Services to SIP calls on behalf of the DMA system, resulting in the IVR Only Service Provider Entry Queue routing SIP calls to the DMA system. For more details, see IVR Provider Entry Queue (Shared Number Dialing).
	External IVR Control - IVR Services can be controlled externally from an application server (such as the DMA) supporting the MCCF-IVR (Media Control Channel Framework-Interactive Voice Response) package. When selected, the connection process of the participant to the conference via the Virtual Entry Queue is controlled and managed by an external IVR service of an application server (for example, DMA).

Entry Queue Definitions Parameters

Option	Description
Entry Queue IVR Service	The default Entry Queue IVR Service is selected. 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.
Cascade	Set this field to **None** for all Entry Queues other than cascading. If this Entry Queue is used to connect dial-in cascaded links, select **Master** or **Slave** depending on the Master/Slave relationship in the Cascading topology. Set this field to **Master** if: • The Entry Queue is defined on the MCU on level 1 and the dialing is done from level 2 to level 1. • The Entry Queue is defined on the MCU on level 2 and the dialing is done from level 3 to level 2. Set this field to **Slave** if the Entry Queue is defined on the MCU on level 2 (Slave) and the dialing is done from MCU level 1 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. When the Entry Queue is saved on the MCU, the dial-in number will be automatically assigned to the Entry Queue. This number is taken from the dial-in numbers range in the default ISDN (audio/video) Network Service.
ISDN (audio/video) Network Service	The default Network Service is automatically selected. 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 not defined. To define a second-dial-in number, enter a required number from the dial-in number range defined for the selected Network Service.

Entry Queue List

The list of Entry Queues:



Transit Entry Queue

A Transit Entry Queue is an Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred.

IP Calls are routed to the Transit Entry Queue when:

- A gatekeeper is not used, or where calls are made directly to the Collaboration Server's Signaling IP Address, with incorrect or without a Conference ID.
- When a gatekeeper is used and only the prefix of the Collaboration Server is dialed, with incorrect or without a Conference ID.
- When the dialed prefix is followed by an incorrect conference ID.

When no Transit Entry Queue is defined, all calls containing incomplete or incorrect conference routing information are rejected by the Collaboration Server.

In the Transit Entry Queue, the Entry Queue IVR Service prompts the participant for a destination conference ID. Once the correct information is entered, the participant is transferred to the destination conference.

IVR Provider Entry Queue (Shared Number Dialing)

In an environment that includes a RealPresence DMA system, the Collaboration Server Entry Queue can be configured to provide the IVR Services on behalf of the RealPresence DMA system to SIP endpoints. It displays the Welcome Slide, plays the welcome message and retrieves the destination conference ID that is entered by the participant using DTMF codes.

To enable this feature, a special Entry Queue that is defined as IVR Only Service Provider is created. This Entry Queue does not forward calls to conferences running on the Collaboration Server and its main functionality is to provide IVR services.

Call Flow

The SIP participant dials the DMA Virtual Entry Queue number, for example 1000@dma.polycom.com.

The DMA forwards the SIP call to the Collaboration Server, to a special Entry Queue that is configured as IVR Only Service Provider. The participant is prompted to enter the conference ID using DTMF codes.

Once the participant enters the conference ID, the conference ID is forwarded to the DMA, enabling the DMA to connect the SIP endpoint to the destination conference or create a new conference and connect the participant to that conference.

Guidelines for Setting the Entry Queue as IVR Provider

- An Entry Queue defined as IVR Only Service Provider does not route the SIP call to a target conference and it cannot be used to route calls on the Collaboration Server. In such a configuration, the DMA handles the calls. Therefore, normal Entry Queues must be defined separately.
- **Operator Assistance** must be disabled in the IVR Service assigned to this Entry Queue.
- Only the conference ID prompts should be configured. Other prompts are not supported in IVR Only Service Provider configuration.
- ISDN-voice, ISDN-video, and H.323 calls to this Entry Queue are rejected.

- The DMA must be configured to locate the IVR Only Service Provider Entry Queue on the Collaboration Server. To locate the Entry Queue the DMA requires the Entry Queue's ID number and the Collaboration Server Signaling IP address (xxx.xx.xxx.xx).

Using External IVR Services via the MCCF-IVR

IVR Services can be controlled externally from an application server supporting the MCCF-IVR (Media Control Channel Framework-Interactive Voice Response) package. The external IVR service is currently being implemented with the integration of the Polycom RealPresence Virtualization Manager (DMA) as the application server. When the application server is deployed in the enterprise environment and the Polycom RealPresence Collaboration Server (MCU) is deployed as a media server, the external IVR service can be used to play audio messages, display slides, and collect DTMF input from the participant. The external IVR service is managed by the application server at the pre-conference phase when the participant is placed into a special external IVR-controlled Entry Queue in the Collaboration Server (MCU), collecting information before connecting to the conference.

The external IVR-controlled Entry Queue plays recorded voice messages or sends video slides such as splash screens to the participant and collects DTMF input from the participant such as conference ID and conference password for various functions.

IVR media files, WAV for voice messages and JPG for video slides, are stored on the application server. In order to provide external IVR control, a TCP-based MCCF channel is created between the application server and the media server. Because of real-time considerations, when the MCCF channel is established, the application server notifies the media server about the media files. The media server downloads the media files. The media server is notified by the application server when to download new or updated media files.

When the call has completed the pre-conference phase in the external IVR-controlled Entry Queue, the application server disconnects the call from the Entry Queue and routes the call to an ongoing conference or creates a new VMR.

Call Flows

The external IVR-controlled Entry Queue can be initiated for various types of calls from SIP endpoints such as standalone endpoints and Cisco TIP endpoints. Standalone endpoints are SIP or H.264 TIP endpoints. These endpoints can include HDX systems, multiple Telepresence (ITP) screens, and RealPresence Desktop client applications.

Call Flow for Standalone SIP Endpoints

The following describes how a standalone SIP endpoint call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

1. A SIP call is routed through the application server to the IVR-controlled Entry Queue.
2. The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.
3. The application server may request, through the MCCF channel - IVR package, to play an audio file and display a slide. When the audio file has finished playing, the MCU notifies the application server that the audio file has been played for the call.
4. The application server may request, through the MCCF channel - IVR package, to collect DTMF input such as a conference ID or password, from the caller. The DTMF input is transferred from the MCU to the application server. When the application server receives the DTMF input, it validates the

input for the required conference ID or password. If the input is incorrect, the application server will request the MCU to replay the audio file and collect the DTMF input again. The MCU transfers the DTMF input to the application server for revalidation.

5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

`<conf-id>**<password>@mcu-sig-ip.`

The call is disconnected from the application server. The MCU now has control of the call.

6 The call is transferred to a conference, which can reside on another MCU.

Call Flow for Standalone TIP Endpoints

The following describes how a standalone TIP endpoint call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

1 A TIP call is routed through the application server to the IVR-controlled Entry Queue. TIP endpoints can either have a single screen or multiple screens.

2 The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.

3 The application server may request, through the MCCF channel - IVR package, to play an audio file and display a video slide. When the TIP endpoint uses multiple screens, the video slide is displayed on the main screen only. When the audio file has finished playing, the MCU notifies the application server that the audio file has been played for the call.

4 The application server may request, through the MCCF channel - IVR package, to collect DTMF input such as a conference ID or password, from the caller. When the TIP endpoint uses multiple screens, the DTMF input is collected only once from the main screen. The DTMF input is transferred from the MCU to the application server. When the application server receives the DTMF input, it validates the input for the required conference ID or password. Because TIP uses DTLS, it can optionally enable re-keying of DTMF input and the calls to the Entry Queue and the conference can be encrypted.

5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

`<conf-id>**<password>@mcu-sig-ip.`

The call is disconnected from the application server. The MCU now has control of the call.

6 The call is transferred to a conference, which can reside on another MCU.

Call Flow for TIP Endpoints from a Polycom ITP System

The following describes how a TIP call from Cisco TPS endpoints or TIP calls from a Polycom ITP system working as a TIP call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

1 A TIP call is routed through the application server to the IVR-controlled Entry Queue.

2 The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.

3 While the call is in the Entry Queue, video is only displayed on the main screen.

4 DTMF input is collected only once from the main screen. Because TIP uses DTLS, it can optionally enable re-keying of DTMF input and the calls to the Entry Queue and the conference can be encrypted.

5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

`<conf-id>**<password>@mcu-sig-ip. The MCU now has control of the call.`

The call is transferred to a conference, which can reside on another MCU.

Guidelines for Using External IVR Services via the MCCF-IVR Package

- Only AVC SIP and TIP protocols are supported.
- MCCF channels support both IPV4 and IPV6.
- When the MCCF channel is disconnected, an alarm is displayed and all external IVR files are deleted. When the MCCF channel is reconnected, the external IVR files are sent to the MCU.
- When the Collaboration Server (MCU) is restarted, all existing external IVR files are deleted. When the MCCF channel connects to the Collaboration Server, the external IVR file are sent to the Collaboration Server.
- H.323 and ISDN-video protocols are not supported.
- Video Switching conferences do not support the TIP protocol
- TIP-based conferencing does not 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 participant connection to the conference via the Virtual Entry Queue, the Media files have to 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 x 1088 resolution

Configuring the MCU to Support External IVR Services via the MCCF-IVR

The support of External IVR Services via the MCCF-IVR package is enabled by default in the Collaboration Server (RMX) systems, by the flag **ENABLE_MCCF** which is set to **YES**.

However, in Ultra Secure Mode and in secured environments where the External IVR Services via the MCCF-IVR package is not required and unused ports should be closed, this flag should be set to **NO**.

To change this flag value from YES to NO, you must first add it to the System Configuration.

SIP Factories

A SIP Factory is a conferencing entity that enables SIP endpoints to create Ad Hoc conferences. The system is shipped with a default SIP Factory, named DefaultFactory.

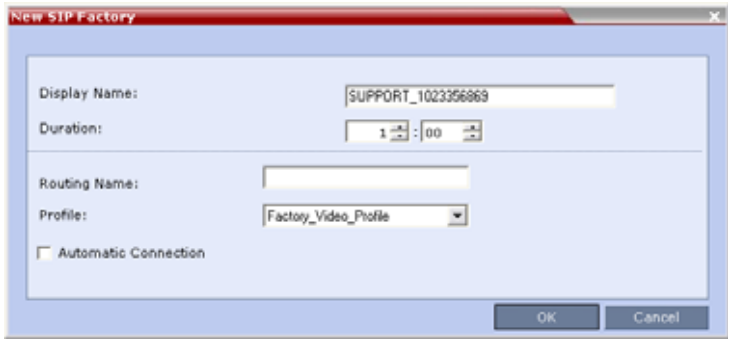
Note: Default SIP Factory ID - 7001 Reserved

The default SIP Factory uses the conferencing ID 7001. If a SIP Factory is being used, do not assign this ID to any conferencing entity, including conferences, reservations, and meeting rooms.

When a SIP endpoint calls the SIP Factory URI, a new conference is automatically created based on the Profile parameters, and the endpoint joins the conference.

The SIP Factory URI must be registered with the SIP server to enable routing of calls to the SIP Factory. To ensure that the SIP factory is registered, the option to register **Factories** must be selected in the Default IP Network Service.

New SIP Factory:



New Factory Properties

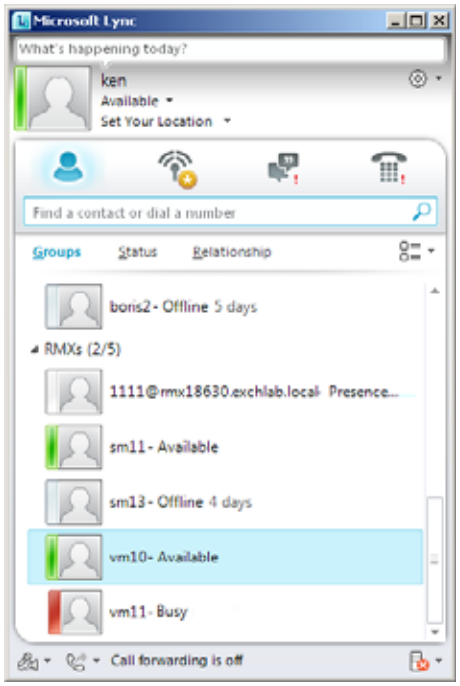
Option	Description
Display Name	Enter the SIP Factory name that will be displayed. The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Manager. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the **Display Name** field that can be modified using Unicode encoding. • 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. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.

New Factory Properties

Option	Description
Routing Name	The Routing Name is defined by the user, however if no Routing Name is entered, the system will automatically assign a new name when the Profile is saved as follows: • If an all ASCII text is entered in **Display Name**, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in **Display Name**, the ID (such as Conference ID) is used as the Routing Name.
Profile	The default Profile is selected by default. If required, select the conference Profile from the list of Profiles defined in the MCU. A new conference is created using the parameters defined in the Profile.
Automatic Connection	Select this check box to immediately accept the conference creator endpoint to the conference. If the check box is cleared, the endpoint is redirected to the conference and then connected.

SIP Registration & Presence for Entry Queues and SIP Factories with SIP Servers

Entry Queues and SIP Factories can be registered with SIP servers. This enables Office Communication Server or Lync server client users to see the availability status (**Available**, **Offline**, or **Busy**) of these conferencing entities, and to connect to them directly from the Buddy List.

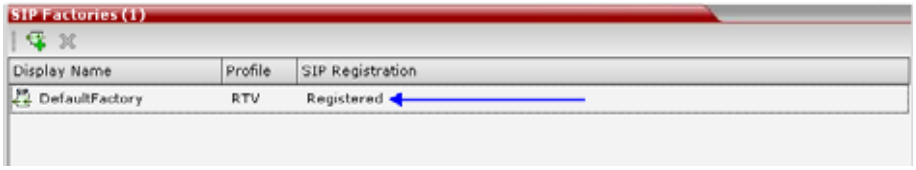


Guidelines for registering Entry Queues and SIP Factories with SIP Servers

- The Entry Queue or SIP Factory must be added to the Active Directory as a User.
- SIP Registration must be enabled in the Profile assigned to the Entry Queue or SIP Factory**.** For more information see Defining New Profiles**.**

Monitoring Registration Status

The SIP registration status can be viewed in the **Entry Queue** or **SIP Factory** list panes.



The following statuses are displayed:

- Not configured - Registration with the SIP Server was not enabled in the Conference Profile assigned to the Entry Queue or SIP Factory.

  When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address. In 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.

  This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP Server may be down, or any other reason the affects the connection between the Collaboration Server or the SIP Server to the network.
- Registered - The conferencing entity is registered with the SIP Server.
- Partially Registered - This status is available only in Multiple Networks configuration, when the conferencing entity failed to register to all the required Network Services, if more than one Network Service was selected for Registration.

Ad Hoc Conferencing

The Entry Queue can also be used for Ad Hoc conferencing. If the **Ad Hoc** option is enabled for the Entry Queue, 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. The conference parameters are based on the Profile linked to the Entry Queue. As opposed to Meeting Rooms, that are predefined conferences saved on the MCU, Ad Hoc conferences are not stored

on the MCU. Once an Ad Hoc conference is started, it becomes an ongoing conference, and is monitored and controlled as any standard ongoing conference.

An external database application can be used for authentication with Ad Hoc conferences. The authentication can be done at the Entry Queue level and at the conference level. At the Entry Queue level, the MCU queries the external database server whether the participant has the right to create a new conference. At the conference level the MCU verifies whether the participant can join the conference and if the participant is the conference chairperson. The external database can populate certain conference parameters.

For more information about Ad Hoc conferencing, see Appendix - Ad Hoc Conferencing and External Database Authentication.

Gateway to Polycom® RealPresence Distributed Media Application™ (DMA™) System

Gateway to DMA 7000 enables audio only ISDN-voice, ISDN-video (video endpoints using only their audio channels), SIP and H.323 calls to connect to the Polycom DMA 7000 via gateway sessions running on the Collaboration Server. Each Collaboration Server conference acting as a gateway session includes one connection to the endpoint and another connection to the DMA. The DMA 7000 enables load balancing and distribution of multipoint calls on up to 10 Collaboration Server media servers.

As part of this solution, the Collaboration Server acts as a gateway for the DMA that supports H.323 calls. The ISDN-voice, ISDN-video or SIP endpoint dials the virtual Meeting Room on the DMA via a special Entry Queue on the Collaboration Server.

Gateway functionality is not supported by Collaboration Server (RMX) 1800 with no DSP cards.

System Flags

In general, configure the RealPresence Collaboration Server using the 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 do not.

Managing System Flags

The following procedures describe how to add, edit, and delete system flags.

Add a System Flag

Add system flags to the RealPresence Collaboration Server.

To add a flag:

1. In RMX Manager, go to **Setup > System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, click **New Flag**.
3. Enter a value in the New Flag and Value field, and click OK.
4. Click **OK** to close the **New Flag** dialog box.
   The new flag gets added to the flags list.
5. Click **OK** to close the **System Flags** dialog box.

Edit a System Flag

You can modify the value of system flags from their default settings.

To edit a system flag:

1. In RMX Manager, go to **Setup > System Configuration** > **System Configuration**.
2. In the **MCMS_PARAMETERS_USER** tab, select the flag to be modified 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.

To delete a flag:

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**.

System Flags

The following tables lists the predefined RealPresence Collaboration Server 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

Flag Name	Description	Platform	Add?
ACCEPT_VOIP_DTMF_TYPE	Defines the type of DTMF tones (inband) or digits (outband) that the RealPresence Collaboration Server will accept in VoIP calls depending on the endpoint's current setting. Range: • 0 - Auto (default) If the endpoint switches from inband to outband and vice versa, the value of the SET_DTMF_SOURCE_DIFF_IN_SEC flag determines the time interval after which both inband and outband tones/digits will be accepted. • 1 - Outband (H.245) only • 2 - Inband only	HW/VE	Yes
ALLOW_SIREN7_CODEC	Prevents disconnection of Lync clients using audio rates smaller than 42 Kbps, when the Lync server is configured to allow 33 Kbps audio rate. Siren 7 audio codec is preferred for SIP/Lync calls, depending on the value of this flag. Default value: NO Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
ALWAYS_APPLY_CONTENT_THRESHOLD	When set 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	When set to YES, the gateway session forwards the DTMF codes to all ISDN-voice and video participants. Default Value: NO Possible values: YES/NO	HW	Yes
AV_MCU_PANORAMIC_LAYOUT_ENABLED	Enables panoramic layout on the MCU. Default value: NO Possible values: YES/NO	HW/VE	Yes
BLOCK_CONTENT_LEGACY_FOR_LYNC	When set to YES, content is not sent to Lync clients over the video channel. Also includes those with the Polycom CCS plug-in installed, even when the Send Content to Legacy Endpoints is enabled. Other non-Lync legacy endpoints will not be affected by this flag and will receive content according to the Send Content to Legacy Endpoints settings in the conference profile. When set to NO, content is sent to all Lync clients over the video channel, including those with the plug-in installed, even when the Send Content to Legacy Endpoints is disabled. Other non-Lync legacy endpoints will not be affected by this flag and will 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	When set to YES, all Microsoft Lync 2013 functionality can be disabled. All Lync 2013 clients, whether connected directly or through cascading, will connect using the RTV codec. Default value: NO Possible values: YES/NO		Yes

General System Flags

Flag Name	Description	Platform	Add?
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	When set to SEQUENTIAL, the MCU initiates channel connections until it reaches the number of channels defined by the BONDING_NUM_CHANNELS_IN_GROUP flag. When a channel is connected, dialing begins for the next channel in the group. When set 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 between dialing attempts for each channel in the group. Default value: SEQUENTIAL	HW	Yes
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 in the bonding group to be connected before dialing the next sequential channel. Default value: 50	HW	Yes
BURN_BIOS	Although not recommended, setting this flag's value to NO will prevent BIOS upgrade. Default value: YES Possible values: YES/NO	HW/VE	Yes
CAC_ENABLE	When set to YES, enables Call Admission Control implementation in the RealPresence Collaboration Server. Default value: NO (CAC is disabled) Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
CASCADE_LINK_PLAY_TONE_ON_CONNECTION	When set to YES, the RealPresence Collaboration Server plays a tone when a cascading link between conferences is established. The tone is played in both conferences. This tone is not played when the cascading link disconnects from the conferences. The tone volume is controlled by IVR_MESSAGE_VOLUME flag. 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	You can configure the duration of an ad-hoc conference* by setting the flag to one of the following values: Default value: 60 minutes Possible values: 90 minutes, 180 minutes, and 270 minutes. * An ad-hoc conference is automatically created when the participant dials into an Ad-hoc Entry Queue and enters a conference ID that is not being used by any other conferencing entity. It is based on the Conference Profile assigned to the EQ.<does ad-hoc conference need to be defined>	HW/VE	No

General System Flags

Flag Name	Description	Platform	Add?
CONTENT_SLAVE_LINKS_INTRA_ SUPPRESSION_IN_ SECONDS	Defines the interval when RealPresence Collaboration Server is allowed to forward an Intra Request received from any of the Slave Cascading Links. The Slave Cascading Link can be connected to the local RealPresence Collaboration Server, to an MCU on a higher cascade level or to the content sharer. The first Intra request that is received from any of the subordinate MCUs connected to the RealPresence Collaboration Server starts the interval counter and is forwarded to the next level MCU or to the content sharer. All other Intra requests that are received within this interval are registered but ignored. After an interval, the system checks if during the last interval any additional intra requests were registered. If there is at least one Intra request it will be forwarded. If there is no additional Intra request, no action is taken other than to wait for the next cycle. This filtering process is repeated every <flag value> second. Default value:30 seconds	HW/VE	No
CP_REGARD_TO_INCOMING_SET UP_RATE	For use in the Avaya environment. When set to YES, the RealPresence Collaboration Server calculates the line rate for incoming calls in CP conferences, according to the line rate which is declared by the endpoint in the H.225 setup message. When set to NO, the rate is calculated according to the conference line rate regardless of the rate in the H.225 setup message. Default value: YES Possible values: YES/NO	HW/VE	Yes
CPU_BONDING_LINK_MONITORI NG_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

General System Flags

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. Receive Load Balancing is achieved by ARP negotiation. Intercepted Outbound ARP Replies and their source hardware address are overwritten with the unique hardware address of one of the subordinate in the bond. In this way, different peers will 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 <have changed ‘slave’ to ‘subordinate. kindly confirm if this usage is correct.>	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, this default might be too long and the TCP connection is lost. In such a case, the default value should be changed 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
DELAY_BETWEEN_H320_DIAL_OUT_PARTY	The delay in milliseconds that the MCU waits when connecting dial out ISDN-video and voice participants. Default vlaue: 1000	HW	Yes

General System Flags

Flag Name	Description	Platform	Add?
DISABLE_DUMMY_REGISTRATIO N	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_INDICAT ION	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 displayed 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_DIA L_OUT	When set to NO, the RealPresence Collaboration Server sends a widescreen resolution to dial-out SIP endpoints. Endpoint types that do not support wide screen resolutions are automatically identified by the RealPresence Collaboration Server according to their product type and version. When set to YES, the RealPresence Collaboration Server does not send wide screen. Default value: NO Possible values: YES/NO	HW/VE	Yes
DTMF_FORWARD_ANY_DIGIT_TI MER_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, and does not apply them to conferences running on itself. Default value: 60 seconds Range: 0 - 360000 seconds	HW/VE	Yes
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

General System Flags

Flag Name	Description	Platform	Add?
ENABLE_AUTO_EXTENSION	When set to YES, this flag allows conferences running on the RealPresence Collaboration Server to be automatically extended as long as there are participants connected and the system has free resources. When set to NO, this flag prevents the conference duration from being automatically extended. Default value: YES Possible values: YES/NO Note: If this flag is set to: • YES, Gateway calls are not limited in duration while endpoints are connected. • NO, Gateway calls are limited to 60 minutes.	HW/VE	No
ENABLE_AQUA_FEATURE_SYSTEM_FLAG	This system flag is used 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	
ENABLE_AQUA_DOUGH_BOY_FLAG	This system flag is required to enable the Doughboy feature, provided the ENABLE_AQUA_FEATURE_SYSTEM_FLAG is already enabled. This feature is intended display a Doughboy image in the place of the normal image of a Microsoft Skype for Business or Lync user on the video layout of a Video Teleconference user participating in a Polycom RealConnect conference, when that Skype for Business or Lync user disables its video output. If the Skype for Business or Lync user enables its video output once again, the RealPresence Collaboration Server stops displaying the Doughboy image and reverts to the normal image of the Skype for Business or Lync user on the Video Teleconference user's video layout. 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

General System Flags

Flag Name	Description	Platform	Add?
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, ensure that the MCU is defined as master at all times, When cascading between the RealPresence Collaboration Server and a Codian MCU. Possible values: YES/NO		
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 in all the MCUs within the H.323 cascaded topology, and these MCUs using RealPresence Collaboration Server version 8.6 and up, content snatching is enabled. 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, allowing a time-out to be used as a stop indicator for the string input for the local IVR, when the MCU collects the Conference ID in the local entry queue or the password while routed to the conference.		

General System Flags

Flag Name	Description	Platform	Add?
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
ENABLE_FLOW_CONTROL_REINVITE	Used to enable or disable sending a re-INVITE to endpoints to adjust their data rate. When set to YES, re-INVITE is used for endpoints that do not 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 that the G.729 codec is disabled, and G.711 is used instead. This is useful in calls where the audio quality is affected by lower line rates. Default value: YES Possible values: YES/NO Note: The modified flag setting will affect new calls.	HW/VE	Yes
ENABLE_H239	When set to YES, Content is sent through a separate Content channel. Endpoints that don't support H.239 will not be able to receive. This flag is enabled when sending content as a separate stream. When set to NO, the Content channel is closed. In such a case, H.239 Content is sent through the video channel ("people" video) enabling endpoints that do not support H.239 Content sharing to receive the content in their video channel. Default value: YES Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
ENABLE_H239_ANNEX_T	In H.239-enabled MIH cascading, when MGC is on Level 1, this flag enables sending Content using Annex T. This flag should be set 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=YES	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_LYNC_RTCP_INTRA	When set to YES, RTCP FIR is used for sending Intra Requests. When set to NO, Intra Requests are sent 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 is enabled. In Ultra Secure Mode and in secured environments where the External IVR Service through the MCCF-IVR package is not required and unused ports should be closed, this flag should be set to NO. 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 and further call data recording is stopped. In that case, the additional data is lost. When 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. Default value: NO (disabled) Possible values: YES/NO		

General System Flags

Flag Name	Description	Platform	Add?
ENABLE_MODULAR_MCU	Indicates whether the system is in MMCU mode. Possible values: Default value: NO - System is not in MMCU mode. Possible values: • MIX - System is in partial MMCU mode. • YES - System is in full MMCU mode. Note: MCU reset is required for changes to take effect.	HW/VE	No
ENABLE_MS_FEC Managing System Flags	Enables the Microsoft FEC (Forward Error Correction) support for RTV. When set to **Auto**, FEC support is enabled. FEC uses the DV00 option (DV=00 - one FEC per frame using XOR). When set to **No**, FEC support is disabled. 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 in the RealPresence Collaboration Server and that they will be connected 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 recording control operations to be performed using either DTMF tones or a SIP INFO request. When set to NO, the RealPresence Collaboration Server will send Recording Control Operation commands to the Polycom® RealPresence® Media Suite using DTMF as in all previous version. When set to YES, the RealPresence Collaboration Server will send 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

General System Flags

Flag Name	Description	Platform	Add?
ENABLE_SELECTIVE_MIXING	You need to manually add this flag and enable or disable the function by changing the value to YES/NO. MCU reset isn't required when changing the system flag value. Possible values: YES/NO		Yes
ENABLE_SIP_PEOPLE_PLUS_CONTENT	If security is of a higher priority than SIP Content sharing, SIP People+Content™ technology can be disabled by setting this system flag to NO. (The content management control (BFCP) uses an unsecured channel (port 60002/TCP) even when SIP TLS is enabled). Default value: YES Possible values: YES/NO	HW/VE	Yes
ENABLE_SIP_PPC_FOR_ALL_USER_AGENT	When set to YES, SIP People+Content and BFCP capabilities are declared 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_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. This setting is recommended for MCUs running Telepresence conferences. Default value: YES Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
ENFORCE_SAFE_UPGRADE	When set to YES this flag enables the RealPresence Collaboration Server to notify users when an incorrect version upgrade/downgrade or upgrade/downgrade path is selected. When set to NO, after initiating an upgrade or downgrade software installation, the RealPresence Collaboration Server activates a fault alert in the Faults List: Warning: 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	When an Entry Queue is set as IVR Service Provider for the RealPresence DMA 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 you have changed the default names used by the RealPresence Resource Manager application. Default value: /PlcmWebServices	HW/VE	Yes
EXTERNAL_CONTENT_IP	Enter the IP address of the RealPresence Resource 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 RealPresence Resource Manager global Address Book. <is this listing required?> When empty, the integration of RealPresence Resource Manager address book with RealPresence Collaboration Server is disabled.	HW/VE	Yes
EXTERNAL_CONTENT_PASSWORD	The password associated with the user name defined for RealPresence Collaboration Server in RealPresence Resource Manager server.	HW/VE	Yes
EXTERNAL_CONTENT_PORT	The RealPresence Resource 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 RealPresence Resource Manager server defined in the format: domain name/user name	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
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 used. 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 defined 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 associated with the user name defined for the RealPresence Collaboration 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	The Fade-In/Fade-Out feature can be disabled by adding this as a new flag to the System Configuration, and setting its value to NO. Possible values: YES/NO		
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, the Apache Server is not rebooted when a new CRL is automatically uploaded. When set to YES, the Apache Server is rebooted upon a new CRL automatic upload. Note: Applicable to automatically uploaded 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.		

General System Flags

Flag Name	Description	Platform	Add?
FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE	Used to force the use of a specific audio algorithm when a Microsoft Office Communicator R2 or Lync client is hosted on a workstation with a single core processor. The flag value overrides the default audio algorithm selection (G.722.1) that might cause audio quality problems when G.722.1 is used by Microsoft clients running on single processor workstations. This flag can be set 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 will assign 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
FORCE_CIF_PORT_ALLOCATION	Sets the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. 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. Enter 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.	HW/VE	No
FORCE_G711A	Forces the use of the G.711A audio codec. Default value: NO Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
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 does not manage the layouts while Content is sent. 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 Content is sent. Personal layout changes, for example, by MLA, are ignored. The layouts for legacy endpoints are managed by the MCU.		
FORCE_RESOLUTION	Use this flag to specify IP (H.323 and SIP) endpoint types that cannot receive wide screen resolution and that weren't automatically identified as such by the RealPresence Collaboration Server. 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 SEND_WIDE_RES_TO_IP is set to YES.	HW/VE	Yes
FORCE_STATIC_MB_ENCODING	This flag supports Tandberg MXP mode of sending and receiving video by IP endpoint in HD 720p resolution and Video Quality set to Motion. This mode is not supported for ISDN-video endpoints. 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

General System Flags

Flag Name	Description	Platform	Add?
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: YE/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, a gatekeeper is required to receive incoming H.323 calls. If a gatekeeper is not configured in the RealPresence Collaboration Server, the calls will fail. When set to NO (default), gatekeeper is not required 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
GK_MANDATORY_FOR_CALLS_OUT	When set to YES, a gatekeeper is required to perform H.323 outgoing calls. If a gatekeeper is not configured on the RealPresence Collaboration Server, the call fails. When set to NO (default), gatekeeper is not required to dial out to H.323 participants and calls can be dialed 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 declared by an endpoint before receiving or transmitting Content. Default value: NO Possible value: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
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
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=NO	When set to NO, disables the highest common mechanism in H.264 and enables selection of H.264 Video Protocol in fixed mode 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). To ensure that the participants' video resources remain available for them, and aren't released for use by audio only calls, set this flag to NO. If set to YES, the RealPresence Collaboration Server will release video resources for Audio Only calls. Default value: YES Possible value: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
HD_THRESHOLD_BITRATE	The value of this flag is the system minimum threshold bitrate for HD resolutions. The line rate selected in the Conference Profile must be the same of higher than specified by this flag. Default value: 768 Kbps Range: 384 Kbps - 4 Mbs	HW/VE	No
HW_FOLLOW_SPEAKER_RESOLUTION_ON_1X1_LAYOUT	Enables endpoints capable of higher resolution in a conference where some endpoints are lower than 4CIF and others are higher to receive the Indication icons. Possible values: • AUTO (default) - When any of the Indication icons are configured for display, do not follow the speaker. When the Indication icons are not configured for display, follow the speaker. • YES - Always follow the speaker in 1x1 layout. • NO - Never follow the speaker in 1x1 layout.	HW	No
IGNORE_AIM	Audio Indicate Muted (AIM) is relevant to H.323 endpoints. When an endpoint mutes its microphone, it does not necessarily mute its entire audio stream. This allows sharing of content that includes audio while microphones are muted. Default value: NO Possible values: NO - When the AIM signal is received, the participant is muted and a mute icon is displayed in the RMX Web Client or RMX Manager. YES - When the AIM signal is received, the participant is not muted and a mute icon is not displayed in the RMX Web Client or RMX Manager. Range: YES, NO	HW	Yes
RPCSVE_ENHANCE_CAPACITY	Setting this flag to “YES” results in rejection of all Mixed mode conferences, since in this case AVC-only and SVC-only are the only conference modes supported. This flag can be enabled to achieve a higher capacity for a given hardware and virtual machine configuration. Default value: NO Possible values: YES/NO	VE	

General System Flags

Flag Name	Description	Platform	Add?
INTERNAL_SCHEDULER	When set to NO (default) this flag prevents potential scheduling conflicts from occurring as a result of system calls from external scheduling applications such as 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
IP_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD video switching conferences run on the RealPresence Collaboration Server 1800, 2000 or 4000 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 flag MIX_LINK_ENVIRONMENT is set to NO, the IP_ENVIRONMENT_LINK flag must be set to YES. Possible values: YES/NO	HW/VE	Yes
IP_RESPONSE_ECHO	When set to YES, the RealPresence Collaboration Server will respond to ping (IPv4 and IPv6) commands. When set to NO, the RealPresence Collaboration Server will not respond to ping commands. Possible values: YES/NO	HW/VE	Yes
IPV6_AUTO_ADDRESS_CONFIGURATION_METHOD	SLAAC (Stateless Address Auto Configuration) and DHCPv6 related system behavior is controlled by setting this flag's value as required. 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 in which the MCU is located. Default value: COUNTRY_NIL	HW	No
ISDN_IDLE_CODE_E1	The Idle code (silent), transmitted on the ISDN-video E1 B channels, when there is no transmission on the channels. Default value: 0x54	HW	No

General System Flags

Flag Name	Description	Platform	Add?
ISDN_IDLE_CODE_T1	The Idle code (silent), transmitted on the ISDN-video T1 B channels, when there is 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 to be received by the MCU. Default value: 9	HW	No
ISDN_RESOURCE_POLICY	Determines how the ISDN-video B-channels within configured spans are allocated. The robustness of the ISDN-video network can be improved by allocating channels evenly (load balancing) among the spans, minimizing 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 that the appropriate license is installed). Default value: NO Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
ITP_CROPPING	If the conference is set to telepresence mode, cropping of the image is done 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: If the flag was added with no value, and the conference is set to telepresence mode, the left-right areas aren't cropped, and the top-bottom areas are asymmetrically cropped (16% from top, 84% from bottom).	HW/VE	No
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**: • It is not recommended to disable IVR messages by setting the flag value to 0. • System reset is not required for flag changes to take effect.	HW/VE	No
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected 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:** System reset is not required 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

General System Flags

Flag Name	Description	Platform	Add?
IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE	When set to YES, the system does not playback the Roll Call names when participants enter the conference. Possible values: YES/NO		
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: • It is not recommended to disable the Roll Call by setting the flag value to 0. • System reset is not required for flag changes to take effect.	HW/VE	No
LEGACY_EP_CONTENT_DEFAULT_LAYOUT	Defines the video layout to be displayed on the screen of the legacy endpoints when switching to Content mode. Default value: CP_LAYOUT_1P7 (1+7).	HW/VE	No

General System Flags

Flag Name	Description	Platform	Add?

LPR_CONTENT_RATE_ADJUST_WEAK_LPR	When Polycom Lost Packet Recovery (LPR) is initiated by an endpoint in an AVC-CP conference due to experienced packet loss, the MCU reduces video rate (minimum is 64K) to avoid exceeding bandwidth.
	At times, further reduction is required to preserve the bandwidth, which is regulated by this system flag.
	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 protocol used by the endpoint 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 protocol used by the endpoint 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, the content rate is not reduced, and MCU packet loss protection is guaranteed for 5%.
	Default value: NO
	Possible values: YES/NO
	Notes:
	• No system restart is required for this flag new value to take effect.
	• This flag should not be set to YES in systems using TIP conferencing.
		HW/VE	Yes

General System Flags

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 if video optimized mode is selected. 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 AV MCU 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 RealPresence Collaboration Server does not manage Telepresence Room Switch Layouts and they continue to be managed by the MLA. • 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	Allows to get the count of Skype for Business and nonSkype Business audio/video participants connected to cascaded conference through AVMCU. Flag values are as follows: Default value: 20 Range: 0-99	HW/VE	Yes

General System Flags

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 Recording Links available for selection in the Recording Links list and the Conference Profile - Recording dialog box. Default value: 20 Range: 1 - 100	HW/VE	Yes
MCU_DISPLAY_NAME	The MCU name that is displayed 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 and might be required to adjust its MTU size according to the network environment in which it is deployed. Default value: 1,500 Range: 500-20,000. Values outside that range are treated as 1,500.	HW/VE	Yes
MIN_H239_HD1080_RATE	Used to set the threshold line rate for HD Resolution Content: the line rate at which the RealPresence Collaboration Server will send Content at HD1080 Resolution. Setting the flag to 0 disables HD Resolution Content. Default value: 768 Kbps	HW/VE	Yes
MIN_SYSTEM_DISK_SPACE_TO_ALERT	Defines a minimum remaining the RealPresence Collaboration Server disk capacity in megabytes. Raises an active alarm if the remaining disk capacity falls below this level. Default value: 2048	HW/VE	No

General System Flags

Flag Name	Description	Platform	Add?
MIN_TIP_COMPATIBILITY_LINE_RATE	Determines the minimum line rate at which conferencing entities such as an Entry Queue or Meeting Room can be TIP-enabled to connect endpoints. CTS version 7 requires a minimum line rate of 1024 Kbps and will reject calls at lower line rates. 0 means that no minimum line rate is enforced 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 will adjust the line rate of HD Video Switching conferences run on the RealPresence Colalboration Server from 1920 Kbps to 17897, 100bits/sec to match the actual rate of the HD Video Switching conference running on the MGC. Note: If the flag is set to YES, the IP_ENVIRONMENT_LINK flag must be set to NO. Possible values: YES/NO	HW/VE	Yes
MMCU_BLOCK_TR_ABORTED	When set to NO, enables the MMCU recovery mechanism, otherwise the MMCU recovery is disabled. Default value: NO (recommended) Possible values: YES/NO	HW/VE	Yes
MS_AV_MCU_ MONITORING	The system behavior can be controlled 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 is not connected. Default value: 30 Possible values: 0 - 384	HW/VE	Yes
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 is not connected 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

General System Flags

Flag Name	Description	Platform	Add?
MS_KEEP_ALIVE_ENABLE	Enables the Microsoft Keep Alive flag. When set to YES, this flag ensures that endpoints such as HDX remain connected to the conference for its duration when the RealPresence Collaboration Server is configured with FQDN address and Lync server is working with load balancing holding more than one address. Default value: NO Possible values: YES/NO Note: The functionality of this flag has been replaced with the following system flags: • SIP_TCP_KEEP_ALIVE_TYPE • SIP_TCP_KEEP_ALIVE_BEHAVIOR	VE	Yes
MS_PROXY_REPLACE	Enables the proxy=replace parameter in the SIP Header. When set to YES, the outbound proxy replaces the contact information in the contact header on its own. This enables other clients and servers to reach the client using the proxy's IP address, even if the client is behind a firewall. 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 of the conference can selectively to mute all participants or only mute the Skype for Business participants. Default value: YES Possible Values: YES/NO	HW/VE	Yes
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 a Hello message is sent from the RealPresence Collaboration Server to an endpoint 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 redialing attempts required. Dialing might continue until the conference is terminated. Default value: 3	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
NUMERIC_CONF_ID_LEN	Defines the number of digits in the Conference ID that will be assigned by the MCU. 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
OCSP_RESPONDER_TIMEOUT	Determines the number of seconds the RealPresence Collaboration Server is to wait for an OCSP response from the OCSP Responder before the connection fails. Network latency or slow WAN links can cause login problems when logging in to the management network of the RealPresence Collaboration Server. This system flag's value determines the number of seconds the MCU is to wait for an OCSP response from the OCSP Responder before failing the connection. 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 they were muted by the administrator, chairperson (*86) or themselves (*6). 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

General System Flags

Flag Name	Description	Platform	Add?
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	The value of this flag determines the duration of the display of the Gathering slide for participants that connect to the conference after the conference 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
POLYCOM_EPS_DISPLAY_NAME_PREFIX_IN_LYNC_ROSTER	Determines the prefix of the RealPresence Collaboration Server participant names in Lync conference roster. Default: “Polycom/”	HW/VE	Yes
PORT_GAUGE_ALARM	When set to YES, if the system resource usage reaches the High Port Usage Threshold as defined for the Port Gauges, System Alerts in the form of an Active Alarm and an SNMP trap are generated. Possible values: YES/NO	HW/VE	Yes
PRESENTATION_INDICATOR_ENABLED	This flag is required to enable the Presentation Indicator feature, provided the ENABLE_AQUA_FEATURE_SYSTEM_FLAG is already enabled. The Presentation Indicator feature is intended to display an appropriate notification using the Message Overlay functionality to the participants directly connected to the MCU in a Polycom RealConnect conference, to indicate certain restrictions pertaining to the presentation and viewing of content. Default value: No Possible values: YES/NO	VE	

General System Flags

Flag Name	Description	Platform	Add?
PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE	When set to NO (default), the ICE channel is closed after applying CAC bandwidth management when Call Admission Control is enabled 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
PRESERVE_PARTY_CELL_ON_FORCE_LAYOUT	Used to prevent reassignment of cells in a forced layout that were assigned to endpoints that have disconnected, paused their video, or have been removed from the conference. The cell will remain black until the endpoint reconnects or a new layout is used, or the conference ends. Range: YES/NO Default: NO • NO - Cells of dropped endpoints are reassigned. Endpoints that reconnect will be treated as new endpoints. • YES - Cells of dropped endpoints are not reassigned, but will be reserved until the endpoint reconnects. Forced Layout Guidelines:<can guidelines be included in the table> • It is recommended that this flag be set to YES if the RealPresence Collaboration Server is used primarily for ITP conferences with MLA. • When a new forced layout is sent 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 is switched from the forced layout to automatically assigned, the MCU no longer preserves the cell. Any other endpo int can be assigned to that particular cell. • This feature works the same way in Telepresence conferences, even where the layouts are controlled by the MLA.	HW/VE	Yes
PSTN_RINGING_DURATION_SECONDS	If there is a slow response from the ISDN-video switch, ISDN-voice dial-out ringing duration (in seconds) is used by the RealPresence Collaboration Server to disconnect the call. Default value: 45	HW	Yes

General System Flags

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 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 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, the flag must be set 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 the flag value should be set equal 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
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

General System Flags

Flag Name	Description	Platform	Add?
REDUCE_CAPS_FOR_REDCOM_SIP	To accommodate Redcom's SDP size limit, when the flag value = YES, the SDP size is less than 2kb and includes only one audio and one video media line. Default value: NO Possible values: YES/NO	HW/VE	Yes
REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME	When set to YES, if the Precedence Domain of a SIP dial-in call does not match the Precedence Domain of the RealPresence Collaboration Server, the call is rejected. 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): The feature is disabled. • 20 – 300 (seconds): The feature is enabled.	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
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

General System Flags

Flag Name	Description	Platform	Add?
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 if the E.164 number is to be substituted for the IP address in the dial string. Default value: YES - The IP address will be substituted with the E.164 number. 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 will receive 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. The flag must be set to **YES** (RealPresence Collaboration Server 2000). Possible values: YES/NO	HW	No
RRQ_WITHOUT_GRQ	To enable registration, some gatekeepers require sending first RRQ and not GRQ. Set the flag to YES, if this behavior is required by the gatekeeper in your environment. GRQ (Gatekeeper Request) - Gatekeeper discovery is the process an endpoint uses to determine which gatekeeper to register with. RRQ - registration request sent to the gatekeeper. Default: NO Possible values: YES/NO	HW/VE	No
RTCP_FIR_ENABLE	When set to YES, the Full Intra Request (FIR) is sent as INFO (and not RTCP). Default = YES Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
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, the (Picture Loss Indication (PLI) is sent 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
SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD	When set to YES, the RealPresence Collaboration Server sends a busy notification to a SIP audio endpoint or a SIP device when dialing in to the RealPresence Collaboration Server whose audio resource usage exceeded the Port Usage threshold. When set to NO, the system does limit the SIP audio endpoint connections to a certain capacity and will not send a busy notification when the resource capacity threshold is exceeded. Default value: NO Possible value: YES/NO	HW/VE	Yes

General System Flags

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. Setting 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 RealPresence Collaboration Server will not have Microsoft Lync clients participating and will have 3rd party endpoints participating.
	  ◦ When using endpoints (for example, CounterPath Bria 3.2 Softphone) that cannot decrypt SRTP-based audio and video streams if the MKI (Master Key Identifier) field is included in SRTP packets sent by the RealPresence Collaboration Server.
	  We recommend this setting for Maximum Security Environments.
	• YES
	  ◦ When any conferences on the RealPresence Collaboration Server will have both Microsoft Lync clients and Polycom endpoints participating.
	  ◦ Some third-party endpoints might be unsuccessful in participating in conferences with this setting.
	Notes:
	• This system flag must be added and set to YES (default) when Microsoft Office Communicator and Lync clients are used as they all support SRTP with MKI.
	• The system flag must be added and set to NO when Siemens phones (Openstage and ODC WE) are used in the environment as they do not support SRTP with MKI.
	• Polycom endpoints function normally regardless of the setting of this flag.
	Default value: YES
	Possible value: YES/NO
	<Kindly advise on how to minimize this content>
		HW/VE	Yes

General System Flags

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. Endpoint types that do not support widescreen resolutions are automatically identified by the RealPresence Collaboration Server according to their product type and version and will not receive the wide resolution even when the flag is set to YES. When manually added and set to NO, the RealPresence Collaboration Server does not 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 does not 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

General System Flags

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 Possible value: OFF/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 does not 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 is set to 0 (Auto) this flag determines the interval, in seconds after which the RealPresence Collaboration Server will accept both DTMF tones (inband) and digits (outband). Default value: 120	HW/VE	Yes
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:<is listing of example essential?> Participant Name = john.smith Company Domain = maincorp.com SIP_AUTO_SUFFIX_EXTENSION flag value = @maincorp.com Entering john.smith will generate 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

General System Flags

Flag Name	Description	Platform	Add?
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 the request is sent 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 send the Intra request to Microsoft OC endpoints only. Default value: 6 seconds	HW/VE	Yes
SIP_FORMAT_GW_HEADERS_FOR_REDCOM	Controls whether the RealPresence Collaboration Server adds a special gateway prefix and postfix characters to the user 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, video resources remain allocated to participants as long as they are 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 are not guaranteed to participants if they want to add video again. Default value in Microsoft environment: NO Possible values: YES/NO	HW/VE	Yes

General System Flags

Flag Name	Description	Platform	Add?
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
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 is set to YES, the value of this flag is used as the MS Keep-Alive Timer value.	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 Lync registrations.	HW	Yes

General System Flags

Flag Name	Description	Platform	Add?
SYSTEM_BROADCAST_VOLUME	This value is used when the system flag FORCE_SYSTEM_BROADCAST_VOLUME is set to YES. 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	This value is used when the system flag FORCE_SYSTEM_LISTENING_VOLUME is set to YES. 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 will wait 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.		

General System Flags

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: If 99 is configured, the timeout will be identical to the existing timeout value configured 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 RealPresence DMA solution deployment. Default value: NO Possible Values: YES/NO	HW/VE	No
V35_MULTIPLE_SERVICES	This flag must be set to YES if the connection of multiple Serial Gateways to RTM-LAN cards is required. 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 RealPresence Collaboration Server 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 is not reduced). This flag is applicable only when traffic shaping is enabled. Default value: 15 Range: 0-60 ENABLE_RTP_TRAFFIC_SHAPING	HW/VE	Yes
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.		

General System Flags

Flag Name	Description	Platform	Add?
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 will allow a participant to connect to the conference if the allocated 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
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 multiple certificates will be retrieved, one for each IP service. Default value: ONE_CERTIFICATE Possible values: ONE_CERTIFICATE, MULTIPLE_CERTIFICATE
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 is no CRL. • **OPTIONAL** - The system fails the connection request if the certificate is revoked but does not fail the connection request if there is no CRL. • **DISABLED** - Does not check the CRL and does not fail the connection request based on the CRL content. Default value: DISABLED Possible values: ENABLED, OPTIONAL, DISABLED

802.1x Authentication System Flags

Flag Name	Description
802_1X_SKIP_CERTIFICATE_VALIDATION	If the flag value is: • **YES** - The retrieved certificate is not 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 neither displayed as a selectable option nor 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 Alternative Network Address Type (ANAT)

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 Re-invite that is determined by a timer. Default value: 10 seconds Range: 1-60 seconds (values outside this range are rejected and an error message is displayed).

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 will use the same signaling port. Default value: NO Possible value: YES/NO
H323_RAS_IPV6	If the RealPresence Collaboration Server is configured for IPv4 & IPv6 addressing, RAS (Registration, Admission, and Status) messages are sent in both IPv4 and IPv6 format. If the gatekeeper cannot operate in IPv6 addressing mode, registration fails and endpoints cannot 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, this flag must be set to 1.
MS_UPDATE_CONTACT_REMOVE	When the flag value is set to: • YES - The Contact Header is removed from the UPDATE message that is sent periodically to the endpoints. This is required when the SIP Server Type field of the IP Network Service is set as Microsoft. Removal of the Contact Header from the UPDATE message is required specifically by OCS R2. • NO - The Contact Header is included in the UPDATE message. This is the system behavior when the SIP Server Type is set as Generic. This is required when the RealPresence Collaboration Server is configured to accept calls from both Microsoft Lync and Cisco CUCM as CUCM requires the Contact Header. Possible values: YES/NO

CS System Flags

Flag Name	Description
QOS_IP_SIGNALING	Used to select the Diffserv priority of signaling 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 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>
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, this flag must be set to 1.
SIP_TO_TAG_CONFLICT	For use in Microsoft environments. In case of forking, a tag conflict will be resolved when Status 200 OK is received from an answering UA.<require more clarity> 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. Available Layouts

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
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):
	• Conference and chairperson passwords that are displayed in the RMX Web Client or RMX Manager are hidden when viewing the properties of the conference.
	• Automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags:
	  ◦ NUMERIC_CONF_PASS_DEFAULT_LEN
	  ◦ NUMERIC_CHAIR_PASS_ DEFAULT_LEN
	Default value: NO
	Automatic Password Generation Flags

Password Generation Flags

Flag Name	Description
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 is not enforced. No cross reference has been provided here. Please confirm.
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	Defines the frequency with which a user can change a password. Default value: 0 - users do not 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
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

Password Generation Flags

Flag Name	Description
NUMERIC_CHAIR_PASS_ DEFAULT _LEN	Enables or disables the automatic generation of chairperson passwords. The flag value determines the length of the automatically generated passwords. Default value: • 6 - In non-secured mode • 9 - In Ultra Secure Mode. Range: 0 – 16, where 0 disables automatic generation of passwords. Any value other than 0 enables automatic generation of chairperson passwords provided the flag HIDE_CONFERENCE_PASSWORD is set to NO. If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.
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 is set to **NO**. • 1 – 16, default: 6 (Standard Security Mode) • 9 – 16, default: 9 (Ultra Secure Mode). If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	The maximum number of digits that the user 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 is not enforced. Range: 0-16

Password Generation Flags

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 non-secured mode • 9 - In Ultra Secure Mode Any value other than 0 enables automatic generation of conference passwords provided the flag HIDE_CONFERENCE_PASSWORD is set to NO. If the default is used, in nonsecured mode the system will automatically generate 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 do not 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 to the user of the number of days until password expiration. Value: between 0 and 14 days. 0 - password expiry warnings are not displayed. In Ultra Secure Mode, the earliest display - 14 days, the latest 7 days (default).

Password Generation Flags

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 re-using 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
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 - Destination Unreachable Message is sent 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. If the conference is encrypted, the recording link will be encrypted. 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 are disconnected. When set to **NO** (default) and the conference Encryption Profile is set to **Encrypt When Possible**, both the encrypted and non-encrypted 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. If the conference is encrypted, the recording link will be encrypted. 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 is not 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 non-panoramic layouts, control cropping, and striping by adding this flag and setting its value accordingly. Default value: -1 Range: 1-100
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 are not to be forced to 1x1. Default value: YES Possible value: YE/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

Network Quality Icon - Display Customization Flags

Flag Name	Description
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 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 enabled. When set to **YES**, traffic shaping is applied to all ports, resulting in some port capacity reduction in MCUs with MPMRx cards. When set to **NO**, traffic shaping is disabled. Default value: NO Possible values: YES/NO Capacity Reduction During Traffic Shaping
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 (). 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 is not reduced). This flag is applicable only when traffic shaping is enabled. Default value: 15 Range: 0-60 ENABLE_RTP_TRAFFIC_SHAPING

PCM_FECC System Flag

Flag Name	Description
PCM_FECC	Determines whether the DTMF Code, ##, the Arrow Keys (FECC), or both will 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, the Gathering slide is displayed from the time of connection until the end of the Gathering duration period. Default value: 180 seconds Range: 0 - 3600 seconds

Content Connection Flags

Flag Name	Description
CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS	Controls the requests to refresh (intra) the content sent from the RealPresence Collaboration Server to the content sender as a result of refresh requests initiated by other conference participants. 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

Content Connection Flags

Flag Name	Description
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
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 are 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	
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

Network Security System Flags

Flag Name	Description
SIP_FIPS_MODE	This flag controls availability of the PFX/PEM Certificate Method. Range: • YES - PFX/PEM is not available for selection in the user interface. • NO - PFX/PEM is available for selection in the user interface. Default value: • Standard Security Mode - NO • Ultra Secure Mode - YES
SNMP_FIPS_MODE	Controls the availability of DES and MD5 Authentication methods. **Possible**: • YES - DES and MD5 are not available for selection in the user interface. • NO - DES and MD5 are available for selection in the user interface. **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 the last login of the user. Default value: NO Possible values: YES/NO User Login Record
MAX_KEEP_ALIVE_REQUESTS	The number of *KeepAliveTimeout* request intervals for the *Apache* server. In a *Maximum Security Environment* this value must be set to a value of **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 that is connected and the number of requests. **Default**: 0 (This value should **never** be used as the connection time is unlimited.) (If the SESSION_TIMEOUT_IN_MINUTES *System Flag* if configured, RMX Manager will disconnect after the specified period if there is no keyboard or mouse activity.)

Login and Session Management System Flags

Flag Name	Description
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 is terminated if there is no user input or the connection is idle for longer than the number of minutes specified by this flag. If the ULTRA_SECURE_MODE = NO: • Default value: 0 (Feature is disabled) • 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 permanent user lockout until the administrator re-enables the user within the system. Default value: 0 Range: 0 - 480
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 set to **YES** and either of the LAN connections (LAN1 or LAN2) experiences a problem, an active alarm is displayed stating that there is no LAN connection, specifying 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 is set to **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 have changed the default names used by the RealPresence Resource Manager application. Default value: /PlcmWebServices	HW/VE	Yes
EXTERNAL_CONTENT_IP	Enter the IP address of the RealPresence Resource 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 RealPresence Resource Manager global Address Book. When empty, the integration of RealPresence Resource Manager address book with RealPresence Collaboration Server is disabled.	HW/VE	Yes
EXTERNAL_CONTENT_PASSWORD	The password associated with the user name defined for RealPresence Collaboration Server in RealPresence Resource Manager server.	HW/VE	Yes

Global Address Book Integration Flags

Flag Name	Description	Platform	Add?
EXTERNAL_CONTENT_PORT	The RealPresence Resource 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 RealPresence Resource Manager 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 have changed the default names used by the RealPresence Resource 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		
2	PREDEFINED_AUTO_LAYOUT_2		
3	PREDEFINED_AUTO_LAYOUT_3		CP_LAYOUT_1x2VER
4	PREDEFINED_AUTO_LAYOUT_4		CP_LAYOUT_2X2
5	PREDEFINED_AUTO_LAYOUT_5		
6	PREDEFINED_AUTO_LAYOUT_6		CP_LAYOUT_1P5
7	PREDEFINED_AUTO_LAYOUT_7		
8	PREDEFINED_AUTO_LAYOUT_8		CP_LAYOUT_1P7
9	PREDEFINED_AUTO_LAYOUT_9		

Auto Layout – Default Layouts in CP Conferences Flags

No. of Video Participants	Auto Layout Flag	Auto Layout Default	Default Value
10	PREDEFINED_AUTO_LAYOUT_10		CP_LAYOUT_2P8
11	PREDEFINED_AUTO_LAYOUT_11		
12	PREDEFINED_AUTO_LAYOUT_12		CP_LAYOUT_1P12
13	PREDEFINED_AUTO_LAYOUT_13		
14	PREDEFINED_AUTO_LAYOUT_14		
15	PREDEFINED_AUTO_LAYOUT_15		
16	PREDEFINED_AUTO_LAYOUT_16		
17	PREDEFINED_AUTO_LAYOUT_17		
18	PREDEFINED_AUTO_LAYOUT_18		
19	PREDEFINED_AUTO_LAYOUT_19		
20	PREDEFINED_AUTO_LAYOUT_20		

Available Layout Flags

No. of Cells	Layout Flag Value	Layout
1	CP_LAYOUT_1X1	
2	CP_LAYOUT_1X2	
	CP_LAYOUT_1X2HOR	
	CP_LAYOUT_1x2VER	
	CP_LAYOUT_2X1	
	CP_LAYOUT_1X2_FLEX	

Available Layout Flags

No. of Cells	Layout Flag Value	Layout
3	CP_LAYOUT_1P2HOR	
	CP_LAYOUT_1P2HOR_UP	
	CP_LAYOUT_1P2VER	
	CP_LAYOUT_1P2HOR_RIGHT_FLEX	
	CP_LAYOUT_1P2HOR_LEFT_FLEX	
	CP_LAYOUT_1P2HOR_UP_RIGHT_FLEX	
	CP_LAYOUT_1P2HOR_UP_LEFT_FLEX	
4	CP_LAYOUT_2X2	
	CP_LAYOUT_1P3HOR	
	CP_LAYOUT_1P3HOR_UP	
	CP_LAYOUT_1P3VER	
	CP_LAYOUT_2X2_UP_RIGHT_FLEX	
	CP_LAYOUT_2X2_UP_LEFT_FLEX	
	CP_LAYOUT_2X2_DOWN_RIGHT_FLEX	
	CP_LAYOUT_2X2_DOWN_LEFT_FLEX	
	CP_LAYOUT_2X2_RIGHT_FLEX	
	CP_LAYOUT_2X2_LEFT_FLEX	
5	CP_LAYOUT_1P4HOR_UP	
	CP_LAYOUT_1P4HOR	
	CP_LAYOUT_1P4VER	

Available Layout Flags

No. of Cells	Layout Flag Value	Layout
6	CP_LAYOUT_1P5	
8	CP_LAYOUT_1P7	
9	CP_LAYOUT_1P8UP	
	CP_LAYOUT_1P8CENT	
	CP_LAYOUT_1P8HOR_UP	
	CP_LAYOUT_3X3	
	CP_LAYOUT_1TOP_LEFT_P8	
10	CP_LAYOUT_2P8	
	CP_LAYOUT_2TOP_P8	
13	CP_LAYOUT_1P12	
16	CP_LAYOUT_4X4	
20	CP_LAYOUT_4X5	
Overlay Layouts		
2	CP_LAYOUT_OVERLAY_1P1	
3	CP_LAYOUT_OVERLAY_1P2	
	CP_LAYOUT_OVERLAY_ITP	
4	CP_LAYOUT_OVERLAY_1P3	

Call Detail Records

The Polycom® 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 Multi-part CDRS

CDR Tasks

- View the MCU CDR List
- Retrieve and Save a CDR for Viewing
- Retrieve and Save CDRs for Billing and Reporting

Enabling a CDR Backup Alarm

CDRs can be used by businesses to generate billing information and resource usage reports, so saving CDRs may be important. However, CDRs are not included in the MCU system backup, so if CDRs are required for reporting and billing purposes, they should be backed up manually.

The RealPresence Collaboration Server stores the CDRs of up to 2000 conferences. The RealPresence Collaboration Server 4000 stores the details of up to 4000 conferences. When the MCU threshold is close to being exceeded, the MCU can display active alarms before overwriting the older CDRs, allowing you to back up the CDRs before they are deleted.

To enable the CDR backup alarms:

» Set the system flag `ENABLE_CYCLIC_FILE_SYSTEM_ALARMS` to YES.

When the default setting `ULTRA_SECURE_MODE` system flag is set to YES and the file storage threshold limit is reached, an active alarm is triggered with the following message.

“`Backup of CDR files is required`.”

Enabling 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.

To enable the Multi-Part CDR option:

» Set the value of **ENABLE_MULTI_PART_CDR** system flag to **YES**.

To modify the default setting, the flag must be manually added to the System Configuration. For more information, see Managing System Flags .

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.

View the MCU CDR List

Each conference is a separate record in the MCU memory and is archived as a separate CDR file.

To access the MCU CDR List:

» 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

Each conference is a separate record in the MCU memory and is archived as a separate CDR file. To view the content of a single CDR, you must retrieve and save it in a viewable format.

To retrieve and save a CDR for viewing:

1. In RMX Manager, go to **Administration** > **CDR**.
2. To view the CDR for a single conference, select the CDR for the conference and click **Retrieve Formatted** or **Retrieve Formatted XML** depending on which format you prefer
3. Browse to a location to save the file and click **OK**.

   The MCU saves the formatted file to the selected location.
4. Open the saved file

   The file contains general information about the conference, such as the conference name, ID, start time and duration, as well as information about events occurring during the conference, such as adding a new participant, disconnecting a participant or 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.

To retrieve and archive CDRs for billing and reporting:

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 appendix 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: UTF8 Formatted Fields

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 Collaboration Server or external application does the processing and sorting. The Collaboration Server ignores events that it does not recognize, that is, events written in a higher version that do not 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.

The 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.
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 will contain 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 will be subtracted from the GMT Time. 1 - Offset is positive. GMT Offset will be added to the GMT Time.

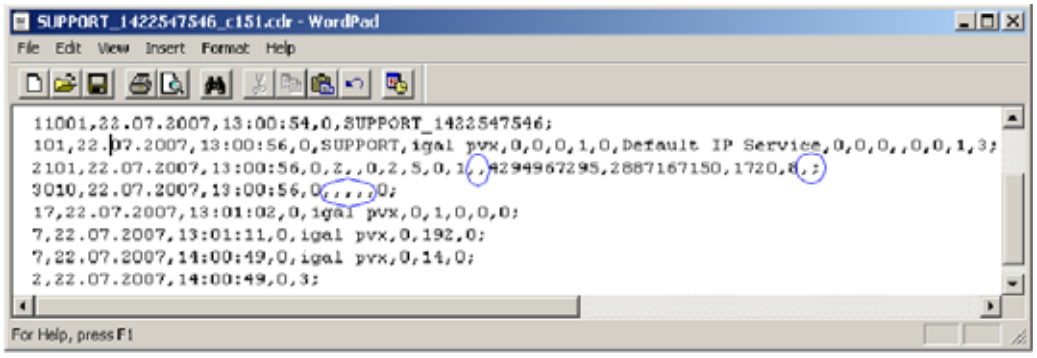
Conference Summary Record Fields

Field	Description
GMT Offset	The time zone difference between Greenwich and the 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 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 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 Collaboration Server's physical location is +4, which will be 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 example below:



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**.

For information of codes used for the various disconnection causes in event descriptions, see Disconnection Cause Values.

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: Event Code

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. For more information about the fields, see Event Fields for Event 1 - CONFERENCE START. Note: There is one CONFERENCE START event per conference. It is 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. For more information about the fields, see Event Fields for Event 2 - CONFERENCE END. Note: There is one CONFERENCE END event per conference, and it is always the last event in the file.
3	ISDN/PSTN CHANNEL CONNECTED	This field is not applicable for RealPresence Collaboration Server, Virtual Edition.
4	ISDN/PSTN CHANNEL DISCONNECTED	This field is not applicable for RealPresence Collaboration Server, Virtual Edition.
5	ISDN/PSTN PARTICIPANT CONNECTED	This field is not applicable for RealPresence Collaboration Server, Virtual Edition.
7	PARTICIPANT DISCONNECTED	A participant disconnected from the conference. For more information about the fields, see Event Fields for Event 7 - PARTICIPANT DISCONNECTED.
10	DEFINED PARTICIPANT	Information about a defined participant, that is, a participant who was added to the conference before the conference started. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT. Note: There is one event for each participant defined before the conference started.

CDR Event Types

Event Code	Event Name	Description
15	H323 CALL SETUP	Information about the IP address of the participant. For more information about the fields, see Event fields for Event 15 - H323 CALL SETUP.
17	H323 PARTICIPANT CONNECTED	An H.323 participant connected to the conference. For more information about the fields, see .
18	NEW UNDEFINED PARTICIPANT	A new undefined participant joined the conference. For more information about the fields, see Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT.
20	BILLING CODE	A billing code was entered by a participant using DTMF codes. For more information about the fields, see Event Fields for Event 20 - BILLING CODE.
21	SET PARTICIPANT DISPLAY NAME	A user assigned a new name to a participant, or an end point sent its name. For more information about the fields, see Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME.
22	DTMF CODE FAILURE	An error occurred when a participant entered a DTMF code. For more information about the fields, see Event Fields for Event 22 - DTMF CODE FAILURE.
23	SIP PARTICIPANT CONNECTED	A SIP participant connected to the conference. For more information about the fields, see .
26	RECORDING LINK	A recording event, such as recording started or recording resumed, occurred. For more information about the fields, see Event fields for Event 26 - RECORDING LINK.
28	SIP PRIVATE EXTENSIONS	Contains SIP Private Extensions information. For more information about the fields, see Event Fields for Event 28 - SIP PRIVATE EXTENSIONS.
30	GATEKEEPER INFORMATION	Contains the gatekeeper caller ID, which makes it possible to match the CDR in the gatekeeper and in the MCU. For more information about the fields, see Event Fields for Event 30 - GATEKEEPER INFORMATION.
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. For more information about the fields, see Event fields for Event 31 - PARTICIPANT CONNECTION RATE.
32	EVENT NEW UNDEFINED PARTY CONTINUE IPV6 ADDRESS	Information about the IPv6 address of the participant's endpoint.

CDR Event Types

Event Code	Event Name	Description
33	PARTY CHAIR UPDATE	Participants connect to the conferences as standard participants and they are designated as chairpersons either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code. For more information about the fields, see Event fields for Event 33 - PARTY CHAIR UPDATE.
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.
35	SVC SIP PARTICIPANT CONNECTED	An SVC user connected over SIP. For more information about the fields, see Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED.
100	USER TERMINATE CONFERENCE	A user terminated the conference. For more information about the fields, see Event Fields for Event 100 - USER TERMINATE CONFERENCE.
101	USER ADD PARTICIPANT	A user added a participant to the conference during the conference. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT.
102	USER DELETE PARTICIPANT	A user deleted a participant from the conference. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
103	USER DISCONNECT PARTICIPANT	A user disconnected a participant. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
104	USER RECONNECT PARTICIPANT	A user reconnected a participant who was disconnected from the conference. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
105	USER UPDATE PARTICIPANT	A user updated the properties of a participant during the conference. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT.
106	USER SET END TIME	A user modified the conference end time. For more information about the fields, see Event Fields for Event 106 - USER SET END TIME.

CDR Event Types

Event Code	Event Name	Description
107	OPERATOR MOVE PARTY FROM CONFERENCE	The participant moved from an Entry Queue to the destination conference or between conferences. For more information about the fields, see Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY.
108	OPERATOR MOVE PARTY TO CONFERENCE	The Collaboration Server User moved the participant from an ongoing conference to another conference. For more information, see Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,OPERATOR ATTEND PARTY TO CONFERENCE.
109	OPERATOR ATTEND PARTY	The Collaboration Server User moved the participant to the Operator conference. For more information, see Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY.
111	OPERATOR BACK TO CONFERENCE PARTY	The Collaboration Server User moved the participant back to his Home (source) conference. For more information, see Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY.
112	OPERATOR ATTEND PARTY TO CONFERENCE	The Collaboration Server User moved the participant from the Operator conference to another conference. For more information, see Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,OPERATOR ATTEND PARTY TO CONFERENCE.
1001	NEW UNDEFINED PARTICIPANT CONTINUE 1	Additional information about a NEW UNDEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1.
2001	CONFERENCE START CONTINUE 1	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 2001 - CONFERENCE START CONTINUE 1.
2007	PARTICIPANT DISCONNECTED CONTINUE 1	Additional information about a PARTICIPANT DISCONNECTED event. For more information about the fields, see Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1.
2010	DEFINED PARTICIPANT CONTINUE 1	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1,USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1.
2011	RESERVED PARTICIPANT CONTINUE PV6 ADDRESS	Additional information about a DEFINED PARTICIPANT event that includes the IPv6 addressing of the defined participant. For more details, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1,USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1.

CDR Event Types

Event Code	Event Name	Description
2012	RESERVED PARTICIPANT CONTINUE 2	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Events 2011, 2012, and 2016.
2015	USER UPDATE PARTICIPANT CONTINUE 1	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1,USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1
2016	USER UPDATE PARTICIPANT CONTINUE 2	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Event Fields for Events 2011, 2012, and 2016.
2101	USER ADD PARTICIPANT CONTINUE 1	Additional information about a USER ADD PARTICIPANT event.
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.
3010	PARTICIPANT INFORMATION	The contents of the participant information fields. For more information about the fields, see Event Fields for Event 3010 - PARTICIPANT INFORMATION.
5001	CONFERENCE START CONTINUE 4	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 5001 - CONFERENCE START CONTINUE 4. Note: An additional CONFERENCE START CONTINUE 4 event will be 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.

CDR Event Types

Event Code	Event Name	Description
6001	CONFERENCE START CONTINUE 5	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 6001 - CONFERENCE START CONTINUE 5.
11001	CONFERENCE START CONTINUE 10	Additional information about a CONFERENCE START event. This event contains the Display Name. For more information about the fields, see Event Fields for Event 11001 - CONFERENCE START CONTINUE 10.

Event Specific Fields

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 was not a dial-out manually conference, that is, the MCU initiates the communication with dial-out participants, and the user does not need to connect them manually.
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 was not 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**.

Event Fields for Event 1 - CONFERENCE START

Field	Description
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
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 could not 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.
Connect Initiator	Indicates who initiated the connection, as follows: 0 - 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

Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED

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.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.

Event fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED

Field	Description
Disconnect Initiator	Indicates who initiated the disconnection, as follows: 0 - 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 could not 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.
Remote Communication Mode	Note: This field is only relevant to ISDN-video participants. The remote communication mode in H.221 format.

Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED

Field	Description
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 are not compatible with the conference video parameters 12 - H.323 card failure 13 - The conference video settings are not compatible with the endpoint capabilities 14 - The new conference settings are not 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 could not be established 24 - The endpoint closed its video channels 25 - The participant video settings are not compatible with the conference protocol 26 - The endpoint could not re-open 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 disconnection cause. For more information about possible values, see Disconnection Cause Values.
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 is **not** an Audio Only participant 1 - The participant is an Audio Only participant 255 - Unknown
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 **Notes:** • 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.

Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT

Field	Description
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.
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.

Event fields for Event 15 - H323 CALL SETUP

Field	Description
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 could not connect the video channels and is connected via audio only 10 - Connected with problem 11 - Redialing
Capabilities	Not supported. Always contains the value 0.

Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED

Field	Description
Remote Communication Mode	Not supported. Always contains the value 0.
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 are not compatible with the conference video parameters 13 - The conference video settings are not compatible with the endpoint capabilities 14 - The new conference settings are not 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 could not be established 24 - The endpoint closed its video channels 25 - The participant video settings are not compatible with the conference protocol 26 - The endpoint could not re-open 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.
Net Channel Width	Not supported. Always contains the value 0.

Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
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 is **not** 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.
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.

Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
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 are not the participant is an undefined participant, as follows: 0 - The participant is not an undefined participant. 2 - The participant is an undefined participant.
Node Type	The node type, as follows: 0 - MCU 1 - Terminal
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

Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
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 did not press any key.
Correct Data	The correct DTMF code, if known.
Failure Type	The type of DTMF failure, as follows: 2 - The participant did not enter the correct conference password. 6 - The participant did not enter the correct chairperson password. 12 - The participant did not 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.
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 the trusted element will insert.

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 is not 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.

Event fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION

Field	Description
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.
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 could not 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

Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED

Field	Description
Audio Codec	SAC, Other
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
Voice Mode	Indicates whether or not the participant is an Audio Only participant, as follows: 0 - The participant is not an Audio Only participant 1 - The participant is an Audio Only participant 255 - Unknown

Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,OPERATOR ATTEND PARTY TO CONFERENCE

Field	Description
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 SubService 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.
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.

Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,OPERATOR ATTEND PARTY TO CONFERENCE

Field	Description
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 is 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
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.

Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,OPERATOR ATTEND PARTY TO CONFERENCE

Field	Description
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 is **not** 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. Collaboration Servers 2000/4000: 5 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
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

Event Fields for Event 2001 - CONFERENCE START CONTINUE 1

Field	Description
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**.
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.

Event Fields for Event 2001 - CONFERENCE START CONTINUE 1

Field	Description
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.
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.

Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1

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.
Video Protocol	The video protocol used by the participant, as follows: 1 - H.261 2 - H.263 4 - H.264 255 - Auto

Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1,USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1

Field	Description
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 are not the participant is an undefined participant, as follows: 0 - The participant is not 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.
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 is **not** 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 e-mail 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
Note: When this event occurs as the result of a change to the value of one of the event fields, the event will only contain the value of the modified field. All other fields will be empty.	
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.

Event Fields for Event 5001 - CONFERENCE START CONTINUE 4

Field	Description
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.

Event Fields for Event 6001 - CONFERENCE START CONTINUE 5

Field	Description
Encryption	Indicates the conference encryption setting, as follows: 0 - The conference is **not** 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.

Active Alarms

The following table describes the active alarms the RealPresence Collaboration Server may experience.

Active Alarms

Alarm Text	Alarm Description
A matching activation key is required. To cancel the upgrade process, reset the Collaboration Server	The system upgrade requires that a valid activation key be entered. If none is available, resetting the Collaboration Server will cancel the upgrade and return the Collaboration Server to the previous version.
The card type in slot <n> is not compatible with RMX version, card will not be powered on	A Collaboration Server Appliance Edition was upgraded to versions 8.6, yet it contains an MPMx media card(s) which is not supported. The card is not powered on. Note: Applicable to Collaboration Servers 2000/4000.
A new activation key was loaded. Reset the system.	A new activation key was loaded: Reset the MCU.
A new version was installed. Reset the system.	A new version was installed: Reset the MCU.
Alarm generated by a Central Signaling component	A system alert was generated by a component of the Central Signaling.
Alarm generated by an internal component	A system alert was generated by an internal system component.
Allocation mode was modified	
Automatic reset is unavailable in Safe Mode	The system switches to safe mode if many resets occur during startup. To prevent additional resets, and allow the system to complete the startup process the automatic system resets are blocked.
Backup of audit files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that audit files need to be backed up.
Backup of CDR files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that CDR files need to be backed up.
Backup of log files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that log files need to be backed up.

Active Alarms

Alarm Text	Alarm Description
Bios version is not compatible with Ultra Secure Mode.	The current BIOS version is not compatible with Ultra Secure Mode (ULTRA_SECURE_MODE=YES). Note: Applicable to Collaboration Servers 2000/4000/1800
Card configuration event	Note: Applicable to Collaboration Servers 2000/4000
Card failed to switch to Enhanced Secure Mode	Card failure occurred when the system was set to Ultra Secure Mode (ULTRA_SECURE_MODE=YES). Note: Applicable to Collaboration Servers 2000/4000/1800
Card failure	Possible reasons for the card failure: • Resetting Card • Resetting component • Unknown shelf error • Unknown card error Note: Applicable to Collaboration Servers 2000/4000
Card not found	This occurs when the system does not receive an indication about the card (since it does not exist…) usually when the card was removed from the MCU and the system did not have a chance to recalculate it resources. Note: Applicable to Collaboration Servers 2000/4000
Card not responding	Possible reasons for the card not responding: • No connection with MPM card. • No connection with the Switch. Note: Applicable to Collaboration Servers 2000/4000
Cards wrong file's mode	Note: Applicable to Collaboration Servers 2000/4000
Central signaling component failure	Possible explanations: • Central signaling component failure; unit type: [NonComponent\CSMngnt\CSH323\ Polycom® ContentConnect™IP] • Central signaling component failure; unit type: (invalid: [NonComponent\CSMngnt\CSH323\ ContentConnect IP]) • Central signaling component failure - Invalid failure type. Unit id: [id], Type: [NonComponent\CSMngnt\CSH323\ContentConnect IP], Status: [Ok\Failed\Recovered] • Central signaling component failure - Invalid failure type
Central Signaling indicating Faulty status	Central signaling failure detected in IP Network Service.
Central Signaling indicating Recovery status	
Central Signaling startup failure	Central Signaling component is down.
Conference Encryption Error	

Active Alarms

Alarm Text	Alarm Description
Configuration of external database did not complete.	Check the configuration of the external DB.
Could not complete MPM Card startup procedure	Possible explanations: • Unit loading confirmation was not received. • No Media IP for this card. • Media IP Configuration confirmation was not received. • Unspecified problem. Check the card slot and reset the card. Note: Applicable to Collaboration Servers 2000/4000
Could not complete RTM ISDN Card startup procedure	The RTM ISDN card cannot complete its startup procedure (usually after system reset). Check the card slot and reset the card. Note: Applicable to Collaboration Servers 2000/4000/1800
CPU IPMC software was not updated.	Turn off the MCU and then turn it on.
CPU slot ID not identified	The CPU slot ID required for Ethernet Settings was not provided by the Shelf Management.
D channel cannot be established	
DEBUG mode enabled	Possible explanations: • System is running in DEBUG mode. • System DEBUG mode initiated. In this mode, additional prints are added and Startup and Recovery Conditions are different then Non Debug Mode. Change the DEBUG_MODE flag value to NO and reset the Collaboration Server.
DEBUG mode flags in use	The system is using the DEBUG CFG flags.
DMA not supported by IDE device	Possible explanations: • DMA (direct memory access) not supported by IDE device: Incompatible flash card / hard disk being used. • Flash card / hard drive are not properly connected to the board / one of the IDE channels is disconnected. • DMA was manually disabled for testing.
DNS configuration error	Check the DNS configuration.
DNS not configured in IP Network Service	Configure the DNS in the IP Network Services.
Encryption Server Error. Failed to generate the encryption key	FIPS 140 test failed while generating the new encryption key.
Error in external database certificate	

Active Alarms

Alarm Text	Alarm Description
Error reading MCU time	Failed to read MCU time configuration file ([status]). Manually configure the MCU Time in the Collaboration Server Web Client or RMX Manager Manager application.
eUserMsgCode_Cs_EdgeServerDnsFailed	
eUserMsgCode_Cs_SipTLS_CertificateHasExpired	
eUserMsgCode_Cs_SipTLS_CertificateSubjNameIsNotValid_Or_DnsFailed	
eUserMsgCode_Cs_SipTLS_CertificateWillExpireInLessThanAWeek	
eUserMsgCode_Cs_SipTLS_FailedToLoadOrVerifyCertificateFiles	
eUserMsgCode_Cs_SipTLS_RegistrationHandshakeFailure	
eUserMsgCode_Cs_SipTLS_RegistrationServerNotResponding	
Event Mode Conferencing resources deficiency due to inappropriate license. Please install a new license	
External NTP servers failure	The MCU could not connect to any of the defined NTP server for synchronization due to the remote server error or network error or configuration error. Change the configuration of the NTP server.
Failed to access DNS server	Failed to access DNS server.
Failed to configure the Media card IP address	Possible reasons for the failure: • Failure type: [OK Or Not supported. • Does not exist Or IP failure. • Duplicate IP Or DHCP failure. • VLAN failure Or Invalid: [status_Number].
Failed to configure the Users list in Linux	The authentication process did not start. Use the Restore to factory Defaults to recover.
Failed to connect to application server	Possible reasons for the failure: • Failed to connect to application server: • Failed to establish connection to server, url = [url].
Failed to connect to recording device	The MCU could not connect to the defined recording device due to configuration error or network error.
Failed to connect to SIP registrar	Cannot establish connection with SIP registrar.

Active Alarms

Alarm Text	Alarm Description
Failed to create Default Profile	Possible reasons for the failure: • Failed to validate the default Profile. • Failed to add the default Profile. Possible action: • Restore the Collaboration Server configuration from the Backup. • Use the Non-Comprehensive Restore To Factory Defaults operation.
Failed to initialize system base mode	
Failed to initialize the file system	Possible reasons for the failure: • Failed to initialize the file system. • Failed to initialize the file system and create the CDR index. Reset the MCU.
Failed to open Users list file	Restore the MCU configuration or re-define the user.
Failed to register with DNS server	Check the DNS configuration.
Failed to subscribe with the OCS, therefore the A/V Edge Server URI was not received	
Failure in initialization of SNMP agent.	
Fallback version is being used	Fallback version is being used. Restore current version. Version being used: [running version]; Current version: [current version].
Fan Problem Level Critical	
Fan Problem Level Major	
File error	Possible reasons for the file error: • XML file does not exist [file name]; Error no: [error number]. • Not authorized to open XML file [file name]; Error no: [error number]. • Unknown problem in opening XML file [file name]; Error no: [error number]. • Failed to parse XML file [file name].
File system scan failure	File system scan failure: Failed to scan [file system path]. Multiple occurrences may point to a hardware problem. System is functioning.
File system space shortage	File system space shortage: Out of file system space in [file system path]; Free space: [free space percentage]% ([free space] Blocks) - Minimum free space required: [minimum free space percentage]% ([minimum free space] Blocks).
FIPS 140 failure	
FIPS 140 test result not received	

Active Alarms

Alarm Text	Alarm Description
Gatekeeper failure	Possible reasons for the Gatekeeper failure: • Failed to register to alternate Gatekeeper. • Gatekeeper discovery state. - Check GK IP address (GUI, ping) • Gatekeeper DNS Host name not found. • Gatekeeper Registration Timeout. • Gatekeeper rejected GRQ due to invalid revision. • Gatekeeper rejected GRQ due to resource unavailability. • Gatekeeper rejected GRQ due to Terminal Exclusion. • Gatekeeper rejected GRQ due to unsupported feature. • Gatekeeper rejected GRQ. Reason 18. • Gatekeeper rejected RRQ due to Discovery Required. • Gatekeeper rejected RRQ due to duplicate alias. - Check duplicate in aliases or in prefixes • Gatekeeper rejected RRQ due to Generic Data. • Gatekeeper rejected RRQ due to invalid alias. • Gatekeeper rejected RRQ due to invalid call signaling address. • Gatekeeper rejected RRQ due to invalid endpoint ID. • Gatekeeper rejected RRQ due to invalid RAS address. • Gatekeeper rejected RRQ due to invalid revision. • Gatekeeper rejected RRQ due to invalid state. • Gatekeeper rejected RRQ due to invalid terminal alias. • Gatekeeper rejected RRQ due to resource unavailability. • Gatekeeper rejected RRQ due to Security Denial. • Gatekeeper rejected RRQ due to terminal type. • Gatekeeper rejected RRQ due to unsupported Additive Registration. • Gatekeeper rejected RRQ due to unsupported feature. • Gatekeeper rejected RRQ due to unsupported QOS transport. • Gatekeeper rejected RRQ due to unsupported transport. • Gatekeeper rejected RRQ. Full registration required. • Gatekeeper rejected RRQ. Reason 18. • Gatekeeper Unregistration State. • Registration succeeded. Check the Gatekeeper configuration. Note: Applicable to Collaboration Servers 2000/4000/1800
GUI System configuration file is invalid xml file	The XML format of the system configuration file that contains the user interface settings is invalid.
Hard disk error	Hard disk not responding.
Hot Backup: Master-Slave configuration conflict.	Possible reasons: • When both the MCUs are configured as Master or as Slave • The slave Collaboration Server is defined with the same IP as the Master.

Active Alarms

Alarm Text	Alarm Description
Hot backup: Network issue	
Hot Backup: Paired MCU is unreachable.	
Initialization of ice stack failed	
Insufficient resources	The number of resources in the license is higher than the actual system resources. Check the media cards or insert a media card.
Insufficient UDP Ports	When defining fixed port, the number of defined UDP ports is lower than the required ports. Configure additional ports.
Internal System configuration during startup	System configuration during startup. Wait until Collaboration Server startup is completed.
Invalid System Configuration	
IP addresses of Signaling Host and Control Unit are the same	IP addresses of Signaling Host and Control Unit are identical. Assign different IP addresses to the Signaling Host and Control Unit.
IP Network Service added	
IP Network Service configuration modified	IP Network Service was modified. Reset the MCU.
IP Network Service deleted	IP Network Service was deleted. Reset the MCU.
IP Network Service not found	IP Service not found in the Network Services list. Configure the IP Network Service.
IPMC software upgrade in component	
IPS 140 test result not received	
ISDN/PSTN Network Services configuration changed	New ISDN (audio/video) configuration. Reset the MCU for the change to take effect. Note: Applicable to Collaboration Servers 2000/4000/1800
LDAP TLS: Failed to connect to OSCP responder	
Management Network not configured	Configure the Management Network.
Missing Central Signaling configuration	Configure the central signaling.
Missing Central Signaling IP configuration	
MPL startup failure. Authentication not received.	Authentication was not received from Switch. Check the switch card.

Active Alarms

Alarm Text	Alarm Description
MPL startup failure. Management Network configuration not received.	Management Network message was not received. Check the Switch card.
Network interface is not configured. New interface need to be chosen	
Network traffic capture is on	
New certificate for CS need Collaboration Server reset to take effect	
No clock source	The system could not use any of the connected ISDN-video spans as clock source. Check the ISDN (audio/video) Settings. Note: Applicable to Collaboration Servers 2000/4000/1800
No default ISDN/PSTN Network Service defined in ISDN/PSTN Network Services list	Set a default ISDN (audio/video) Network Service. Note: Applicable to Collaboration Servers 2000/4000/1800
No default IVR Service in IVR Services list	No default IVR Service in IVR Services list. Ensure that one conference IVR Service and one EQ IVR Service are set as default.
No IP Network Services defined	IP Network Service parameters missing. Configure the IP Network Service.
No ISDN/PSTN Network Services defined	No ISDN (audio/video) Network Services were defined or no default ISDN (audio/video) Network was defined. Note: Applicable to Collaboration Servers 2000/4000/1800
No LAN connection	
No License for ISDN/PSTN. Please activate the RTM ISDN card through Polycom website	Configure the ISDN (audio/video) Network Service. Note: Applicable to Collaboration Servers 2000/4000/1800
No response from Central Signaling	No connection with central signaling.
No response from RTM ISDN card	Note: Applicable to Collaboration Servers 2000/4000/1800
No RTM-LAN or RTM-ISDN installed. One of these cards must be installed in the RealPresence Collaboration Server (RMX) 4000	Note: Applicable to Collaboration Servers 2000/4000/1800
No usable unit for audio controller	No media card is installed, or the media card installed is not functioning. Install the appropriate media card.
OCS Registration failed	
Password expiration warning	
Please install a newer version	
Port configuration was modified	

Active Alarms

Alarm Text	Alarm Description
Power off	
Power Problem Level Critical	
Power Problem Level Major	
Product activation failure	Assign a new activation key.
Product Type mismatch. System is restarting.	The user is alerted to a mismatch between the product type that is stored in MCU software and the product type received from another system component. In such a case the system is automatically restarted.
Received Notification failed	
Recording device has disconnected unexpectedly	
Red Alarm	When a certain timeout will be reached (after startup), MCMS will go over the configured Spans. A configured Span that is related to nonexistent card – will produce a 'RED_ALARM' Alert. Similarly on HotSwap: if an RTM card (or an MPM that has an RTM extension) is removed, MCMS will go over the configured Spans. A configured Span that is related to the removed card – will produce a 'RED_ALARM' Alert.
Requested changes to the certification repository were not completed. Repository must be updated to implement these changes.	
Resource process failed to request the Meeting Room list during startup.	Without the Meeting Rooms list, the system cannot allocate the appropriate dial numbers, Conference ID etc. and therefore cannot run conferences.
Restore Failed	Restoring the system configuration has failed as the system could not locate the configuration file in the selected path, or could not open the file.
Restore Succeeded	Restoring the system configuration has succeeded. Reset the MCU.
Restoring Factory Defaults. Default system settings will be restored once Reset is completed	Default system settings will be restored once Reset is completed.
Collaboration Server fails to connect to Active Directory server.	
Collaboration Server is uploading the version file. To cancel the upload and the upgrade, reset the Collaboration Server	
Collaboration Server user/password list will be reset	

Active Alarms

Alarm Text	Alarm Description
RTM ISDN card not found	RTM ISDN card is missing. Install the RTM ISDN card. Note: Applicable to Collaboration Servers 2000/4000/1800
RTM ISDN card startup procedure error	The RTM ISDN card cannot complete its startup procedure (usually after system reset). Check the card and/or reset the card. Note: Applicable to Collaboration Servers 2000/4000/1800
Secured SIP communication failed	Error status (408) received from SIP proxy.
Security mode failed. Certificate has expired.	
Security mode failed. Certificate host name does not match the Collaboration Server host name.	
Security mode failed. Certificate is about to expire.	
Security mode failed. Certificate not yet valid.	
Security mode failed. Error in certificate file.	
Service Request failed	
Sip connection for conference event package fail	The EventPackage SIP connection to this Collaboration Server within the cascading topology, failed to establish following 3 consecutive attempts. The conference and VMR are specified.
SIP registrations limit reached	SIP registrations limit reached.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the Collaboration Server in the certificate file is different from the FQDN name defined in the OCS.
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the Collaboration Server. Possible causes are: • Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt • Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt • The contents of the certificate file does not match the system parameters

Active Alarms

Alarm Text	Alarm Description
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the Collaboration Server, preventing the Registration of the Collaboration Server to the OCS.
SIP TLS: Registration server not responding	This alarm is displayed when the Collaboration Server does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: • The Collaboration Server FQDN name is not defined in the OCS pool, or is defined incorrectly. • The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. • The Collaboration Server FQDN name is not defined in the DNS server. Ping the DNS using the Collaboration Server FQDN name to ensure that the Collaboration Server is correctly registered to the DNS.
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: • Incorrect IP address of the SIP server • The SIP server listening port is other than the one defined in the system • The OCS services are stopped
Software upgrade in component	
SSH is enabled	
SWITCH not responding	Check the Switch card.
System configuration changed. Please reset the MCU	
System Configuration modified	System configuration flags were modified. Reset the MCU.
System resources of Audio ports usage has exceeded Port Gauge threshold	Note: Applicable to Collaboration Servers 2000/4000
System resources of Video ports usage has exceeded Port Gauge threshold	Note: Applicable to Collaboration Servers 2000/4000
System resources usage has exceeded Port Gauge threshold	
Temperature Level - Critical	Temperature has reached a critical level.
Temperature Level - Major	Temperature has reached a problematic level and requires attention.
The Log file system is disabled because of high system CPU usage	
The MCCF channel is not connected	

Active Alarms

Alarm Text	Alarm Description
The software contains patch(es)	The software contains patch(es).
The system has been configured for Ultra Secure Mode, but communication is not secured until a TLS certificate is installed and the MCU is set to Secured Communication.	Although the System Flag ULTRA_SECURE_MODE is set to YES, the Ultra Secure Mode is not fully implemented as the TLS certificate was not installed. Please install the TLS certificate and set the MCU to Secured Communication Mode to fully enable the Enhanced Security Environment.
Unable to connect to Exchange Server.	
User Name SUPPORT cannot be used in Enhanced Security Mode	
Version upgrade is in progress	
Voltage problem	Possible reasons for the problem: • Card voltage problem. • Shelf voltage problem. • Voltage problem
Warning: Upgrade started and SAFE Upgrade protection is turned OFF	
Yellow Alarm	Problem sending/receiving data from/to network. Check the cables.

Disconnection Causes

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

Call Disconnection Causes

Disconnection Cause	Description
Disconnected by User	The user disconnected the endpoint from the conference.
Remote device did not open the encryption signaling channel	The endpoint did not open the encryption signaling channel.
Remote devices selected encryption algorithm does not match the local selected encryption algorithm	The encryption algorithm selected by the endpoint does not match the MCU's encryption algorithm.
Resources deficiency	Insufficient resources available.
Call close. Call closed by MCU	The MCU disconnected the call.
H323 call close. No port left for audio	Insufficient audio ports.
H323 call close. No port left for video	The required video ports exceed the number of ports allocated to video in fixed ports.
H323 call close. No port left for FECC	The required data ports exceed the number of ports allocated to data in fixed ports.
H323 call close. No control port left	The required control ports exceed the number of ports allocated to control data in fixed ports.
H323 call close. No port left for videocont	The required video content ports exceed the number of ports allocated to video content in fixed ports.

Call Disconnection Causes

Disconnection Cause	Description
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 is not registered in the gatekeeper.
H323 call closed. ARQ timeout	The endpoint sent an ARQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. DRQ timeout	The endpoint sent a DRQ message to the gatekeeper, but the gatekeeper did not 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 did not answer. Possible causes can be due to network problems, the gatekeeper could not find the endpoint's address, or the endpoint was busy or unavailable (for example, the “do not 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. Call failed prior or during the capabilities negotiation stage	The endpoint did not send its capabilities to the gatekeeper.
H323 call closed. Audio channels didn't open before timeout	The endpoint did not open the audio channel.
H323 call closed. Remote sent bad capability	There was a problem in the capabilities sent by the endpoint.

Call Disconnection Causes

Disconnection Cause	Description
H323 call closed. Local capability wasn't accepted by remote	The endpoint did not 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 slave problem	A People + 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 does not 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 are not compatible with the conference settings.
SIP card rejected channels	The IP card could not open the media channels.
SIP client error 400	The endpoint sent a SIP Client Error 400 (Bad Request) response. The request could not 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 cannot accept the call because it does not 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.
SIP client error 409	The endpoint sent a SIP Client Error 409 (Conflict) response. The request could not 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.

Call Disconnection Causes

Disconnection Cause	Description
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 did not understand the protocol extension specified in a Require header field.
SIP client error 481	The endpoint sent a SIP Client Error 481 (Call/Transaction Does Not 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 does not wish to or cannot participate.
SIP global failure 604	A SIP Global Failure 604 (Does Not Exist Anywhere) response was returned. The server has authoritative information that the user indicated in the Request-URI does not 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.

Call Disconnection Causes

Disconnection Cause	Description
SIP not found	The endpoint was not found. The server has definitive information that the user does not 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 was not successful, but alternative services are possible.
SIP remote cancelled call	The endpoint canceled the call.
SIP remote closed call	The endpoint ended the call.
SIP remote stopped responding	The endpoint is not responding.
SIP remote unreachable	The endpoint could not be reached.
SIP request terminated	The endpoint terminated the request. The request was terminated by a BYE or CANCEL request.
SIP request timeout	The request was timed out.
SIP 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.
SIP server error 501	The SIP server sent a SIP Server Error 501 (Not Implemented) response. The server does not support the functionality required to fulfill the request.
SIP 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.
SIP 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.
SIP server error 504	The SIP server sent a SIP Server Error 504 (Server Time-out) response. The server did not receive a timely response from an external server it accessed in attempting to process the request.

Call Disconnection Causes

Disconnection Cause	Description
SIP server error 505	The SIP server sent a SIP Server Error 505 (Version Not Supported) response. The server does not support, or refuses to support, the SIP protocol version that was used in the request.
SIP temporarily not available	The participant's endpoint was contacted successfully but the participant is currently unavailable (e.g., not logged in or logged in such a manner as to preclude communication with the participant).
SIP remote device did not respond in the given time frame	The endpoint did not respond in the given time frame.
SIP trans error TCP Invite	A SIP Invite was sent via TCP, but the endpoint was not 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

ISDN Disconnection Causes

Number	Summary	Description
1	Unallocated (unassigned number)	No route to the number exists in the ISDN network or the number was not found in the routing table. • Ensure that the number appears in the routing table. • Ensure that it is 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 does not 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 cannot 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 does not accept the channel most recently identified.

ISDN Disconnection Causes

Number	Summary	Description
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 has not answered the call.
19	No Answer from User (User Alerted)	Called user has received call alert, but has not 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.
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 does not support this cause value.
26	Non-Selected User Clearing	The incoming call has not been assigned to the user.
27	Destination Out-of-Order	Messages cannot 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 cannot 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.

ISDN Disconnection Causes

Number	Summary	Description
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 is not available. Alternative circuits or channels are not 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, cannot be provided.
50	Requested Facility Not Subscribed	A supplementary service has been requested that the user is not authorized to use.
53	Outgoing Calls Barred Within Closed User Group (CUG)	Outgoing calls are not permitted for this member of the CUG.
55	Incoming Calls Barred within CUG	Incoming calls are not permitted for this member of the CUG.
57	Bearer Capability Not Authorized	A bearer capability has been requested that the user is not authorized to use.
58	Bearer Capability Not Presently Available	A bearer capability has been requested that the user is not 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 is not supported.
66	Channel Type Not Implemented	The requested channel type is not supported.
69	Requested Facility Not Implemented	The requested supplementary service is not supported.

ISDN Disconnection Causes

Number	Summary	Description
70	Only Restricted Digital Information Bearer Capability is Available (national use)	Unrestricted (64kb) bearer service has been requested but is not 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 Does Not 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 Does Not 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 cannot be executed by the network as a result of no call suspended.
86	Call Having the Requested Call Identity Has Been Cleared	A RESUME message cannot 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 is not 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 does not 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 is not 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

ISDN Disconnection Causes

Number	Summary	Description
99	An Information Element or Parameter Does Not Exist or is Not Implemented	A message was received containing elements or parameters that are not 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 are not 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 was not recognized.
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

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 could not be established between the MCU and the remote device

Disconnection Cause Values

Value	Call Disconnection Cause
53	Remote device did not open the encryption signaling channel
59	The remote devices' selected encryption algorithm does not 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
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 has not 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. Master slave problem
251	SIP timer popped out
252	SIP card rejected channels
253	SIP capabilities don't match
254	SIP remote closed call

Disconnection Cause Values

Value	Call Disconnection Cause
255	SIP remote cancelled 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
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

Disconnection Cause Values

Value	Call Disconnection Cause
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
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

Hardware Monitoring

For the Appliance Edition of the Polycom® RealPresence® Collaboration Server (RMX) 1800/2000/4000, use the **Hardware Monitor** to monitor the status and properties of MCU hardware components.

Viewing 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

To view the status of hardware components via the Hardware Monitor:

» 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.

hardware Monitor Fields

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.
Voltage	The voltage threshold of the hardware component; either **Normal** or **Major**.

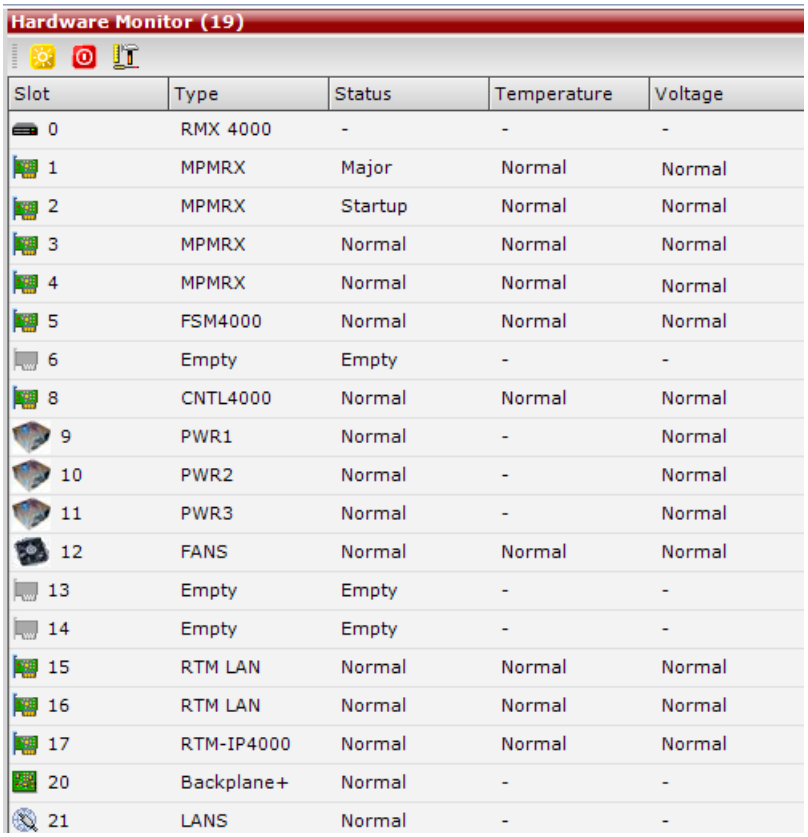
Identifying the Types of Video Cards in an MCU

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 does not apply to a RealPresence Collaboration Server 1800.

To identify the types of cards within an MCU:

1 In the **RMX Management** section, click Hardware Monitor .



Slot	Type	Status	Temperature	Voltage
0	RMX 4000	-	-	-
1	MPMRX	Major	Normal	Normal
2	MPMRX	Startup	Normal	Normal
3	MPMRX	Normal	Normal	Normal
4	MPMRX	Normal	Normal	Normal
5	FSM4000	Normal	Normal	Normal
6	Empty	Empty	-	-
8	CNTL4000	Normal	Normal	Normal
9	PWR1	Normal	-	Normal
10	PWR2	Normal	-	Normal
11	PWR3	Normal	-	Normal
12	FANS	Normal	Normal	Normal
13	Empty	Empty	-	-
14	Empty	Empty	-	-
15	RTM LAN	Normal	Normal	Normal
16	RTM LAN	Normal	Normal	Normal
17	RTM-IP4000	Normal	Normal	Normal
20	Backplane+	Normal	-	-
21	LANS	Normal	-	-

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, i.e. temperatures and main power sensors.

6 Click Close to return to the **Hardware Monitor**.

Viewing 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)

To view the properties of a hardware component:

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**.**

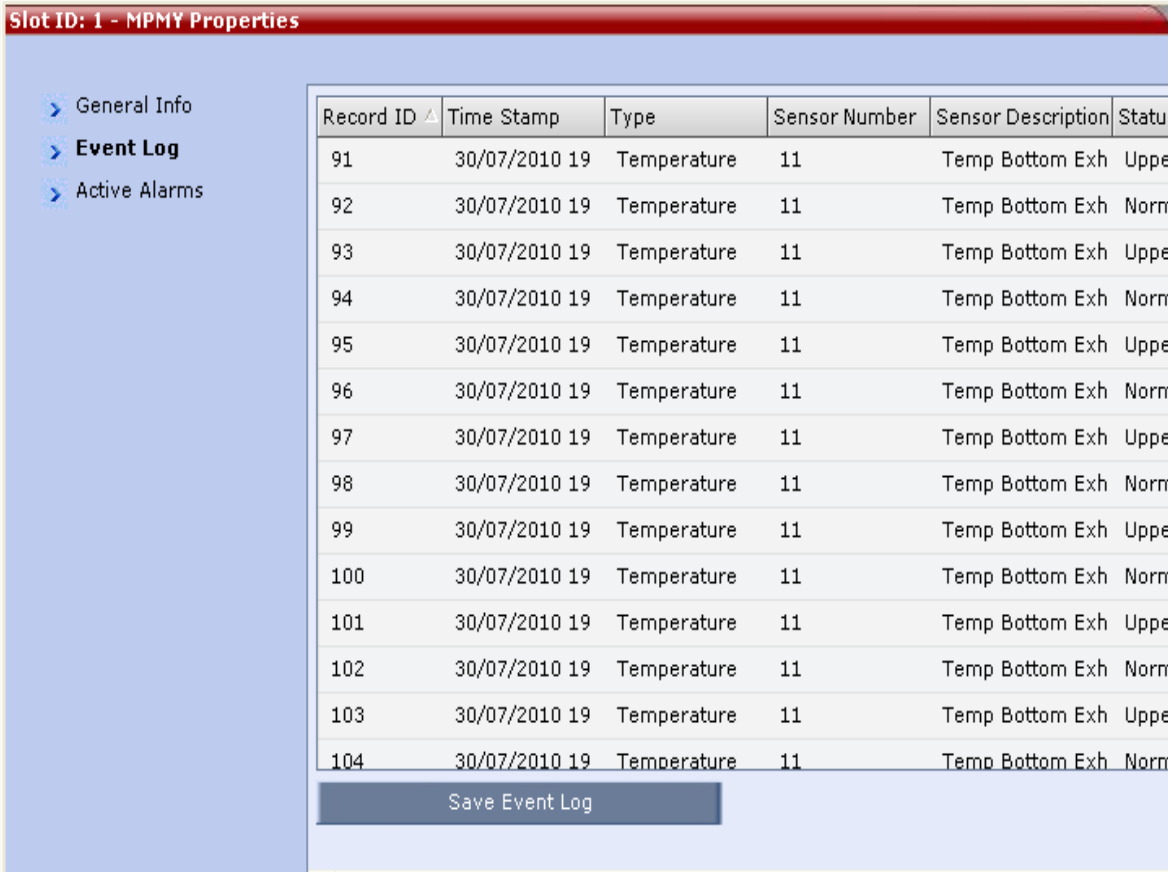
   For more information about the hardware properties displayed, see the hardware guide for the RMX appliance model you have.

Viewing 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 does not apply to a RealPresence Collaboration Server 1800.

To view an MCU event log:

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.



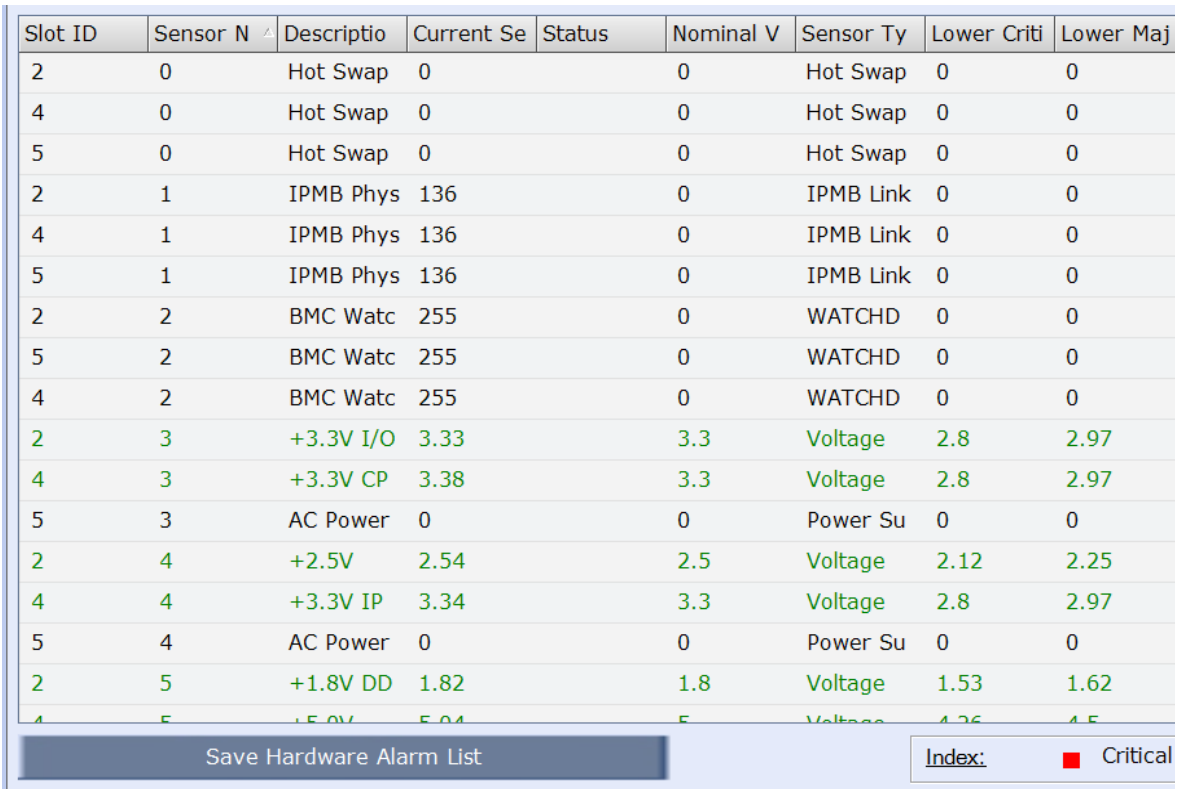
5 The logged events can be saved to a *.xls file by clicking Save Event Log. It is not possible to save individual or multiple selected events; the entire log file must be saved.

Viewing Active Alarms for an MCU

For RealPresence Collaboration Server 2000/4000 models, use the **Hardware Monitor** to view the MCU event log. This procedure does not apply to a RealPresence Collaboration Server 1800.

To view an MCUs active alarms:

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.



Slot ID	Sensor N	Descriptio	Current Se	Status	Nominal V	Sensor Ty	Lower Criti	Lower Maj
2	0	Hot Swap	0		0	Hot Swap	0	0
4	0	Hot Swap	0		0	Hot Swap	0	0
5	0	Hot Swap	0		0	Hot Swap	0	0
2	1	IPMB Phys	136		0	IPMB Link	0	0
4	1	IPMB Phys	136		0	IPMB Link	0	0
5	1	IPMB Phys	136		0	IPMB Link	0	0
2	2	BMC Watc	255		0	WATCHD	0	0
5	2	BMC Watc	255		0	WATCHD	0	0
4	2	BMC Watc	255		0	WATCHD	0	0
2	3	+3.3V I/O	3.33		3.3	Voltage	2.8	2.97
4	3	+3.3V CP	3.38		3.3	Voltage	2.8	2.97
5	3	AC Power	0		0	Power Su	0	0
2	4	+2.5V	2.54		2.5	Voltage	2.12	2.25
4	4	+3.3V IP	3.34		3.3	Voltage	2.8	2.97
5	4	AC Power	0		0	Power Su	0	0
2	5	+1.8V DD	1.82		1.8	Voltage	1.53	1.62

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 alarm lists to *.xls files, click Save Hardware Alarm List and Save Software Alarm List respectively.

Note: Connection via Shelf Management

For RMX 2000/4000 systems, if you connect the Hardware Monitor via the Shelf Management server, the **Software Alarm List** section is not displayed.

Running 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.

To run diagnostics on a card:

1 In the **RMX Management** section, click Hardware Monitor .

2 In the **Hardware Monitor**, click Active Diagnostic Mode .

3 Click Yes to confirm.

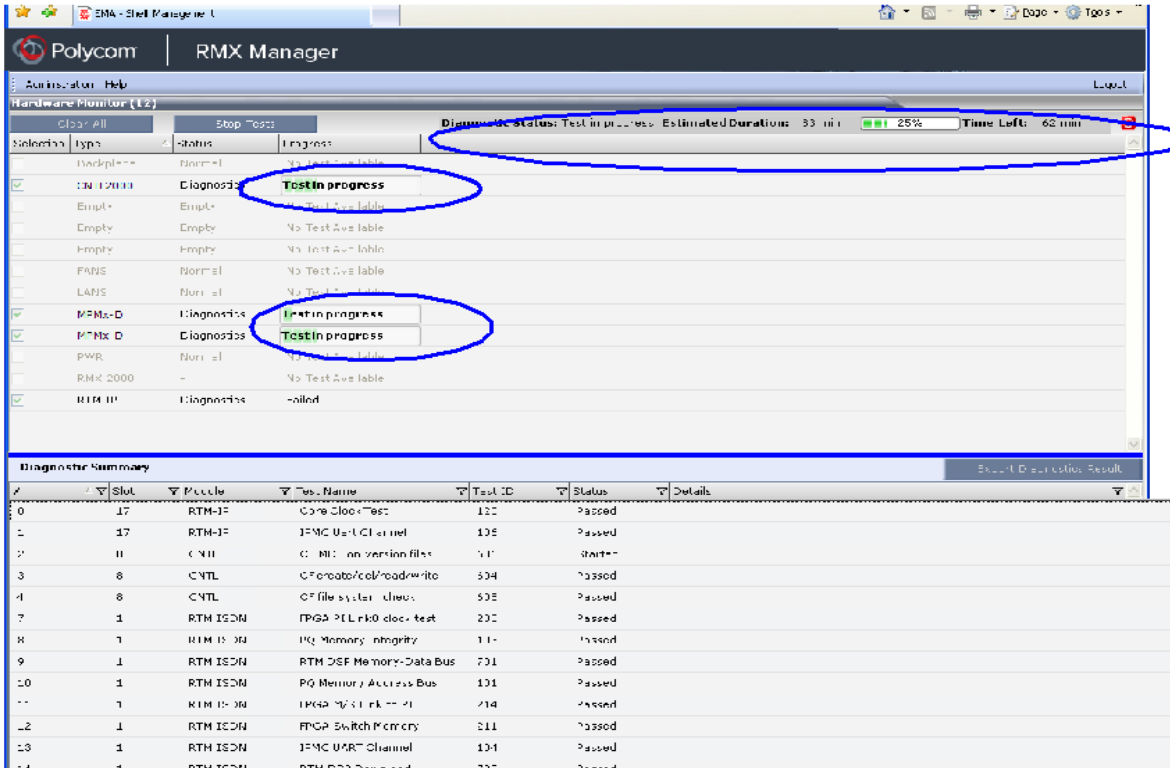
The MCU restarts.

4 For RMX 2000/4000 models, when the RMX Web Client reopens to the **Shelf Manager IP address**, log in as administrator.

5 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.

6 To run diagnostics on one or several cards, select the cards and select **Run Tests**.

7 To stop the diagnostic tests, click **Stop Tests**.



8 When the tests are completed, to download a report for analysis click Export Diagnostics Result.

9 To exit Diagnostic Mode and reset the MCU, in the **Hardware Monitor**, click .

ISDN Diagnostic on RMX 1800

RMX1800 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

Adhere to the followings guidelines when performing diagnostic on RMX 1800 MCUs:

- Before performing RTM DSP T1 FLAC3 Diag and RTM DSP E1 FLAC3 Diag, you must loopback between port1 and port2, port3 and port4.
- You can only perform one of RTM DSP T1 FLAC3 Diag and RTM DSP E1 FLAC3 Diag once RMX1800 enters diagnostic mode. If you perform diagnostic on T1, you will fail the diagnostic on E1. You must reboot the system and re-enter Diagnostic Mode, then perform the diagnostic on E1.
- Once RTM DSP T1 FLAC3 Diag or RTM DSP E1 FLAC3 Diag fails, you will fail the diagnostic on other items. You must reboot the system and re-enter Diagnostic Mode, then perform the diagnostic

If you perform diagnostics on an RMX1800 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 1 hour to complete all tests.

Restore RealPresence Collaboration Server Defaults

Administrators can erase the current Polycom® RealPresence® Collaboration Server configurations and restore default system settings. Two options are available:

- Standard restore

  Delete customer conferencing entities and keep only system default conferencing entities. However, the management network service and license info are not deleted.

- Comprehensive restore

  Restore the MCU to the settings it had when shipped from the factory. The Default Management Network and license information are deleted and the system hard disk file partition is formatted.

These restore functions are applicable only to appliance editions of the RealPresence Collaboration Servers 2000/4000/1800. You must have access to the RealPresence Collaboration Server, and you must have the USB Key included as part of the installation accessory kit to which the server's LAN configuration information was saved.

Perform a Standard Restore from USB

A standard restore deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition, a standard restore deletes all ofthe 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.

To perform a standard restore:

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 Key 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 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 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

Perform a 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: Product Activation Key is required after a Comprehensive Restore

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 key.

  Use the USB key for system restore only when you cannot do it from the system Web Client. For example, when the Web Client is inaccessible.

Warning: Insert a USB device into the Collaboration Server's USB port ONLY when you want to perform a system restore

Inserting a USB key containing the following files causes the Collaboration Server to exit Secure Mode and perform a Comprehensive Restore:

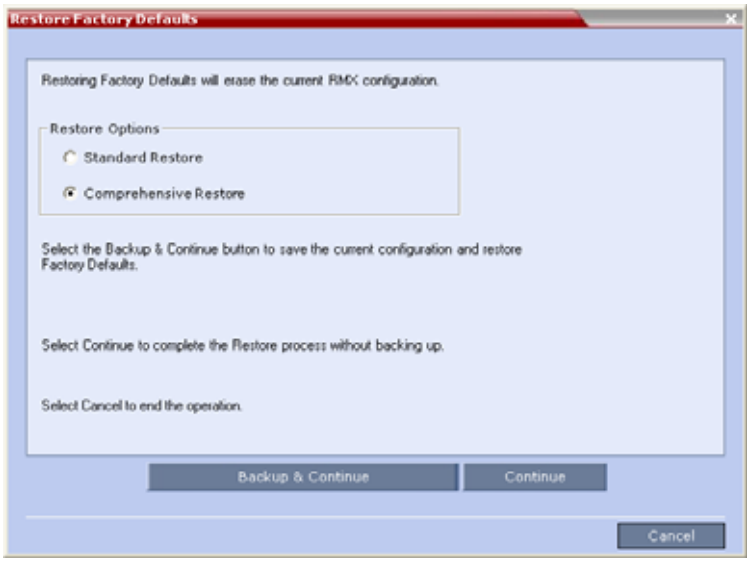
- Collaboration Server (RMX) 2000/4000 - **RestoreToFactoryDefault.txt** and **lan.cfg**
- Collaboration Server (RMX) 1800 - **USB_action.cfg** and l**an.cfg**

Do not insert a USB device into the Collaboration Server's USB port unless it is your intention to disable Secured Mode or perform a Comprehensive Restore to system defaults.

To perform a comprehensive restore using the RMX Web Client:

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 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 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 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

To perform a Comprehensive Restore using the USB key (2000/4000):

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**.

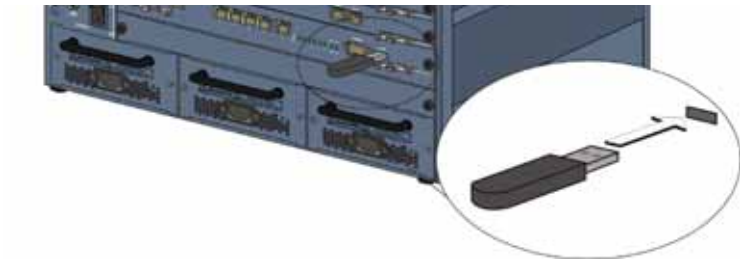
   Perform this step if you wish to restore the current conferencing entities and system configuration after the Comprehensive Restore.

2 Insert the USB key that was included with your system into the workstation.

   By default, the USB key contains files **ToFactoryDefault.txt** and a **lan.cfg** file which are used to trigger the restore. However, if they are 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 Collaboration Server.

4 Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview

To perform a comprehensive restore using the USB key (1800):

1 Insert the USB key 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 will configure 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 key.
7. Remove the USB key from the workstation.
   - Insert the USB key into either of the two USB ports on the back panel of the Collaboration Server (RMX)1800 system.

8. Power off and then power on the Collaboration Server1800 system.
9. Following system restart, follow the instructions in Modifying the Default IP Network Service and ISDN (audio/video) Network Services Overview

Perform a Restore While in Ultra Secure Mode

When the Collaboration Server is in Ultra Secure Mode, restoring Collaboration Servers 1800/2000/4000 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.

To perform a Comprehensive Restore to Factory Defaults:

1. Backup Configuration Files. These files will be used to restore the system in 13Step 13.
2. Configure a workstation for Direct Connection. For more information see Appendix - Direct Connections to the Collaboration Server.
3. Connect to the Collaboration Server and the workstation using a LAN cable.

4 Into the Collaboration Server's USB port, insert a USB key containing a file named RestoreToFactoryDefault.txt and also containing a lan.cfg file.

Note: USB key files

Do not insert a USB key containing a file named RestoreToFactoryDefault.txt if the USB key does not also contain a lan.cfg file.

5 Restart the Collaboration Server.

6 If you are not using an RMX4000 continue with Step 9.

7 Into the Collaboration Server's USB port, insert a USB key containing a file named lan.cfg file only.

8 Restart the Collaboration Server.

9 From the workstation, connect to the Collaboration Server's Alternate Management Network.

10 Apply the Product Activation Key.

11 Unplug the USB key.

12 Restart the Collaboration Server.

13 Restore the System Configuration from the backup by applying the backup files created in procedure Step 1.

14 Restart the Collaboration Server. (If the Collaboration Server is unresponsive after these procedures a further restart may be necessary.)

15 Enable Secured Communication and re-apply the Certification procedures. For more information see Certificate Management.

Appendix - Polycom Lab Features

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 Collaboration Server is in experimental mode.

Experimental features activation does not require system restart, and take effect immediately on newly created conferences.

Warning!
Do not activate any of the lab features in Collaboration Servers used at production sites. Any attempt to do so is at your own peril.

Inactivated features cannot be viewed or examined.

Lab Features Guidelines

- 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 Collaboration Server version. Therefore, the used Interface / RMX Manager should match the current Collaboration Server version, to allow enabling new Lab features.

  In that context, if the Interface / RMX Manager version is higher than that of the Collaboration Server, the newer options are displayed, though the Collaboration Server does not 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 re-activated 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 the DMA.
- In cascaded environments, the Administrator should verify the Lab Features settings across all the cascaded MCUs are the same.

Activate Experimental Lab Features

To de/activate the experimental features mode:

1. In the Collaboration Server main menu select **Setup** > **Polycom Labs**.
2. Select **Enable Polycom Lab Features** to enable experimental mode.
3. Select the check box of the feature(s) 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

Discussion Mode Layout

This brief specification documents the following Polycom Lab Feature.

Feature Name:	Discussion Mode Layout
Release Feature is Being Tested In:	Polycom® RealPresence® Collaboration Server, V8.7.1
Level of Testing Performed To Date:	☐ None ☐ Feature Unit Tested ☐ Feature Unit and Product Regression 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.

Description of Feature

The term Discussion Mode refers to the Collaboration Server ability to identify conferencing scenarios, in which either one or two participants are the main/only speaker(s). In such cases, provided this feature is activated, 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 the main cell(s), 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 (see System Flags below).

Layout Usage 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 is not 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 do not view their own video, but that of the last active speaker(s).
- 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 do not result in using layouts with larger number of cells.

System Flags

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 (i.e. not reset required). Default value: 8 **Note:** A value of 7 results in activating Discussion Mode with 7 participants, with the speaker cell included.
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 the main cell(s). This system flag required a manual addition to be modified, and immediately affects new conferences (i.e. not reset required). Default value: 20 (seconds) Minimal value: 10 (seconds)

Guidelines to Related Issues

- Recording link layout is not 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 (i.e. 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.

Interaction with 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 and Disable this Polycom Lab Feature

To enable/disable Discussion Mode:

1. Right-click on a **CP Only** or **Mixed CP and AVC** conferencing profile, and select **Profile Properties**.
   or
   Right-click on a **CP Only** or **Mixed CP and AVC** conference, and select **Conference Properties**.
2. Select the **Video Settings** tab.

Exclude Inactive-Video Participants from Layout

Polycom Lab features are new technology innovations that may not have undergone all levels of formal testing. We encourage you to try them out, but because they are not fully tested or supported, please don't deploy them in production environments.

Polycom Lab features are experimental and may or may not become official features in a future release.

This brief specification documents the following Polycom Lab Feature.

Feature Name:	Exclude Inactive-Video Participants from Layout
Release Feature is Being Tested In:	Polycom® RealPresence® Collaboration Server, V8.7.1
Level of Testing Performed To Date:	☐ None ☐ Feature Unit Tested ☐ Feature Unit and Product Regression 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.

Description of Feature

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 user experience, provided this feature is activated, the 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.

Presence of static video participants currently connected to the conference, is indicated by the  icon.

The table below lists the guideline for static video rooms' exclusion from the conference layout.

Guidelines for Removing Static Room Video from Conference Layout per Endpoint Type

AVC Endpoints	SVC Endpoints
Auto Layout is defined by the number of active video participants + maximum of 2 static video participants.	The layout used by the endpoint is determined by the endpoint.
Free cells are populated by static video participants.	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.
Once an endpoint is detected as a static video endpoint, it is removed from the layout upon the next layout change, either participant join/leave, or change in active speaker. The same applies to static video room becoming active video room.	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.
So long as the static video room is either the active or last speaker, it remains in the conference layout.	

Interactions with 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 are not 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 and Disable this Polycom Lab Feature

To enable/disable excluding inactive-video participants from layout:

1. Right-click on a **CP Only** or **Mixed CP and AVC** conferencing profile, and select **Profile Properties**.

   or

   Right-click on a **CP Only** or **Mixed CP and AVC** conference, and select **Conference Properties**.
2. Select the **Video Settings** tab.

Popup Site Name on Participant Join/Leave

Polycom Lab features are new technology innovations that may not have undergone all levels of formal testing. We encourage you to try them out, but because they are not fully tested or supported, please don't deploy them in production environments.

Polycom Lab features are experimental and may or may not become official features in a future release.

This brief specification documents the following Polycom Lab Feature.

Feature Name:	Popup Site Name on Participant Join/Leave
Release Feature is Being Tested In:	Polycom® RealPresence® Collaboration Server, V8.7.1
Level of Testing Performed To Date:	☐ None ☐ Feature Unit Tested ☐ Feature Unit and Product Regression 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.

Description of Feature

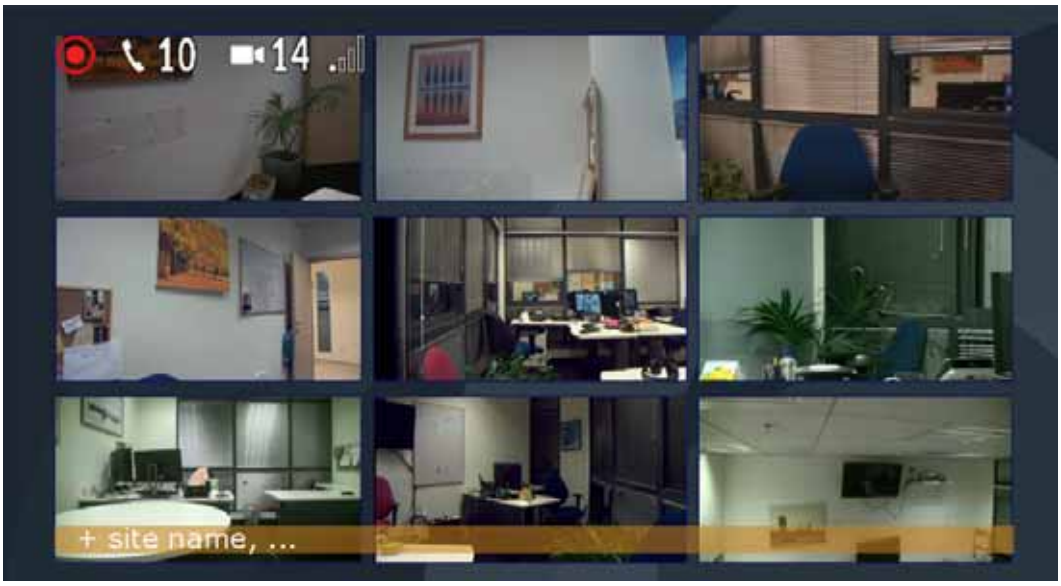
From version 8.7, Polycom® RealPresence Collaboration Server provides video AVC endpoints with indication on participant names upon their joining / leaving the conference.

Appearance Properties

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, when this feature is active, 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 demonstrated below.



General Guidelines

- 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

- Both SVC and audio participants, although incapable of viewing the site name, trigger their site name display at the AVC endpoints.
- Content participants do not trigger this feature.
- Lync clients RealConnect-ed to conferences, do not 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.
- WebRTC clients trigger this feature, however WebRTC endpoints do not display the site name message.

- Recording link participants do not 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 is not sent over the playback link video.

To Enable and Disable this Polycom Lab Feature

To enable/disable site name popup display:

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** area (shown below), determine:
   - 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 **OK** to save settings.

Prerequisites

- 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.

Using Video Clips for IVR Services

Polycom Lab features are new technology innovations that may not have undergone all levels of formal testing. We encourage you to try them out, but because they are not fully tested or supported, please don't deploy them in production environments.

Polycom Lab features are experimental and may or may not become official features in a future release.

This brief specification documents the following Polycom Lab Feature.

Feature Name:	Using Video Clips for IVR Services

Release Feature is Being Tested In:	Polycom® RealPresence® Collaboration Server, V8.7.1
Level of Testing Performed To Date:	☐ None ☐ Feature Unit Tested ☐ Feature Unit and Product Regression 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.

Description of Feature

When connecting a conference running on Polycom RealPresence Collaboration Server via an Entry Queue, a still slide is used, which up until version 8.7 could be replaced by a different still slide.

From version 8.7.1, provided **Polycom Lab** features are enabled, and the motion slides feature is activated, Polycom allows:

- Using a motion slide (video clip) instead of a still slide.
- Replacing the default motion slide Polycom supplies (within both installation and upgrade packages), which is named `General_Polycom_Slide_Motion`, with a different video slide.
- Receiving motion slides from the DMA for external IVRs.

Note: Audio Prompt for Video Slide
The audio prompt to the video slide is taken from the IVR associated with it.

Video Slides Guidelines

- Since TIP endpoints are sometimes prone to encountering problems with customizing IVR slides, it is 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 cannot 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 (i.e. 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 is truncated to 10 seconds.

    Due to clips cyclic playing, it is recommended to harmonize the clip end and beginning.
  - **Effects** - Avoid light effects to prevent imperfect translation to MCU video format.

System Flags

System Flags for Motion Slide blocking for TIP Endpoints

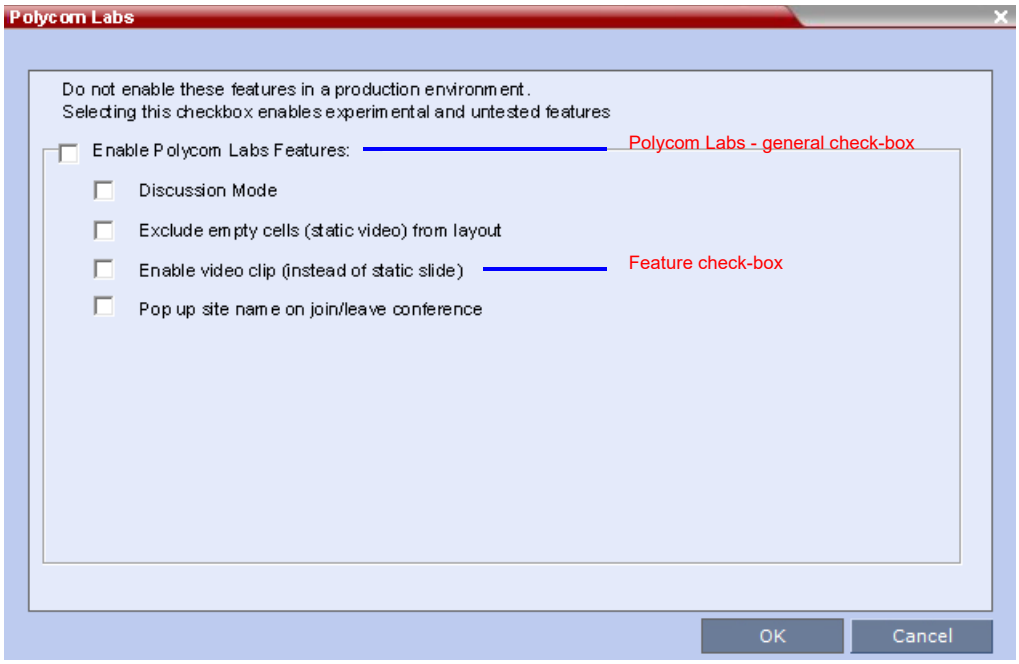
Flag Name	Flag Description
ENABLE_MOTION_SLIDE_TO_TIP_EPS	Enables displaying motion slides to TIP endpoints. This system flag required a manual addition to be modified, and if modified, value takes effect immediately (i.e. not requires reset) for new conferences. **Range:** YES (default), NO **Note:** Set this flag to NO if you experience difficulties in viewing motion slides in TIP endpoints connected to your Collaboration Server.

To Enable and Disable this Polycom Lab Feature

See the last prerequisite below.

Prerequisites

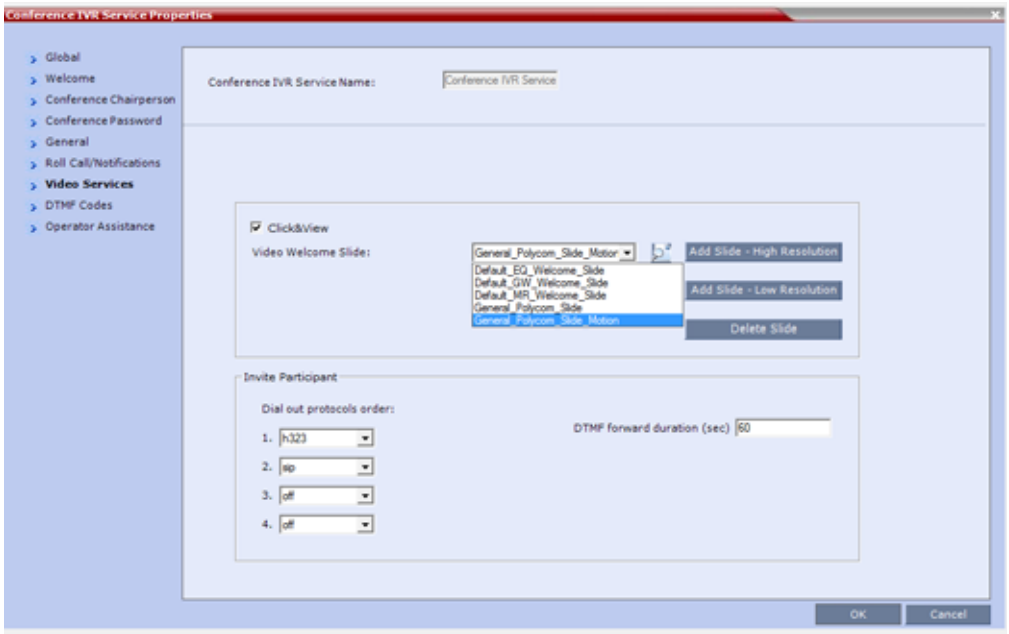
- This feature requires CIF as a minimum resolution supported by the endpoint.
- The media type supported by the endpoint may be H.263, H.264 (Base Profile only), RTV, and TIP. H.261 and H.264 High Profile endpoints are not supported.
- All user interface pertaining to this feature appear only if in the dialog below:
  - Polycom Lab features are enabled in general.
  - The feature check-box is selected.



Procedures

To select a video clip to be used for an IVR service:

1 Select **IVR Service Properties > Video Services**.



2 From the **Video Welcome Slide** list, select the video clip to be used for the IVR service.

Appendix - Secure Communication Mode

Polycom® RealPresence Collaboration Server can be configured to work in Secure Mode or Ultra Secure Mode. For more information see Ultra Secure Mode and Flags Specific to Maximum Security Environments - Ultra Secure Mode.

In Secured mode the 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 in conjunction with private keys to ensure secure communications across the network.

The Collaboration Server supports:

- TLS 1.0
- SSL 3.0 (Secure Socket Layer)

SSL 3.0 utilizes 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	Collaboration Server
	PFX / PEM	1024 or 2048	User
Management	CSR	2048	Collaboration Server
LDAP			

Certificate Configuration and Management

All Polycom devices used in a Maximum Security Environment require security certificates.

For more details see Certificate Management.

Certificate Template Requirements

The specific security certificate requirements for 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 Collaboration Server requirements.

Certificate Requirements

In Secure Mode, the certificate requirements depend on the Skip certificate validation for user logging session field.

For certificate requirements in Ultra Secure Mode, see Certificate Requirements.

Configure 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 Collaboration Server enforces these certificate revocation policies through Certificate Revocation Lists (CRLs). CRLs are required for each CA Chain in use by the Collaboration Server. These CRL files must be kept current. For more information see Certificate Configuration and Management and Public Key Infrastructure (PKI).

Switching to Secure Mode

The following operations are required to switch the Collaboration Server to Secure Mode:

- Purchase and Install the SSL/TLS certificate
- Modify the Management Network settings
- Create/Modify the relevant System Flags

Purchasing and Installing a Certificate

Once a certificate is purchased and received it is stored in the Collaboration Server and used for all subsequent secured connections. For more information see Adding Certificates to the Certificate Repository.

Note: Certificate Vulnerability due to Restoring Factory Defaults

Certificates are deleted when an administrator performs a Restore Factory Defaults with the Comprehensive Restore option selected.

For details see Appendix - Restore Defaults from USB.

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_PROTOCOL does not exist in the system, it must be created by using the **Setup** menu.

For more information see Modifying System Flags.

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 Collaboration Server to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005.

The Collaboration Server must be restarted for modified flag settings to take effect.

Enabling 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 Collaboration Server are accepted.
- The 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.

To enable secure communications mode:

1. In the **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:

Management Network Properties - Certificate Validation Mode

Field: Skip certificate validation for user logging session	
Status	**RMX and Client Certificate Requirements**
De-selected (Restricted Mode)	• The 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 RMX. Note: When the RMX Manager is the Client, all Personal Certificates in the workstation's Certification Repository are sent to the 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 (Un-restricted Mode)	• The RMX must install a personal certificate issued by a CA. • No additional configuration is required for the Client.

5 Click OK.

Alternate Management Network

Alternate Management Network enables direct access to the 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.

For more information see Connect the Alternate Management Network (2000/4000).

Note: Connection of Alternate Management Network

Connection to the Alternate Management Network bypasses LAN and Firewall security. Strict control of access to LAN 3 port is recommended.

Appendix - Ad Hoc Conferencing and External Database Authentication

Note: Feature Applicability
External Database Authentication is not supported in Collaboration Server 1800.

Polycom® RealPresence® Collaboration Servers 1800/2000/4000/Virtual Edition Ad Hoc conferencing feature enables participants to start ongoing conferences on-the-fly, without prior definition when dialing an Ad Hoc-enabled Entry Queue. The created conference parameters are taken from the Profile assigned to the Ad Hoc-enabled Entry Queue.

Ad Hoc conferencing is available in two the following modes:

- Ad Hoc Conferencing without Authentication

  Any participant can dial into an Entry Queue and initiate a new conference if the conference does not exist. This mode is usually used for the organization's internal Ad Hoc conferencing.
- Ad Hoc Conferencing with External Database Authentication

  In this mode, the participant's right to start a new conference is validated against a database.

The external database application can also be used to validate the participant's right to join an ongoing conference. Conference access authentication can be:

- Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow.
- Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Ad Hoc Conferencing without Authentication

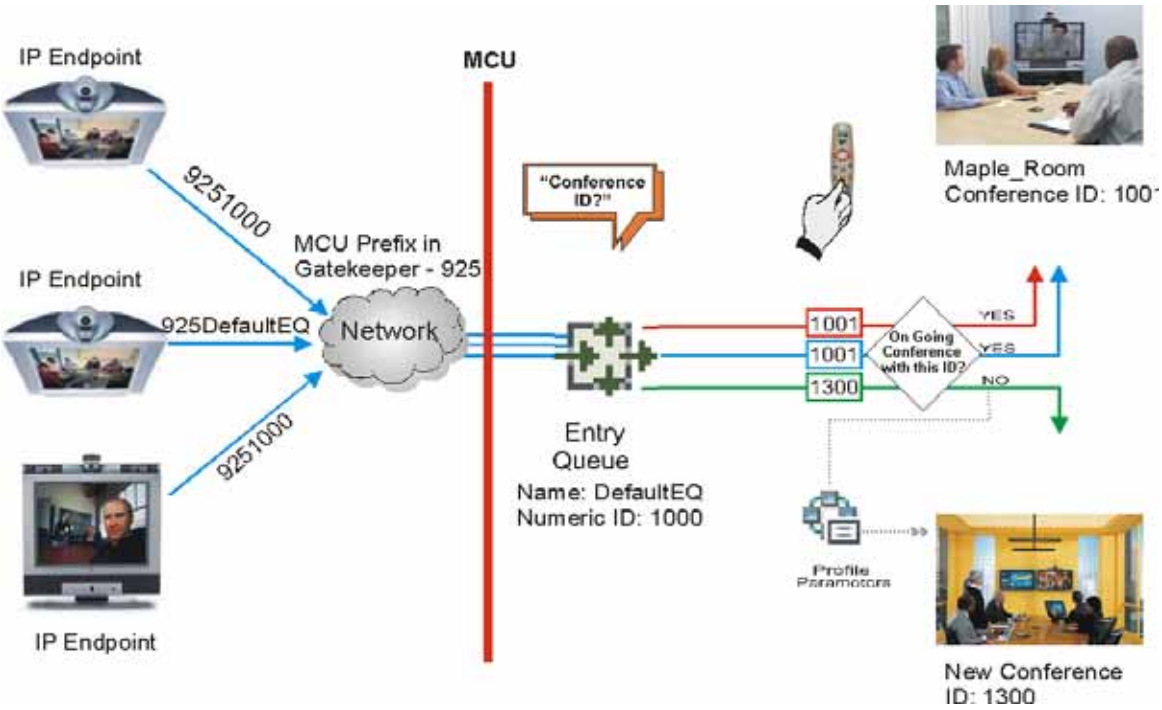
A participant dials in to an Ad Hoc-enabled Entry Queue and starts a new conference based on the Profile assigned to the Entry Queue. In this configuration, any participant connecting to the Entry Queue can start a new conference, and no security mechanism is applied. This mode is usually used in organizations where Ad Hoc conferences are started from within the network and without security breach.

To start a conference:

1. The participant dials in to the Ad Hoc-enabled Entry Queue.
2. The Conference ID is requested by the system.
3. The participant inputs a Conference ID via his/her endpoint remote control using DTMF codes.

4 The MCU checks whether a conference with the same Conference ID is running on the MCU. If there is such a conference, the participant is moved to that conference. If there is no ongoing conference with that Conference ID, the system creates a new conference, based on the Profile assigned to the Entry Queue, and connects this participant as the conference chairperson.

Ad Hoc Conference Initiation without Authentication



To enable this workflow, the following components must be defined in the system:

- An Entry Queue IVR Service with the appropriate audio file requesting the Conference ID
- An Ad Hoc-enabled Entry Queue with an assigned Profile

Ad Hoc Conferencing with Authentication

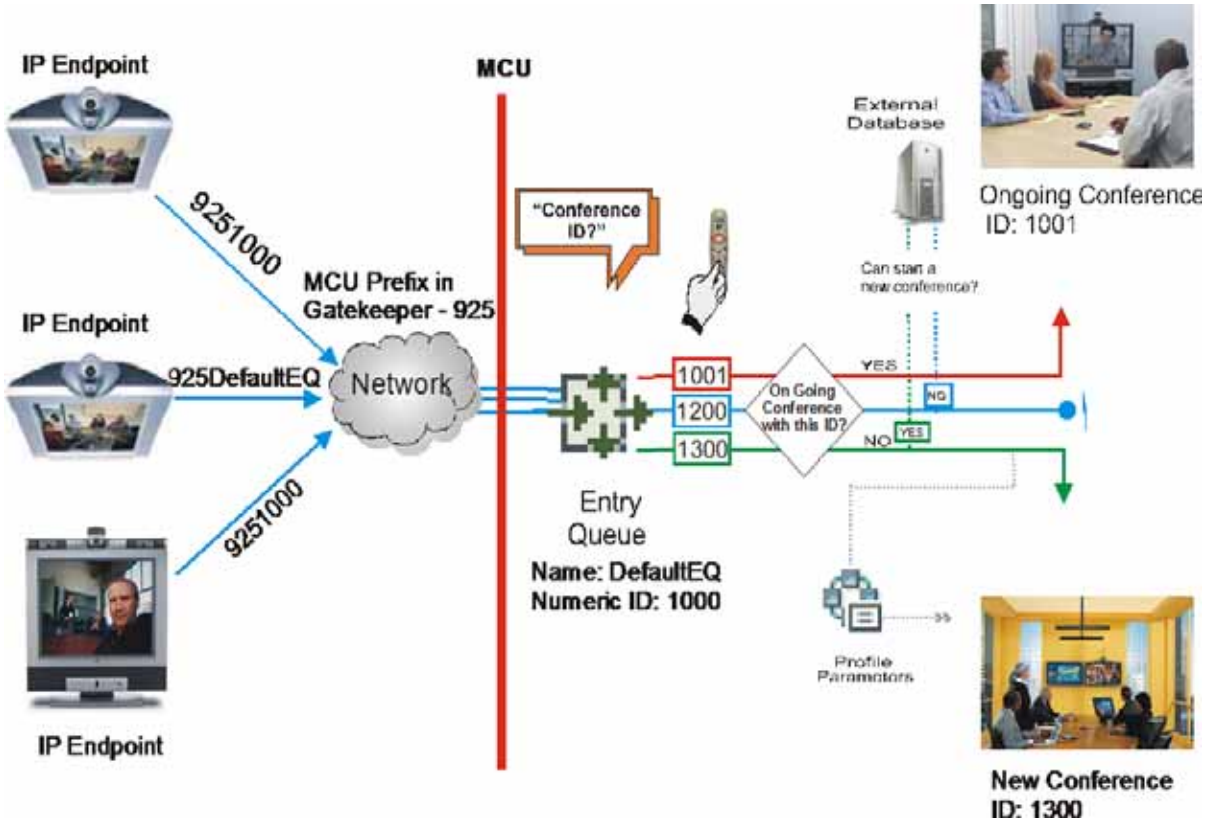
The MCU can work with an external database application to validate the participant's right to start a new conference. The external database contains a list of participants, with their assigned parameters. The conference ID entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to start a new conference.

To work with an external database application to validate the participant's right to start a new conference, the Entry Queue IVR Service must be configured to use the external database application for authentication. In the external database application, you must define all participants (users) with rights to start a new conference using Ad Hoc conferencing. For each user defined in the database, you enter the conference ID, Conference Password (optional) and Chairperson Password (when applicable), billing code, Conference general information (corresponding to the User Defined 1 field in the Profile properties) and user's PIN code. The same user definitions can be used for conference access authentication, that is, to determine who can join the conference as a participant and who as a chairperson.

Entry Queue Level - Conference Initiation Validation with an External Database Application

Starting a new conference with external database application validation entails the following steps:

Conference Initiation Validation with External Database Application



1. The participant dials in to an Ad Hoc-enabled Entry Queue.
2. The participant is requested to enter the Conference ID.
3. The participant enters the conference ID via his/her endpoint remote control using DTMF codes. If there is an ongoing conference with this Conference ID, the participant is moved to that conference where another authentication process can occur, depending on the IVR Service configuration.
4. If there is no ongoing conference with that Conference ID, the MCU verifies the Conference ID with the database application that compares it against its database. If the database application finds a match, the external database application sends a response back to the MCU, granting the participant the right to start a new ongoing conference.

   If this Conference ID is not registered in the database, the conference cannot be started and this participant is disconnected from the Entry Queue.
5. The external database contains a list of participants (users), with their assigned parameters. Once a participant is identified in the database (according to the conference ID), his/her parameters (as defined in the database) can be sent to the MCU in the same response granting the participant the right to start a new ongoing conference. 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

These parameters can also be defined in the conference Profile. In such a case, parameters sent from the database overwrite the parameters defined in the Profile. If these parameters are not sent from the external database to the MCU, they will be taken from the Profile.

6 A new conference is started based on the Profile assigned to the Entry Queue.

7 The participant is moved to the conference.

If no password request is configured in the Conference IVR Service assigned to the conference, the participant that initiated the conference is directly connected to the conference, as its chairperson.

If the Conference IVR Service assigned to the conference is configured to prompt for the conference password and chairperson password, without external database authentication, the participant has to enter these passwords in order to join the conference.

To enable this workflow, the following components must be defined in the system:

- A Conference IVR Service with the appropriate prompts. If conference access is also validated with the external database application it must be configured to access the external database for authentication.
- An Entry Queue IVR Service configured with the appropriate audio prompts requesting the Conference ID and configured to access the external database for authentication.
- Create a Profile with the appropriate conference parameters and the appropriate Conference IVR Service assigned to it.
- An Ad Hoc-enabled Entry Queue with the appropriate Entry Queue IVR Service and Conference Profile assigned to it.
- An external database application with a database containing Conference IDs associated with participants and their relevant properties.
- Define the flags required to access the external database in System Configuration.

  For more information, see MCU Configuration to Communicate with an External Database Application .

Conference Access with External Database Authentication

The MCU can work with an external database application to validate the participant's right to join an existing conference. The external database contains a list of participants, with their assigned parameters. The conference password or chairperson password entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to access the conference.

To work with an external database application to validate the participant's right to join the conference, the Conference IVR Service must be configured to use the external database application for authentication.

Conference access authentication can be performed as:

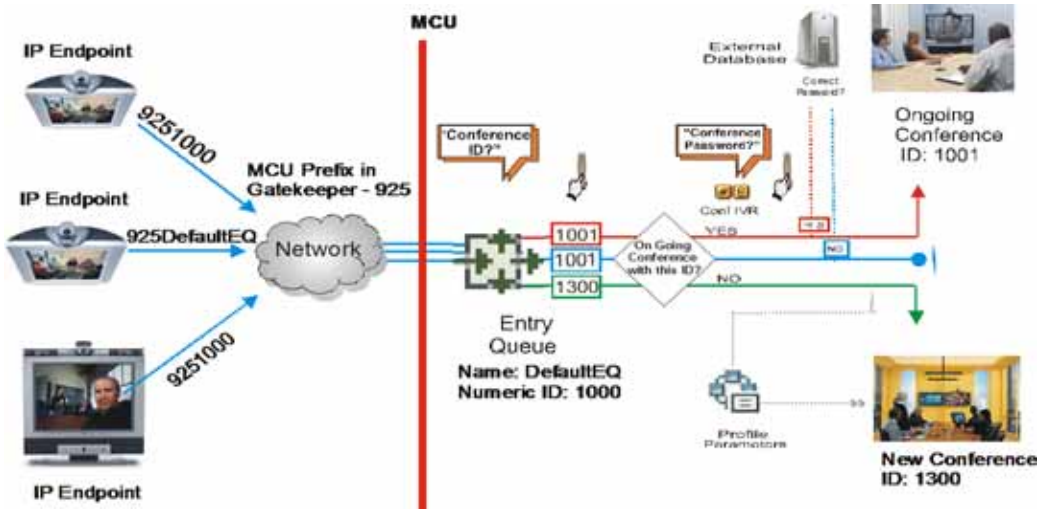
- Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow
- Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Conference access authentication can be implemented for all participants joining the conference or for chairpersons only.

Conference Access Validation - All Participants (Always)

Once the conference is created either via an Ad Hoc Entry Queue, or a standard ongoing conference, the right to join the conference is authenticated with the external database application for all participants connecting to the conference.

Conference Access - Conference Password validation with External Database Application



Joining a conference entails:

1. When the conference is started (either in the Ad Hoc flow or in the standard method), all participants connecting to the conference are moved to the Conference IVR queue where they are prompted for the conference password.
2. When the participant enters the conference or personal password, it is sent to the external database application for validation.
3. If there is a match, the participant is granted the right to join the conference. In addition, the external database application sends to the MCU the following parameters:
   - Participant name (display name)
   - Whether or not the participant is the conference chairperson
   - Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the **Participant Properties - Information** dialog box.

   If there is no match (i.e. the conference or personal password are not defined in the database), the request to access the conference is rejected and the participant is disconnected from the MCU.
4. If the Conference IVR Service is configured to prompt for the chairperson identifier and password, the participant is requested to enter the chairperson identifier.
   - If no identifier is entered, the participant connects as a standard, undefined participant.
   - If the chairperson identifier is entered, the participant is requested to enter the chairperson password.

     In this flow, the chairperson password is **not** validated with the external database application, only with the MCU.
     - If the correct chairperson password is entered, the participant is connected to the conference as its chairperson.
     - If the wrong password is entered, he/she is disconnected from the conference.

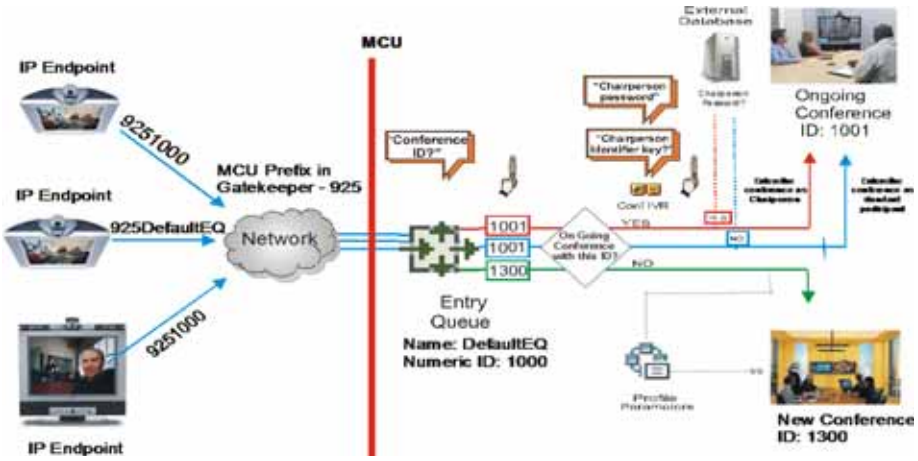
To enable conference access validation for all participants the following conferencing components are required:

- The external database must hold the conference password or the participant personal password/PIN code or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured to authenticate the participant's right to access the conference with the external database application for all requests. In addition it must be configured to prompt for the Conference Password.

Conference Access Validation - Chairperson Only (Upon Request)

An alternative validation method at the conference level is checking only the chairperson password with the external database application. All other participants can be checked only with the MCU (if the Conference IVR Service is configured to prompt for the conference password) or not checked at all (if the Conference IVR Service is configured to prompt only for the chairperson password).

Conference Access - Chairperson Password validation with external database application



Joining the conference entails the following steps:

- When the conference is started (either in the Ad Hoc flow or in the standard method), all participants connecting to the conference are moved to the conference IVR queue where they are prompted for the conference password.
- If the Conference IVR Service is configured to prompt for the Conference password, the participant is requested to enter the conference password. In this flow, the conference password is **not** validated with the external database application, only with the MCU.
  - If the wrong password is entered, he/she is disconnected from the conference.
- If the correct conference password is entered, the participant is prompted to enter the chairperson identifier key.
  - If no identifier is entered, the participant is connected to the conference as a standard participant.
- If the chairperson identifier is entered, the participant is prompted to enter the chairperson password.
- When the participant enters the chairperson password or his/her personal password, it is sent to the external database application for validation.
  - If the password is incorrect the participant is disconnected from the MCU.

- If there is a match, the participant is granted the right to join the conference as chairperson. In addition, the external database application sends to the MCU the following parameters:
  - Participant name (display name)
  - Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the **Participant Properties - Information** dialog box.

To enable conference access validation for all participants, the following conferencing components are required:

- The external database must hold the Chairperson Password or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured to check the external database for the Chairperson password only when the participant enters the chairperson identifier key (either pound or star). In addition, it must be configured to prompt for the chairperson identifier key and password.

System Settings for Ad Hoc Conferencing and External Database Authentication

Ad Hoc Settings

Before a participant can initiate an Ad Hoc conference (with or without authentication), the following components must be defined:

- Profiles

  Defines the conference parameters for the conferences that will be initiated from the Ad Hoc-enabled Entry Queue.

- Entry Queue IVR Service with Conference ID Request Enabled

  The Entry Queue Service is used to route participants to their destination conferences, or create a new conference with this ID.

  In Ad Hoc conferencing, the Conference ID is used to check whether the destination conference is already running on the MCU and if not, to start a new conference using this ID.

- Ad Hoc - enabled Entry Queue

  Ad Hoc conferencing must be enabled in the Entry Queue and a Profile must be assigned to the Entry Queue. In addition, an Entry Queue IVR Service supporting conference ID request.

Authentication Settings

- MCU Configuration

  Usage of an external database application for authentication (for starting new conferences or joining ongoing conferences) is configured for the MCU in the System Configuration.

- Entry Queue IVR Service with Conference Initiation Authentication Enabled

  Set the Entry Queue IVR Service to send authentication requests to the external database application to verify the participant's right to start a new conference according to the Conference ID entered by the participant. For details, see Enabling External Database Validation for Starting New Ongoing Conferences .

- Conference IVR Service with Conference Access Authentication Enabled

  Set the Conference IVR Service to send authentication requests to the external database application to verify the participant's right to connect to the conference as a standard participant or as a chairperson. For details, see Enabling External Database Validation for Conferences Access .
- 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 E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the **Participant Properties - Information** dialog box.

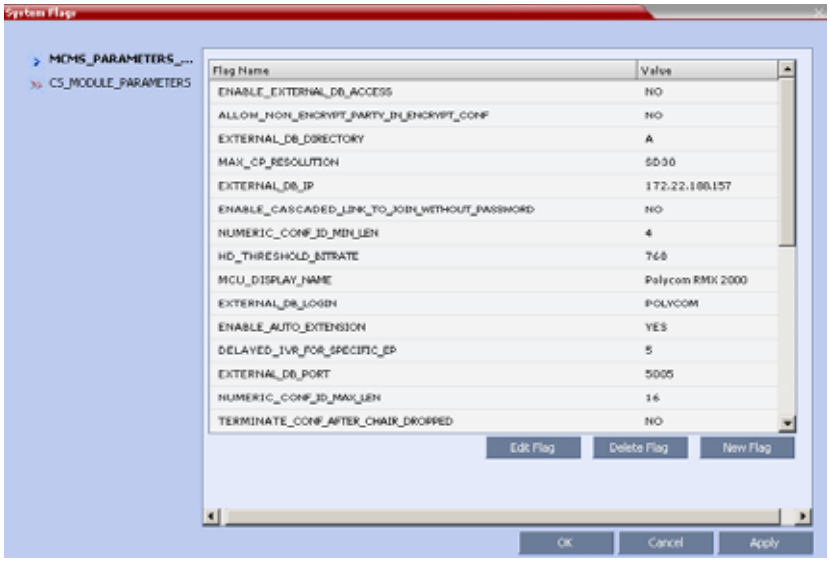
MCU Configuration to Communicate with an External Database Application

To enable the communication with the external database application, several flags must be set in the System Configuration.

To set the System Configuration flags:

1 In the Collaboration Server Main menu, select **Setup > System Configuration**.

The **System Flags** dialog opens.



2 Modify the values of the following flags:

Flag Values for Accessing External Database Application

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.

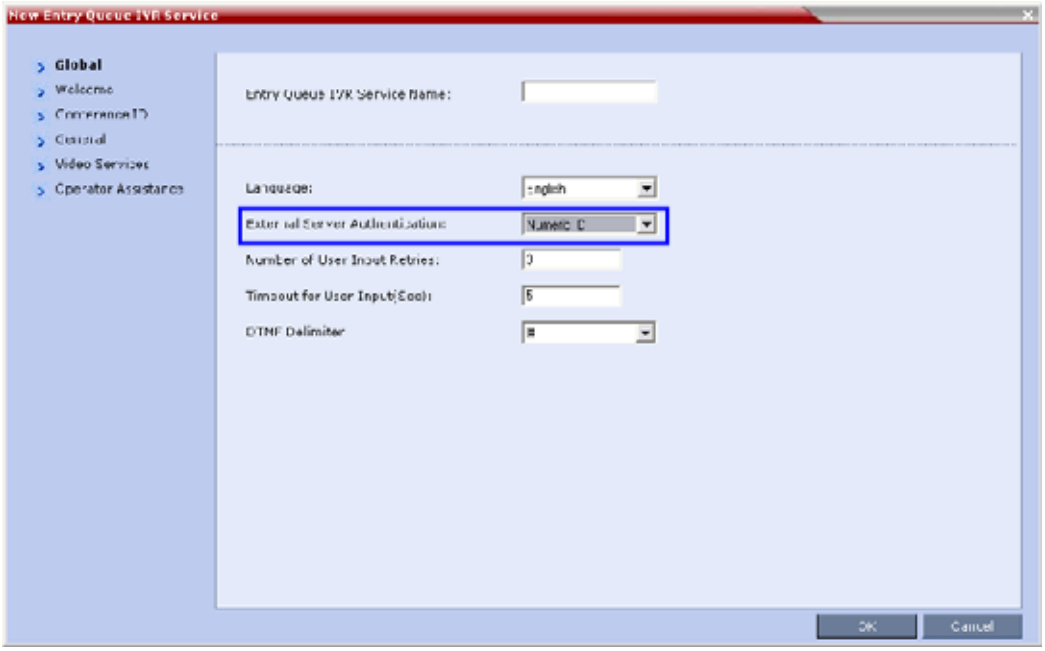
3 Click **OK**.

4 Reset the MCU for flag changes to take effect.

Enabling External Database Validation for Starting New Ongoing Conferences

The validation of the participant's right to start a new conference with an external database application is configured in the **Entry Queue IVR Service - Global** dialog.

» Set the **External Server Authentication** field to **Numeric ID**.

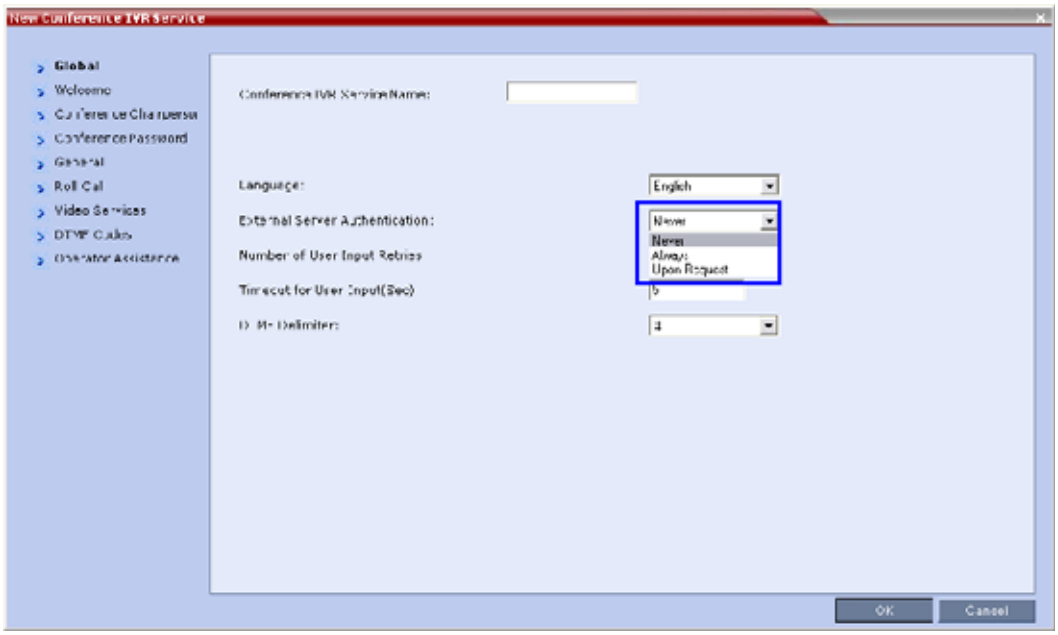


Enabling External Database Validation for Conferences Access

The validation of the participant's right to join an ongoing conference with an external database application is configured in the **Conference IVR Service - Global** dialog.

You can set the system to validate all the participants joining the conference or just the chairperson.

- Set the **External Server Authentication** field to:
  - **Always -** To validate the participant's right to join an ongoing conference for all participants
  - **Upon Request** - To validate the participant's right to join an ongoing conference as chairperson



Appendix - Media Traffic Shaping

Polycom integrated traffic shaping capabilities into the RealPresence Collaboration Server to enable deploying Collaboration Server systems 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 Collaboration Server to flatten the traffic, and minimize traffic bursts, without exceeding the bandwidth allowed within the time interval.

Though the Collaboration Server supports high level network features, high quality of service requires end-to-end video network operation. The Collaboration Server traffic shaping capabilities cannot compensate for network level violations/limitations generated by elements outside the Collaboration Server, such as endpoints, routers, etc.

Traffic shaping can flatten a momentary burst (meaning, within a 100ms time interval). However, it cannot "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 does not 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 Collaboration Server can flatten the video channel but not the incoming content channel.

Traffic Shaping Guidelines

- 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 is not 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 is not applied on audio, since the encoder output audio rate is constant.
- When LPR is enabled, traffic shaping is applied following packets repair and prior to packets sending.

System Flags

Traffic shaping usage is controlled by 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 (see 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 (see Manually Adding a System Flag).

Capacity Reduction During Traffic Shaping

The table below describes the maximum capacity left after reduction due to traffic shaping in Collaboration Servers 2000/4000. There is no capacity reduction in Collaboration Servers 1800 and Virtual Edition.

Capacity Reduction

Resolution	Non-mixed 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		

System Limitation

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.

Appendix - Modular MCU

System Description

Beginning with version 8.6, and further on version 8.7.1, a new infrastructure for Polycom® RealPresence Collaboration Server is introduced - the Modular MCU, or in short MMCU.

The new infrastructure's purpose is to separate the Collaboration Server functionalities, thus enable:

- Better utilizing of resources
- Easy expansion and deployment of new capabilities
- Easy support for previously unsupported media and endpoint types, such as RDP content (Remote Desktop Protocol), a content sharing technology used by Microsoft Lync/Skype for Business, especially in terms of customers' ability to easily adjust their systems to support them.

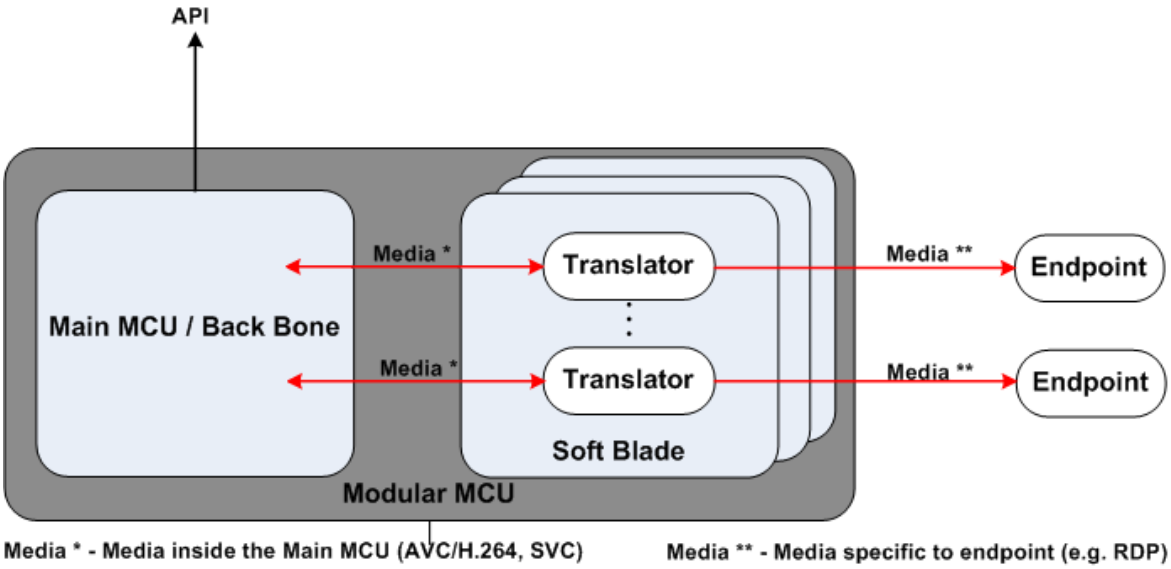
For this purpose, Polycom extended the Collaboration Server infrastructure to include:

- A Main MCU - May be either Collaboration Server Virtual Edition, or one of the Hardware MCUs, i.e. 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 Collaboration Server to endpoints, into the new media type, and vice versa.

It is important to note however, that this change in the infrastructure is not imperative should there be no need of media types other than those heretofore supplied by the Collaboration Server, and the former infrastructure can be maintained, and is actually the default state of the MCU (see MCU Operation Mode).

The Modular MCU (MMCU) infrastructure is illustrated below.



MCU Operation 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) - If there is no WebRTC IP service, MMCU is completely inactive; if there is - MCU is in Modular MCU mode, and supports internal (residing on Main MCU) Translators for WebRTC.
- **MIX** - System is in partial MMCU mode; existing WebRTC IP service enables internal WebRTC Translators, and existing Lync RDP IP service enables external (residing at Soft Blades) Translators for RDP content. If no such IP services exist, the corresponding Translator is not supported.
- 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 is not supported.

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

Deployment of Soft Blades in a Modular 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/Virtual Edition Release Notes.
- The virtual machine must use VMWare.
- All the MMCU components should be located on a single premise (co-located).

To deploy an MMCU from an existing MCU:

1. To turn your current MCU into a Main MCU, set its ENABLE_MODULAR_MCU system flag value to MIX (recommended) or YES. For more information, see MCU Operation Mode.

   Add system flag MMCU_BLOCK_TR_ABORTED MMCU and set the value to NO to enables 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.

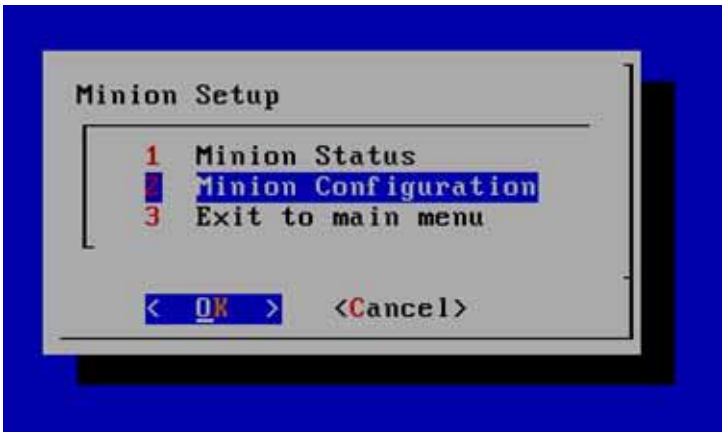
3. Deploy OVA file through vSphere client > File > Deploy OVA Template.

   Note: OVA File Directives

   - Deploy one OVA file at a time.
   - If the Main MCU is a 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.

   For more information, see Network Setup Modes - IP Network Services chapter, in RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Administrator Guide.

6 In the Minion Setup menu, select Minion Configuration, and press Enter.

7 Enter the Main MCU IP address, and press Enter.

Note: Main MCU IP Address
For all 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 (master).

   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: Removing a Soft Blade at this Phase
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. For more information, see IP Network Services - SIP Servers Dialog.

12 Add system flag MMCU_BYPASS_ENABLE_RDP and set it to YES.

13 Select Enable MS RDP content. For more information, see Polycom MCU Video Quality Dialog on DMA.

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. For more information, see Change a Cascade Link (Polycom Participants) from an Attendee to a Presenter in Skype for Business.

Monitoring Modular MCU Components

Provided the Collaboration Server is in MMCU mode (see MCU Operation Mode), the **System Monitor** replaces the Hardware Monitor in the RMX Management pane.

The Main MCU rhythmically (fixed - every 30 seconds) verifies each of the Soft Blades proper operation, and monitors its status.

Note: Monitoring Applicability
The monitoring applies to the connection between the endpoint and the Translator, and not to any internal communications.

To launch the System Monitor:

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 (Collaboration Servers 1800/2000/4000), results in displaying its Hardware Monitor.
- Double-clicking a soft Main MCU (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 Right-click on the Main MCU to display its properties.

Or

Right-click on any of the Soft Blades to select one of the currently available actions for this Soft Blade.

Note: Monitoring Dependency on MCU Infrastructure

When not in MMCU mode, the MCU operates as it used to before this infrastructure was created: Soft Blades are not visible, and Main is replaced by RMX (for HW MCUs).

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 is 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.

Also, no Translator information is displayed for WebRTC participants in 8.7.1, since in that version, these participants are handled by the main MCU, and not by Translators residing in Soft Blades.

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 cannot 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 cannot 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**
		Administrator performs **Reject**.	**Rejected**
		Administrator performs **Delete**. Note: If the console wizard is active at the Soft Blade, the Soft Blade re-appears 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**
		Administrator performs **Reject**.	**Rejected**
		Administrator performs **Delete**. ***	**Soft Blade erased ****
Rejected	Soft Blade awaits the Administrator next action.	Administrator performs **Accept**, and enters password.	**Soft Blade Pend Authentication**
		Administrator **Delete**.	**Soft Blade erased ****
Operational Phase			
Installing	The Soft Blade installation is launched	Installation is successfully completed.	**Initializing**
		Installation fails.	**Faulty**
Initializing	Initializing the Soft Blade	Initialization is successfully completed.	**Ready**
		Initialization fails.	**Faulty (ping)** **Disconnected (no ping)**

Soft Blade Monitoring States

Soft Blade State	State Meaning	Soft Blade/Administrator Operation While in State	Soft Blade New State
Ready	Soft Blade is operational.	Administrator performs **Restart** ***	**Ready (on success)** Faulty (on failure)
		Administrator performs Disable. *	**Disabled**
		No communication with Blade, ping	**Faulty**
		No communication with Blade, no ping	**Disconnected**
		Administrator performs Delete. ***	**Soft Blade erased ******
Operational Phase Error Handling			
Disabled	Ongoing conferences continue, no new ones.	Administrator performs **Enable**.	**Ready**
		Administrator performs **Delete**. ***	**Soft Blade erased ******
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 is not complete.	**Installing**
		Soft Blade is alive following restart, and installation is complete.	**Initializing**
		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)
		Administrator performs **Rescue,** triggering re-installation of internal package followed by reboot.	**Installing**
		Administrator performs **Disable.**	Disabled
		Administrator performs **Delete**.	**Soft Blade erased****
		No ping	**Disconnected**

**** Once a Soft Blade is erased, re-adding it requires re-authentication from the starting point.**
**** Warning to ongoing conferences is generated.**

Initiating a Restore to Factory Defaults operation on a Soft Blade, results in the Soft Blade requiring re-authentication 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 re-authentication 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 is however, a single irregular behavior if a Soft Blade is in Soft Blade Pend Authentication state prior to 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. An Administrator user is then required to log on using the console wizard, and configure the Main MCU (Salt master) IP address mode, either as DHCP or as static.

Note: IP Address Type
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 does not require re-acceptance 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 re-assigned to an alternate Main MCU, until deleted from its original Main MCU, it is considered as Disconnected by this MCU.

RDP Content

Skype for Business clients can share content using a Remote Desktop Protocol (RDP). Standard endpoints does not support RDP and hence it uses the H.239 (for H.323 endpoints) or BFCP (for SIP endpoints). In order 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:

- **RealConnect Mode - 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

RealConnect's capability to translate between RDP and H.264, and vice versa, is embedded in the MMCU and is referred to as 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.

For Polycom RealConnect calls to work, set 'AllowMultiView' to TRUE on the Skype for Business Front End Server. This allows participants to connect and receive multiple video streams.

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 RealConnect content calls if another soft blade is available.
- In the event of MCU fail-over, RealConnect content calls are recovered immediately after the MCU recovers the A/V RealConnect call.

Direct Call Mode

RDP content can be shared in the Direct Call mode, in which Skype for Business clients share the content directly and Polycom 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
- DMA routes Skype for Business content calls to the same MCU where the A/V call is being hosted.
- In cases of MCU fail-over, only non-encrypted Skype for Business A/V calls can be re-established. Recovery requires a re-invite, 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 are not supported on MMCUs that do not 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: Transcoded content call
The transcoded content call reaches the main MCU.

Common Behavior - RealConnect / Direct Call Modes

- In the event of MCU failure DMA will attempt to find another MMCU on which to create the content stream. For 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 is not found, the conference is created on a non-modular 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 RealConnect and Direct Call modes for both on-premise and federated environments.
- Ongoing calls may be disconnected, however the system recovers automatically from the following failures:
  - ICE Server
  - Lync Server

Enabling RDP Content

Enabling RDP content needs configurations on DMA and IP Network Service.

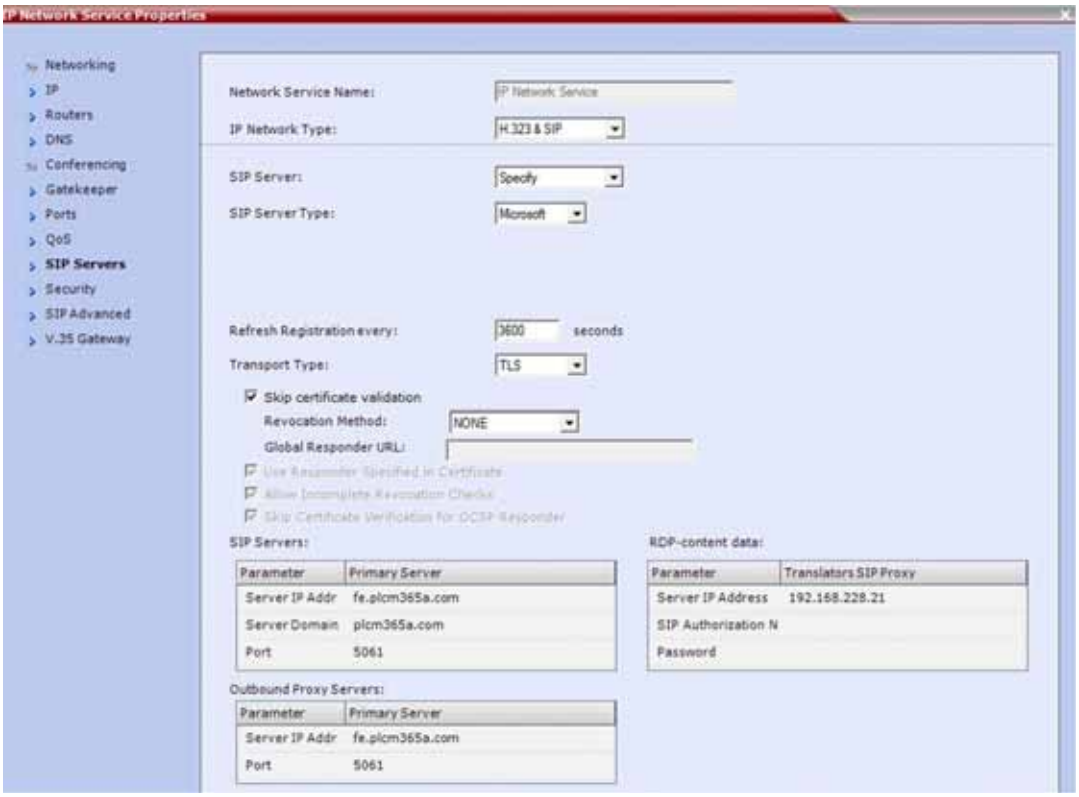
Polycom MCU Video Quality Dialog on DMA

Select Enable MS RDP content on DMA through Polycom MCU Video Quality > Content Video Definition.

Note: Enable MS RDP on DMA
Before enabling MS RDP on DMA, make sue no ContentConnect server is configured in DMA.

IP Network Services - SIP Servers Dialog

If the SIP Server Type is configured to Microsoft, an additional information box for the Translator SIP Proxy is displayed.



Number	Description	Value
1	SIP Server Type	Microsoft
2	Transport Type	TLS
3	**RDP-content data > Translator SIP Proxy**	
	Parameters	Translator SIP Proxy Values
	• Server Address	DMA Server name/address
	• SIP Authorization Name	Optional. DMA server authorization name.
	• SIP Password	Optional. DMA 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.

To change a cascade link from an Attendee to Presenter in Skype for Business:

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 RealConnect (RDPConnect) and Direct Call Mode (RDPDirect) translators can be monitored using the System Monitor.

For more information about Monitoring see Monitoring Modular MCU Components.

Modular MCU Resource Consumption and Management

Some changes in the resource consumption and resource report result from the changes introduced into the Collaboration Server infrastructure.

There is 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.

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.

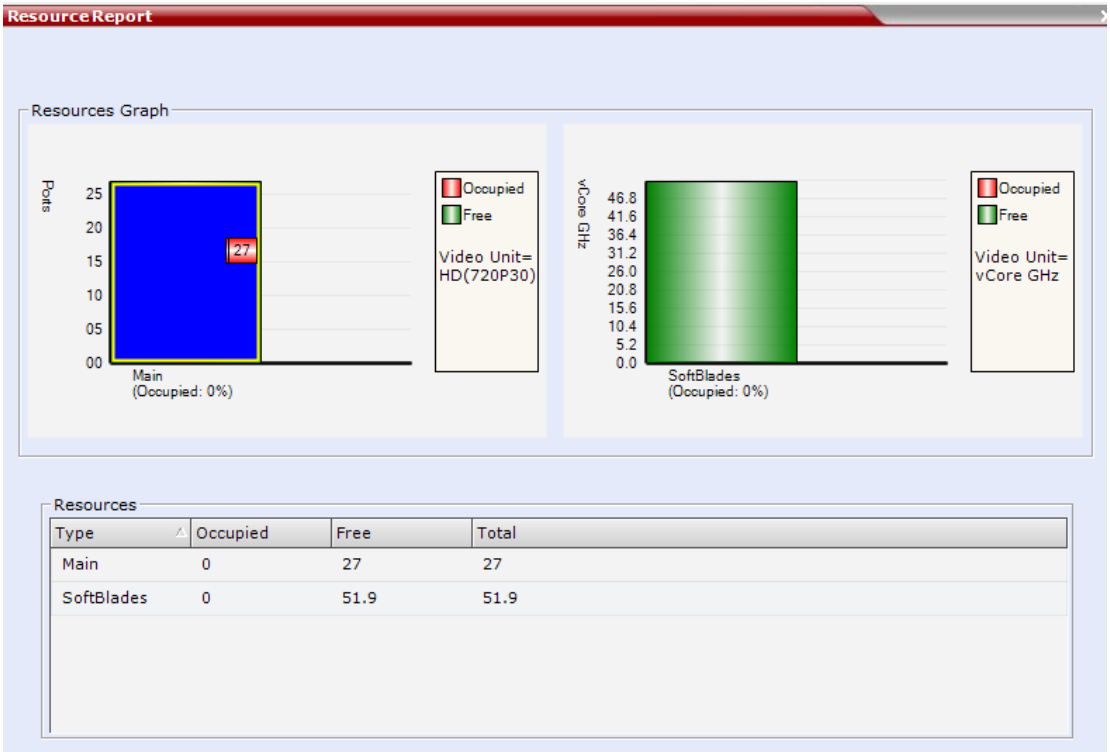
The TC allocates Translators on each Soft Blade, taking into account the resource weight of the required Translator type, until a pre-defined upper threshold is reached, at which point Translator-allocation moves to the next Soft Blade in the system. Each Soft Blade reports to the TC on its own resource availability/usage, thus the TC acts as a resource 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 are 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 RMX Menu, Administration > Resource Report.

- Real-time resource report at the Collaboration Server Status Bar:

Resource Report With no Translators Used on Soft Blade

Resource Report With Translators Used on Soft Blade

These numbers are reported for resource balancing purposes via XML API, as before.

Note: Voice Resource Report

The previous Voice resource report is removed, since it is only applicable to systems with MPMx media cards, which are not 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: Disabled Soft Blades Resources
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.

Port Usage for Skype for Business Client by Resolution

Resolution	Port Usage
720p	1
1080p	2
Note: 1 additional audio port will be consumed per participant for the connection between RealPresence Collaboration Server and Soft Blade.	

Modular MCU Security Aspects

The MMCU model ensures security is preserved on several levels:

- Salt and Soft Blade APIs - For information on ports see Collaboration Server Network Port Usage Summary.
- SIP signaling connections - Both between the Collaboration Server and the Soft Blade, and between the Soft Blade and the DMA.
- Media - Both between the 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 is 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 are 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

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>`

where:

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.

Logging Configuration

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 is designed so that, assuming a total of 15GB storage, approximately one month worth of logs can be stored.

To determine the configuration settings for the Soft Blades:

1 In the 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.

Logs at the Soft Blades

The Soft Blade log files are located under `/opt/polycom/Translator/Logs`.

Note: Salt Logs Location
Salt logs are stored in a dedicated folder under that location.

There are two types of logs at the Soft Blades:

- Call logs
- General logs

Call Logs

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.

General Logs

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 is designed so that, assuming a total of 15GB storage per Soft Blade machine, approximately one month worth of logs can be stored.

Filtering 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` 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 (i.e. Translators residing on the Main MCU, such as for WebRTC).
- Each of the filtered log files is limited to 100MB.
- Furthermore, 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).

To filter logs according to conference and/or participants:

1. In the 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

Should a failure occur at one of the Soft Blades - from best case scenario of the 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

The modular MCU and its soft blades can be upgraded together with one upgrade software (*.bin for RMX 1800/2000/4000, *.upg for Virtual Edition) that also being used for non-modular MCU upgrade, all soft blades will be upgraded automatically during the modular MCU reboot.

You can upgrade modular MCU in the same way of upgrading non-modular MCU, the only difference is that upgrading modular-MCU may take extra 1 or 2 minutes. and you can monitor the soft blades upgrade status on the **MMCU System Monitor** pane.

For both of non-modular 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.

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 will not start, and an active alarm “Insufficient storage space for upgrade” will be raised.

Monitor Soft Blades Upgrade

The modular MCU and its soft blades upgrade process can be monitored through the **RMX Management** > MMCU System Monitor.

- If soft blades upgrade normally, Upgrading displays in each soft blade 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.

- If any soft blades failed to be upgraded, Upgrade failed displays in the modular MCU row.
  - During the modular reboot process, once the modular MCU is verified as an invalid system, the modular MCU will use the previous version software instead and issue an active alarm, in this case, the soft blades will be downgraded automatically to match the main MCU version.
  - You can manually install the new version software on soft blades, which failed to be upgraded. For information of installing soft blades, see Deployment of Soft Blades in a Modular MCU.
  - Only the soft blades are upgraded successfully will work actively with the modular MCU.

Appendix - Polycom Open Collaboration Network (POCN)

Note: Feature applicability
Working with Open Collaboration Server and TIP protocol is supported in AVC Conferencing Mode only.

Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)

TIP is a proprietary protocol created by Cisco for deployment in Cisco TelePresence systems (CTS). Since TIP is not compatible with standard video communication systems, interoperability between Cisco and other vendors' Telepresence systems was initially impossible.

Gateways were developed to provide interoperability but were subject to the inherent problems of additional latency (delay) in connections and low video quality resulting from the reformatting of video and audio content.

Polycom's solution is to allow Polycom® RealPresence® Collaboration Server to natively inter-operate with Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls between:

- Polycom Immersive Telepresence Systems (ITP) Version 3.1.1:
  - RPX 200
  - RPX 400
  - OTX 300

    (A Telepresence License is required on the Collaboration Server.)
- Polycom video conferencing endpoints
  - Standalone HDX
  - Polycom Group Series 300/500
- Microsoft
  - MS Lync (using MS-ICE)
  - RTV 720p
- Cisco TelePresence® System (CTS) Versions 1.10 Collaboration Server
  - CTS 1300
  - CTS 3010

Conferences hosted on the Collaboration Server can include a mix of existing end points (that do not support TIP) and CTS endpoints.

TIP-enabled endpoints must support TIP Version 7 or higher. Calls from endpoints supporting older versions of TIP are rejected.

Note: Collaboration Server 1800 Limitation

- Although Cisco legacy endpoints are inter-operable with Collaboration Server (RMX) 1800 with no DSP cards, the MCU is not supported for integration into third-party and partner environments.
- Collaboration Server (RMX) 1800 Entry Level is not supported in POCN.

Deployment Architectures

The following multipoint topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

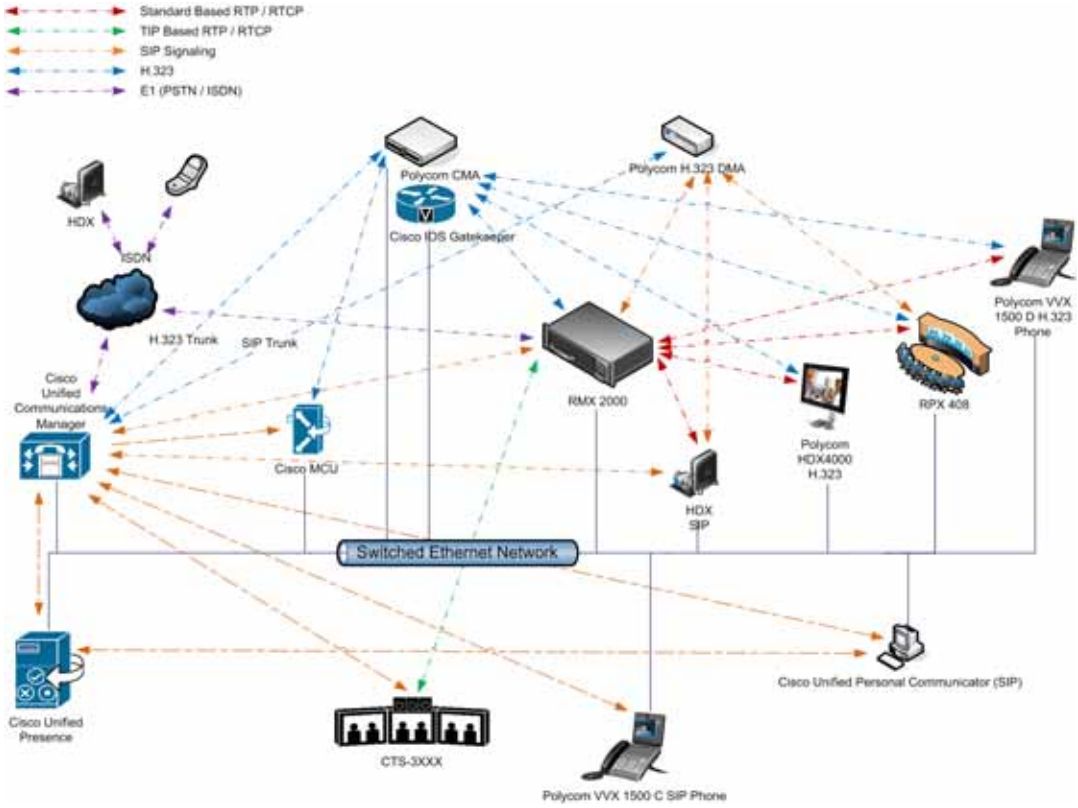
- Single company with Polycom and Cisco Infrastructure
  - CTS and Polycom Telepresence Rooms in a corporate environment.
- Company to company via Service Provider
  - Model 1: Mixed Polycom and Cisco infrastructure at one of the companies, Cisco only infrastructure at the other.
  - Model 2: Polycom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

Single Company Model - Polycom and Cisco Infrastructure

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

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

Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP



Polycom 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 Collaboration Server and Cisco Telepresence Systems (CTS) Integration Solution Architecture.

Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	8.5.1, 8.6.2	Cisco Unified Communication Manager: CUCM must be configured to: • Route calls to DMA (if present). • Route all H.323 calls to the IOS gatekeeper, which can be either DMA or IOS.
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

Solution Architecture Components

Component	Version	Description
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 Communicator	7.0,8.6	Windows PC-based softphone application.
Cisco Unified Personal 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	
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.
Polycom Equipment		
DMA 7000	4.0	Polycom Distributed Media Application • DMA is an optional component but is essential if Content sharing is to be enabled. • All SIP endpoints register to DMA as a SIP Proxy. • DMA should be configured to route SIP calls (with CTS destination) to CUCM. If DMA is not present in the solution architecture, SIP endpoints must register to CUCM as gatekeeper. • DMA must be configured with a VMR (Virtual Meeting Room). Incoming calls are then routed to the Collaboration Server.

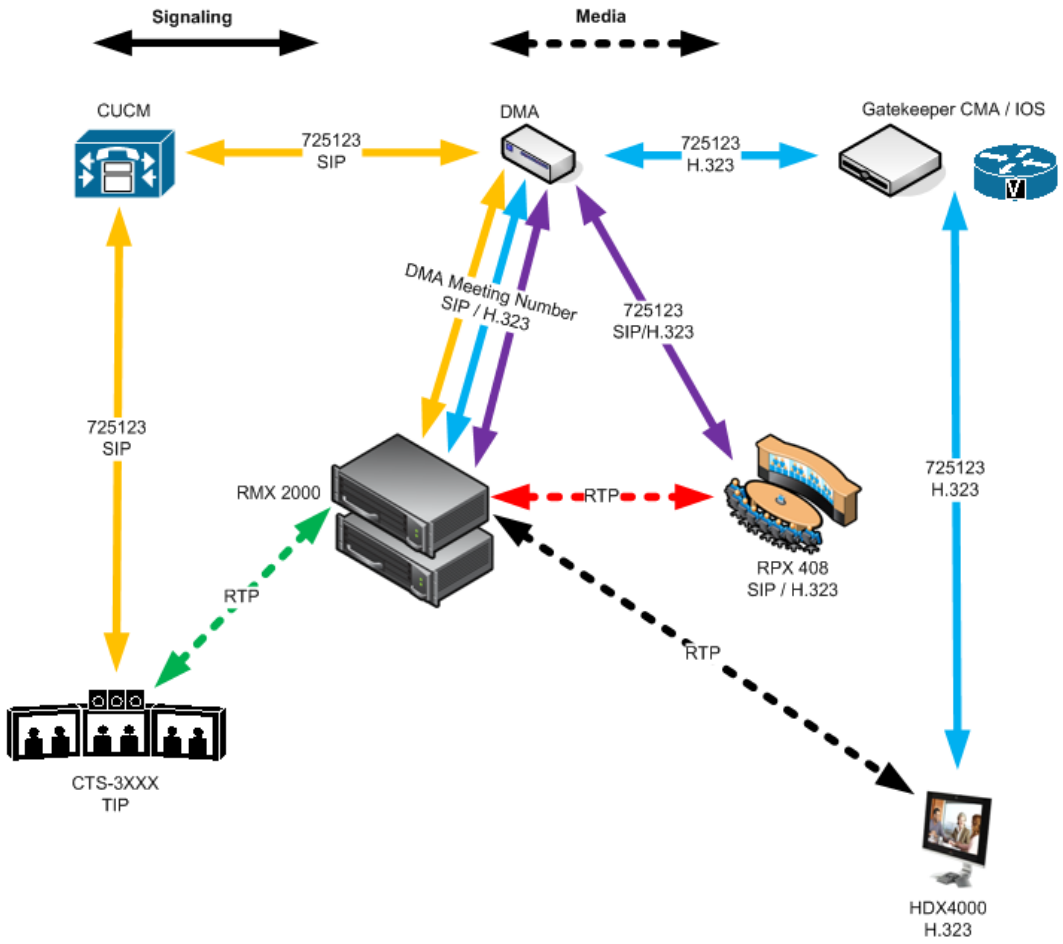
Solution Architecture Components

Component	Version	Description
Collaboration Server	7.6 and higher	MCU: • Functions as the network bridge for multipoint calls between H.323, SIP and TIP endpoints. • The Collaboration Server can be interfaced to CUCM using a SIP trunk, enabling CTS to join multipoint calls on Collaboration Server. Signaling goes through the CUCM while the media in TIP format goes directly between the CTS and Collaboration Server. • The Collaboration Server must be configured to route outbound SIP calls to the DMA. • The H.323 Network Service of the Collaboration Server should register it's dial prefix with the DMA gatekeeper. • When the DMA is not used an Ad-hoc Entry Queue, designated as Transit Entry Queue, must be pre-defined on the Collaboration Server.
MLA	3.0.3	Multipoint Layout Application Required for managing multi-screen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX or OTX systems.
Resource Manager	5.5	Polycom Converged Management Application - Gatekeeper • The gatekeeper must route calls to Collaboration Server Virtual Edition based on the Collaboration Server prefix registration on the gatekeeper.
Endpoints		Telephony, desktop and room systems. • H.323 endpoints must register to the IOS gatekeeper. • Polycom SIP endpoints must register to DMA as SIP Proxy when DMA is used. • H.323 endpoints must register to the IOS gatekeeper.

Call Flow - Multipoint Call with DMA

In this example:

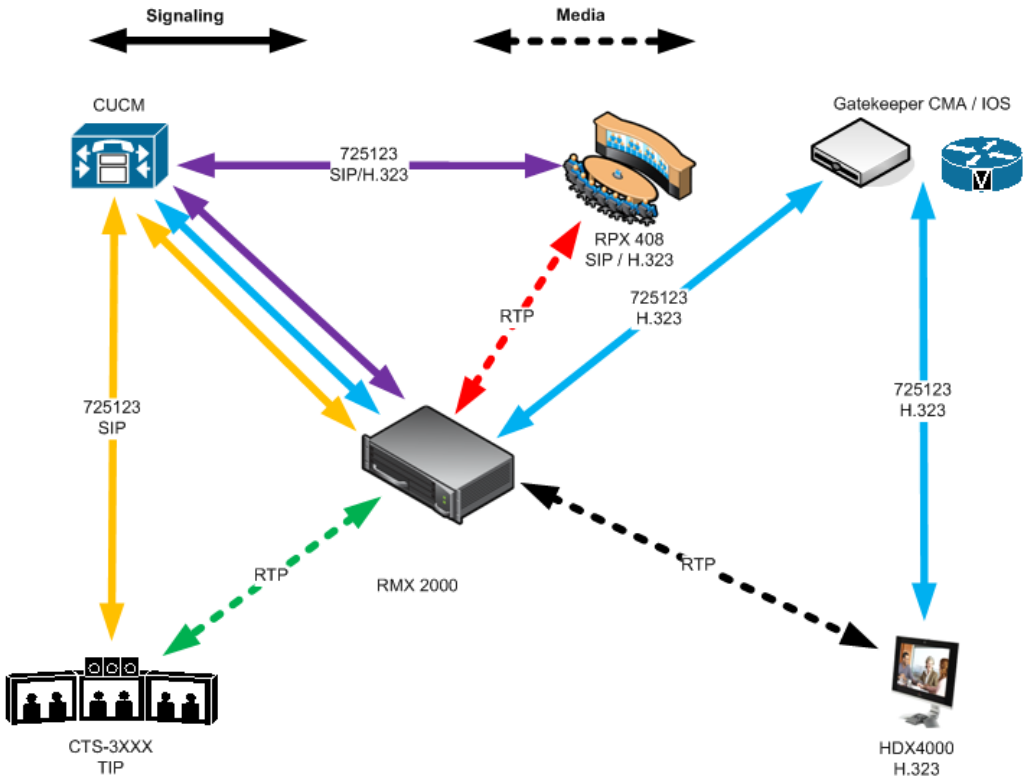
- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- DMA Meeting Number: Generated by DMA



Call Flow - Multipoint Call without DMA

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- CUCM: According to its Dial Plan forwards calls with prefix 72 to the Collaboration Server



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, enabling multipoint calls between the two companies and their respective video and audio endpoints using the 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 do not have to open their corporate firewalls and administer connectivity with the many companies they may need to communicate with.

Two topology models are discussed:

- 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 Polycom solution including:

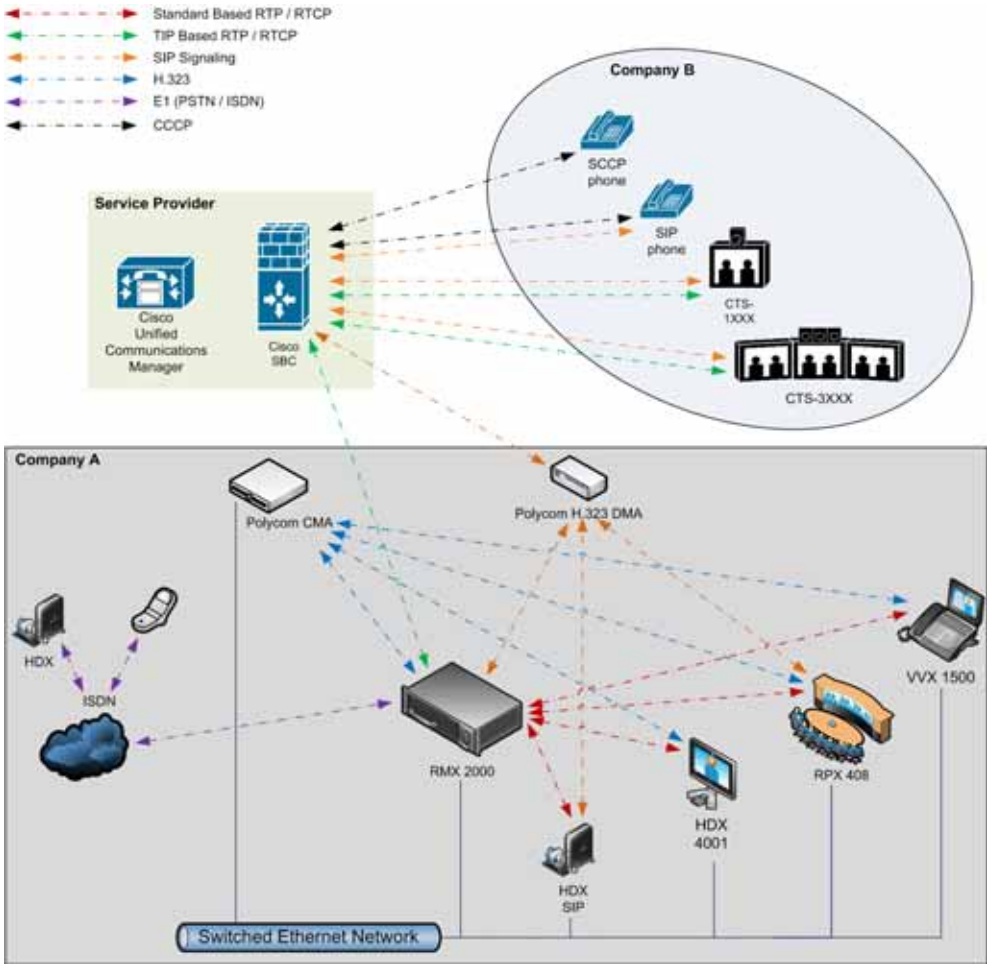
- DMA
- Collaboration Server
- MLA
- Resource Manager Gatekeeper (for Collaboration Server Virtual Edition)
- Polycom telephony and desktop endpoints.

The roles of the Polycom components are described in the Polycom Equipment section of the Solution Architecture Components table.

Company B - has deployed a Cisco solution including:

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

Company to Company via Service Provider - Model 1

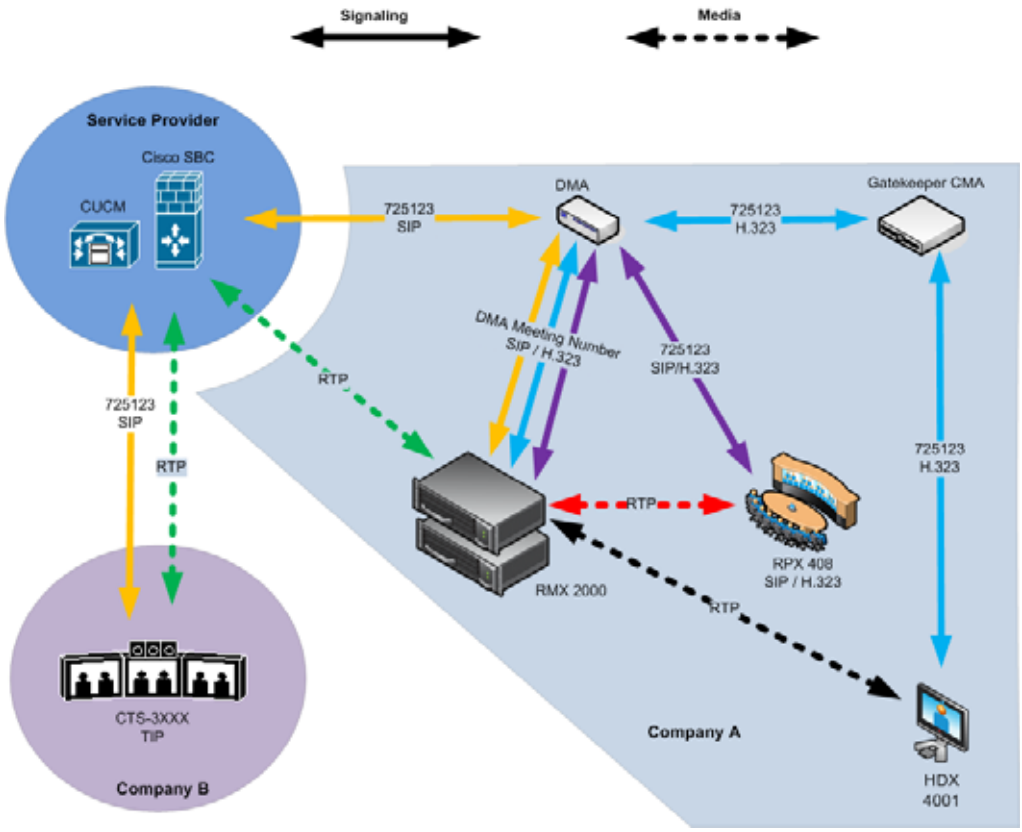


Call Flows - Multipoint Call via Service Provider

Model 1

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- DMA Meeting Number: Generated by DMA



Call Flow - Multipoint Call via Service Provider

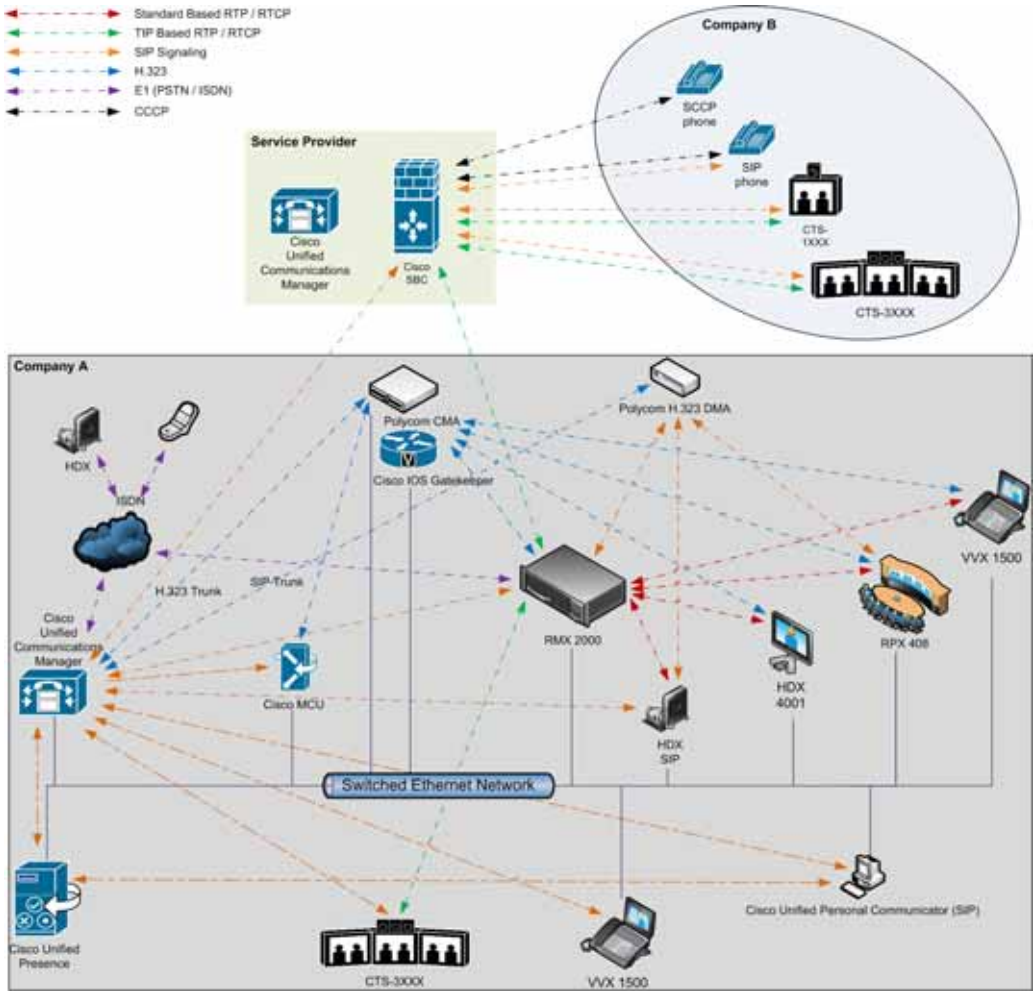
Model 2

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.



Deployment Architecture Composition

Company A

For a full description of Company A's deployment, see Single Company Model - Polycom and Cisco Infrastructure.

Differing or additional configuration requirements for each element of this deployment model are listed below:

Company A Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	8.5	Cisco Unified Communication Manager: CUCM must be configured with a SIP trunk to the Service Provider's SBC.
Polycom Equipment		
Collaboration Server	7.6.x and up	MCU: Collaboration Server must be configured to send and receive RTP streams to and from the Service Provider's SBC.

Company B

Company B Solution Architecture Components

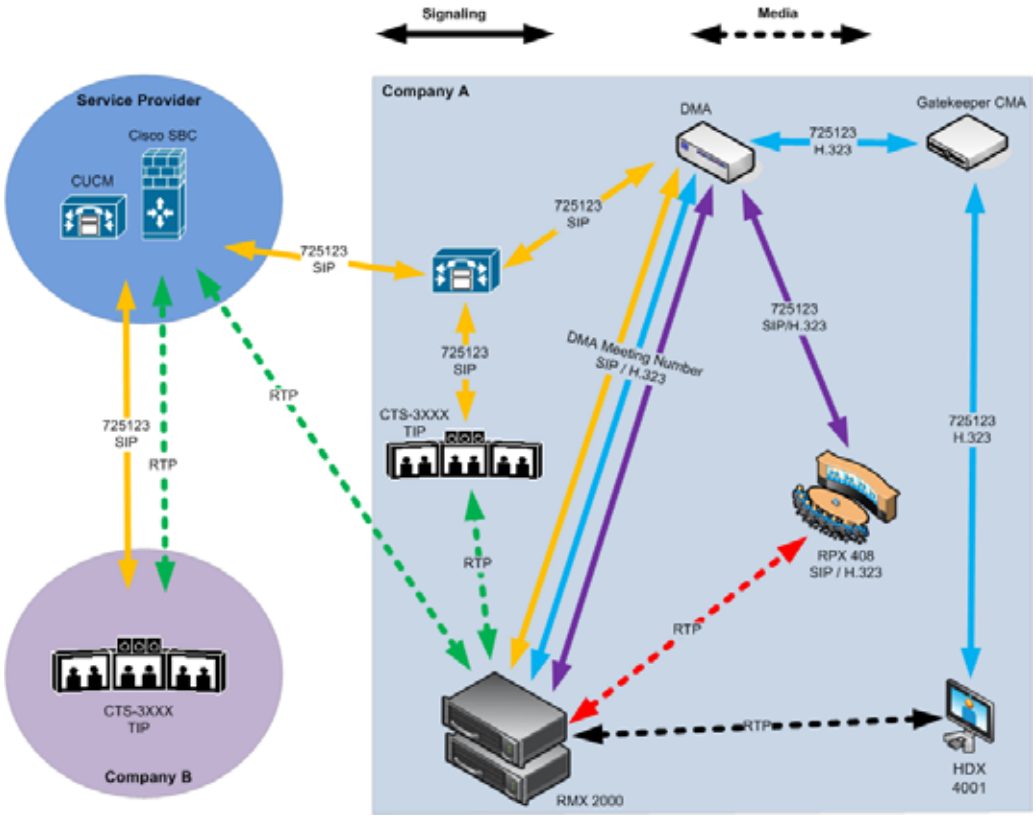
Component	Version	Description
CISCO Equipment		
Endpoints		Endpoints should register with the Service Provider's CUCM (or the local CUCM, if present).

Call Flow - Multipoint Call via Service Provider

Model 2

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- CUCM: According to its Dial Plan forwards calls with prefix 72 to the Collaboration Server



Administration

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

Note: DMA and Resource Manager Interchangeability According to Platform
The DMA acts for Collaboration Servers 2000/4000/1800 as the Resource Manager for Collaboration Server Virtual Edition.

Gatekeepers

Standalone Polycom Resource Manager/DMA System as a Gatekeeper

The Polycom Resource Manager/DMA system can be used as the only gatekeeper for the network. Bandwidth and call admission control of endpoints registered with the DMA/Resource Manager system is split between the DMA/Resource Manager system and the CUCM.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Polycom Resource Manager System as a Gatekeeper.

Standalone Cisco IOS Gatekeeper

The Cisco IOS Gatekeeper can be used as the only gatekeeper for the network if the management capabilities of the Polycom DMA/Resource Manager system are not required.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Standalone Cisco IOS Gatekeeper.

Neighbored Cisco IOS and Polycom Resource Manager/DMA Gatekeepers

Neighbored gatekeepers make it easier to create a common dial plan and should be considered when integrating an existing Cisco telephony environment with an existing Polycom network. Neighbored Gatekeepers allow number translation while maintaining the existing environments.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Neighbored Cisco IOS and Polycom Resource Manager Gatekeepers.

DMA

The Polycom DMA system can be configured as a SIP proxy and registrar for the environment. When used as a SIP peer, the DMA system can host video calls between Cisco endpoints that are registered with the CUCM and Polycom SIP endpoints that are registered with the DMA system.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Polycom DMA System as SIP Peer.

CUCM

When Polycom SIP endpoints (voice and video) are registered 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 will be used in such cases.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants.

Configuring the Cisco and Polycom Equipment

MLA (Multipoint Layout Application) 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 DMA/Resource Manager Gatekeeper and the CUCM for reporting and billing purposes.

Cisco Equipment

To configure the various Cisco entities the following procedures are required.

CUCM

1 Configure the CUCM to send and receive calls from the H.323 network.

   a With Neighbored IOS and DMA/Resource Manager Gatekeepers

      For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Configuring Cisco Unified Communications Manager for H.323.

   b With Resource Manager Gatekeeper

      For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Configuring Cisco Unified Communications Manager for H.323.

   c With IOS Gatekeeper

      For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Configuring Cisco Unified Communications Manager for H.323.

IOS Gatekeeper

- Set up zones and gateway type prefixes to enable dialing to DMA and Collaboration Server systems.

  For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Configuring the Cisco IOS Gatekeeper.

IOS and DMA/Resource Manager Gatekeepers (Neighbored)

- Configure the Cisco IOS Gate*keeper for two separate zones.*

  For more information see the Polycom Unified Communications Deployment Guide for Cisco Environments, Configure the Cisco IOS Gatekeeper for use with a Resource Manager System.

Polycom Equipment

The following table lists the Polycom products supported within the various Deployment Architecture.

Only Collaboration Server configurations are described in detail in this document.

Configuration procedures for all other solution components are described in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Supported Polycom products

Polycom TIP and SIP	Version(s)
Polycom DMA 7000 system	V4.0
Polycom RealPresence Collaboration Server	V7.6 and higher
Immersive Telepresence Systems: • RPX 200 and 400 systems • OTX 300 system • TPX HD 306 system • ATX HD 300 system	V3.0.3 Requires TIP option key. Requires Polycom Touch Control.

Supported Polycom products

HDX Systems: • 7000 HD Rev C • 8000 HD Rev B • 9006 • 4500	V3.0.3 Requires TIP option key.
Peripheral Polycom Touch Control	1.3.0
SIP ONLY (no TIP support)	**Version(s)**
Spectralink wireless phones 8020/8030	
Polycom VVX 1500	V4.0
Polycom VVX 1500 C	V3.3.1
KIRK Wireless Server 300/600v3/6000	

The following procedures are a summary of the configuration procedures.

The detailed procedures begin with Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag.

Configuring the Collaboration Server

1. Set the **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag
2. Configuring the Collaboration Server to statically route outbound SIP calls to DMA or CUCM
3. Configuring the Collaboration Server's H.323 Network Service to register with DMA/Resource Manager gatekeeper
4. Configuring a TIP enabled Profile on the Collaboration Server
5. Configuring an Ad Hoc Entry Queue on the Collaboration Server if DMA is not used
6. Configuring a Meeting Room on the Collaboration Server
7. Configuring Participant Properties for dial out calls

Configuring DMA

If DMA is present in the configuration perform procedures Configuring DMA to route SIP calls to CUCM and Configuring a Virtual Meeting Room (VMR), otherwise skip to procedure Configuring Resource Manager to route H.323 calls to Collaboration Server.

1. Configuring DMA to route SIP calls to CUCM
2. Configuring a Virtual Meeting Room (VMR)

   The procedures for configuring DMA are described in detail in *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring the Resource Manager

1. Configuring Resource Manager to route H.323 calls to Collaboration Server

2 Configuring Resource Manager for use with Cisco IOS Gatekeeper (Neighbored)

3 Configuring Resource Manager to route H.323 calls to CUCM

4 Configuring Resource Manager to route non-H.323 calls to CUCM

The procedures for configuring Resource Manager are described in detail in *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring Endpoints

5 Configuring H.323 endpoints to register to the Resource Manager or IOS gatekeeper

The procedures for configuring H.323 endpoints are described in detail in *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring SIP endpoints to register to:

a DMA as SIP Proxy

b CUCM as SIP Proxy

The procedures for configuring SIP endpoints are described in detail in *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring TIP endpoints to register to:

c DMA

d CUCM

The procedures for configuring TIP- enabled endpoints are described in detail in *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring Entry Queues and IVR Services

Conference IVR and Entry Queue/Virtual Entry Queues are supported with AVC TIP protocol in conferences that include both TIP-enabled and non-TIP-enabled endpoints.

A Virtual Entry Queue can be configured to either IVR Only Service Provider or External IVR Control mode.

TIP-enabled endpoints can be moved from the Entry Queue to the destination conference if the TIP Compatibility Modes settings in the Profile are identical for both conferencing entities (it is recommended to use the same Profile for both entities).

TIP IVR users can access the conference directly or enter the Entry Queue/Virtual Entry Queue and provide a password to access the conference.

The IVR services can be enabled with **Prefer TIP** TIP **compatibility mode**.

IVR media files, WAV for voice messages and JPG for video slides, are all stored on the Collaboration Server.

Guidelines

- IVR default audio files are enabled for all TIP Compatibility Modes.
- In order for the MCU to detect DTMF digits from TIP-enabled endpoints, the system flag SIP_REDUCE_AUDIO_CODECS_DECLARATION must be set to YES.
- If the flag is set to NO, the MCU cannot detect DTMF digits from TIP endpoints.
- In an mixed TIP environment there is 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.

For more information on Multipoint see Call Flow - Multipoint Call with DMA, Call Flow - Multipoint Call without DMA, and Call Flow - Multipoint Call via 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.

Content

Polycom and Cisco endpoints can share Content within a Cisco TelePresence environment. The content sharing experience depends on whether the endpoints are registered with the DMA or CUCM.

Endpoint Registration Options - Content Sharing Experience

Multipoint Calls on Collaboration Server	Content Sharing	People + Content
Endpoints Registered to DMA		
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
  - A variety of resolutions and frame rates are supported.

    For more information see Content Sharing Using H.239 Protocol and Content Sharing Using People+Content Protocol.
  - 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 cannot 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.

    For more information see Procedure 4: Configure a TIP Enabled Profile on the Collaboration Server.

Procedure 1: 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.

In Collaboration Servers 2000/4000/1800, CTS version 1.9.1 is required, and if CUCM is present in the environment, a minimum line rate of 1280 kbps must be set in the conference profile. Calls at lower line rates are rejected, therefore the System Flag value must be set to 1280 or higher.

In Collaboration Server Virtual Edition, CTS version 7 is required, and if CUCM is present in the environment, a minimum line rate of 1024 kbps must be set in the conference profile. Calls at lower line rates are rejected, therefore the System Flag value must be set 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.

For more information see Modifying System Flags.

Procedure 2: Configure Collaboration Server to Statically Route Outbound SIP Calls to DMA or CUCM

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 DMA or CUCM in both the **Server IP Address or Name** and **Server Domain Name** fields.

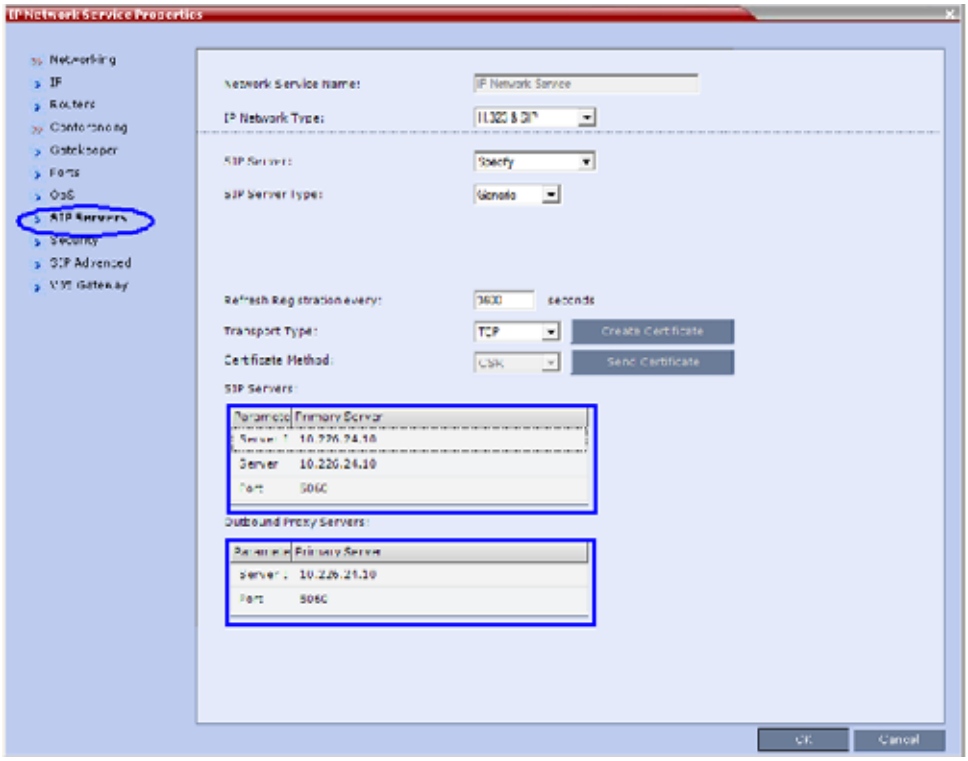
b The **Port** field must be set to it's default value: **5060**. DMA and CUCM use this port number by default.

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 The **Port** field must be set to it's default value: **5060**.

(By default, the Outbound Proxy Server is the same as the SIP Server.)

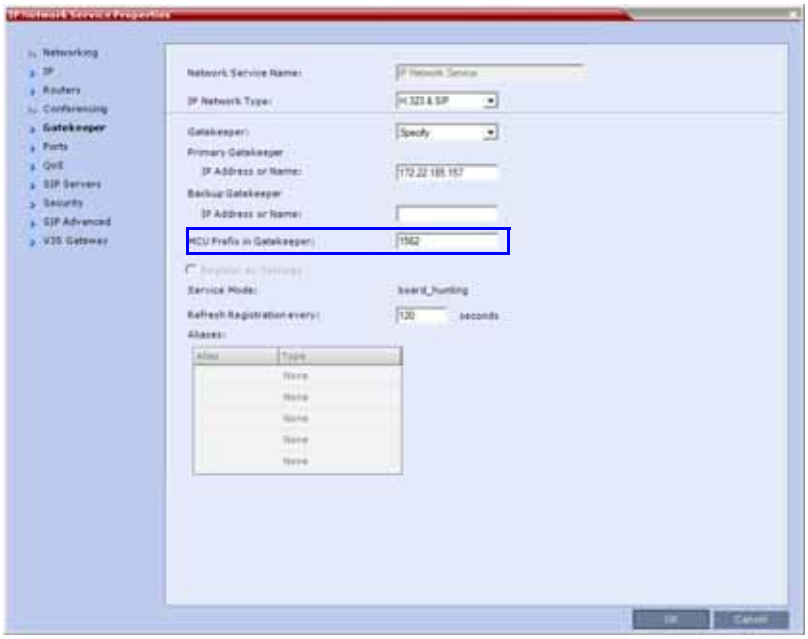


When configuring the Collaboration Server to statically route SIP calls to DMA or CUCM, it is important to also configure the Collaboration Server's H.323 Network Service to register with DMA (in Collaboration Servers 2000/4000/18000) or Resource Manager (in Collaboration Server Virtual Edition) gatekeeper. For more information see Procedure 3: Configure Collaboration Server H.323 Network Service to register with DMA/Resource Manager gatekeeper.

Procedure 3: Configure Collaboration Server H.323 Network Service to register with DMA/Resource Manager gatekeeper

1 In the **IP Network Services Properties** dialog, open the **Gatekeeper** tab.

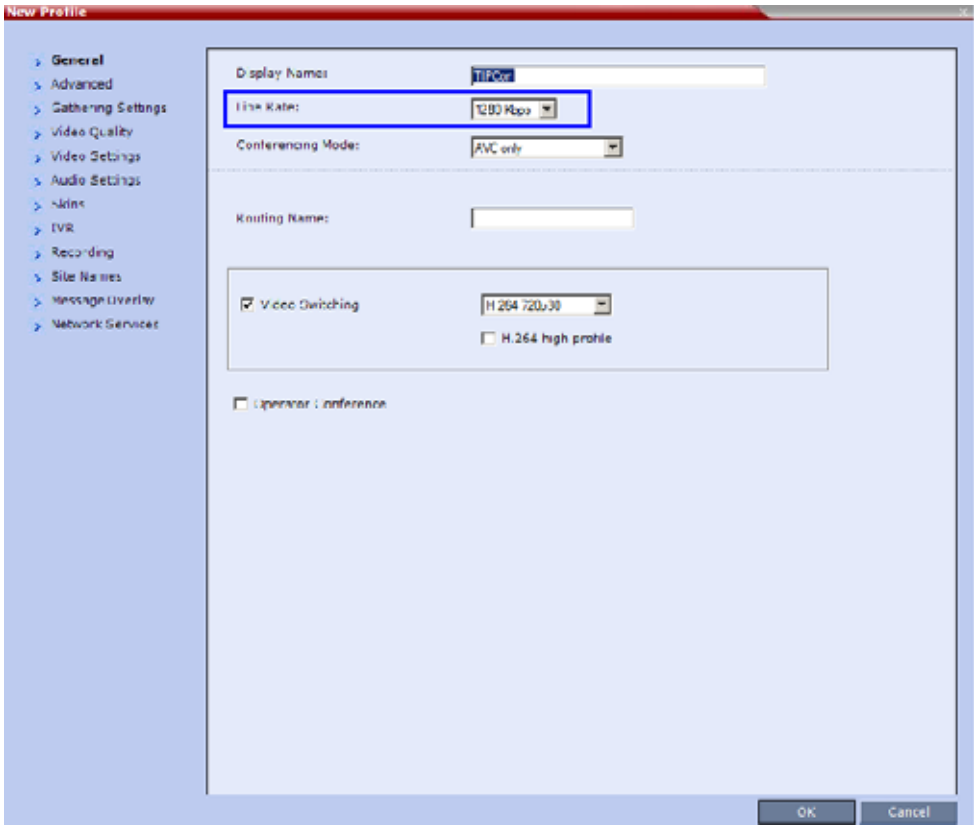
2 In the **MCU Prefix in Gatekeeper** field, enter the prefix the Collaboration Server uses to register with the gatekeeper.



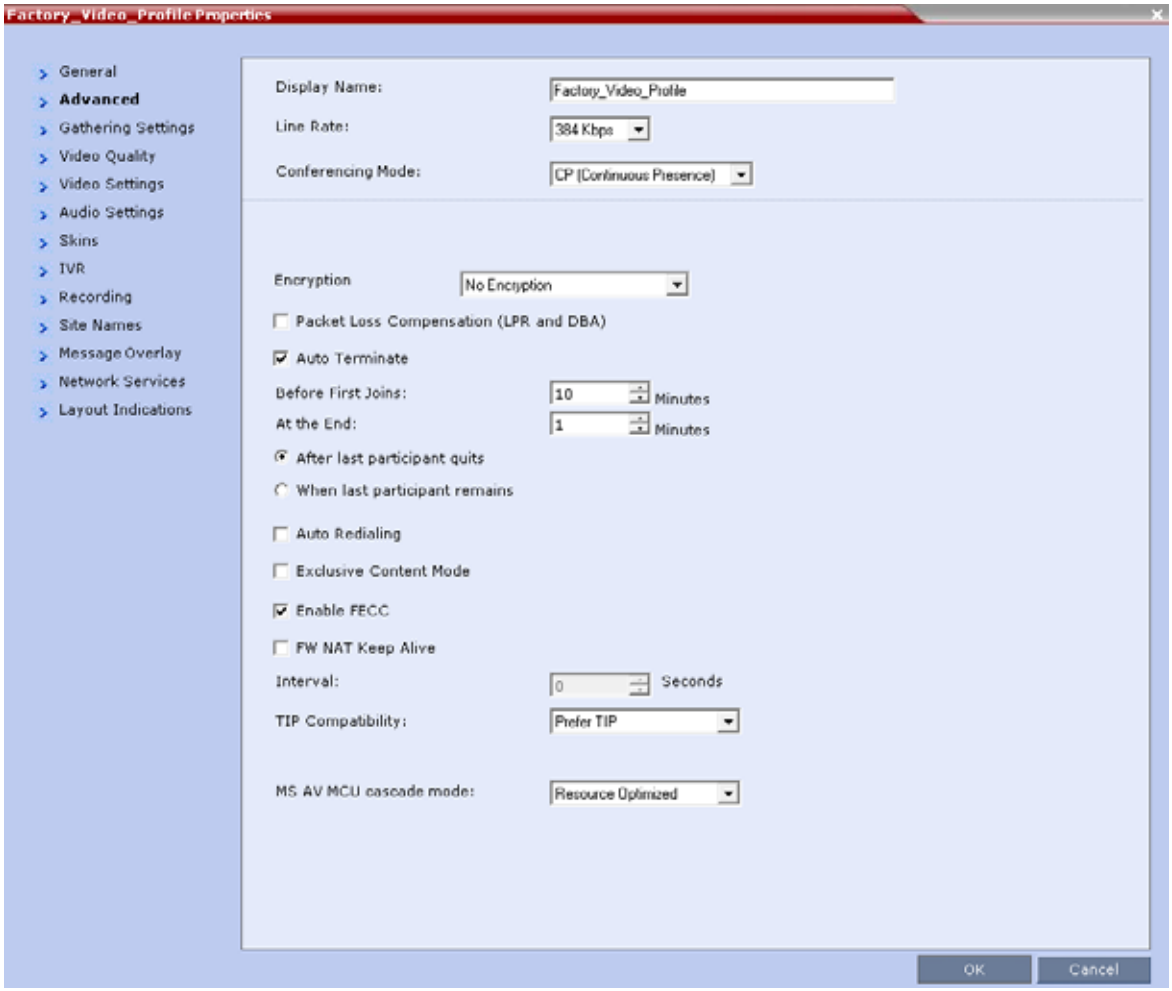
Procedure 4: Configure a TIP Enabled Profile on the Collaboration Server

TIP enabled profiles must be used for the Entry Queues and Meeting Rooms defined on the Collaboration Server. (Different Profiles can be assigned to Entry Queues and Meeting Rooms, however they must be TIP enabled.) When TIP is enabled in the Profile, Gathering Settings and Message Overlay options are disabled.

1. Create a New Profile for the Meeting Room. For more information see Defining AVC CP Conferencing Profiles.
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 in Procedure 1.

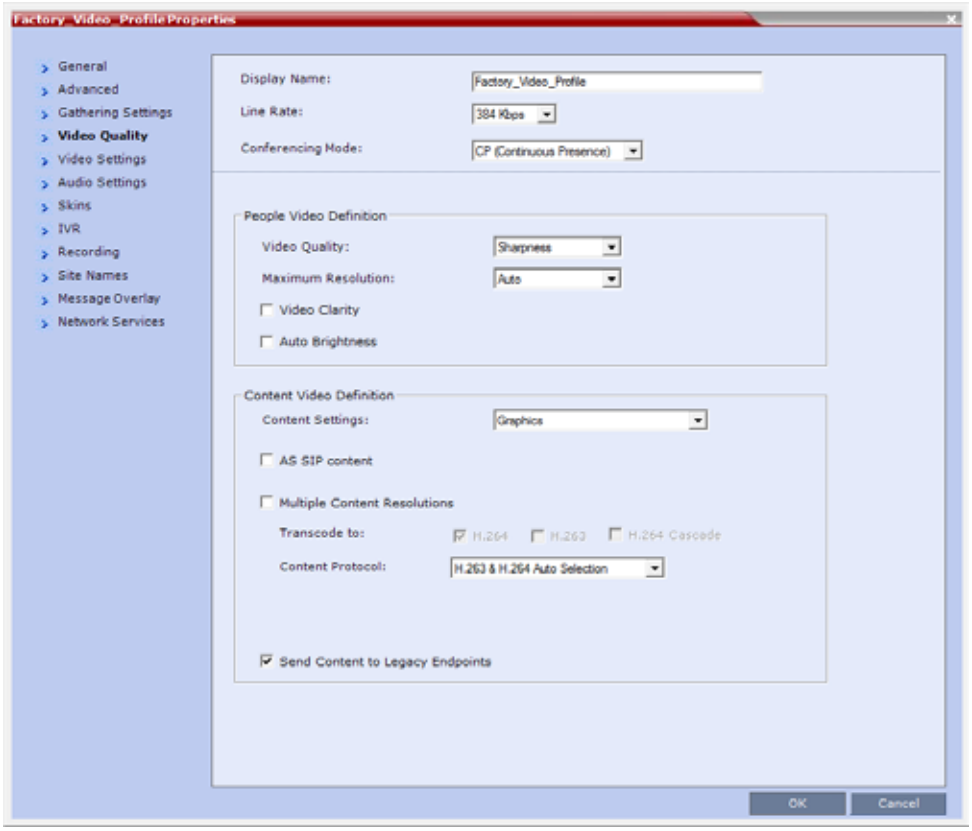


3 Open the **Advanced** tab.



4 Select Prefer TIP as the **TIP Compatibility** mode. To view its behavior, see the Content Sharing Behavior table at the end of this procedure.

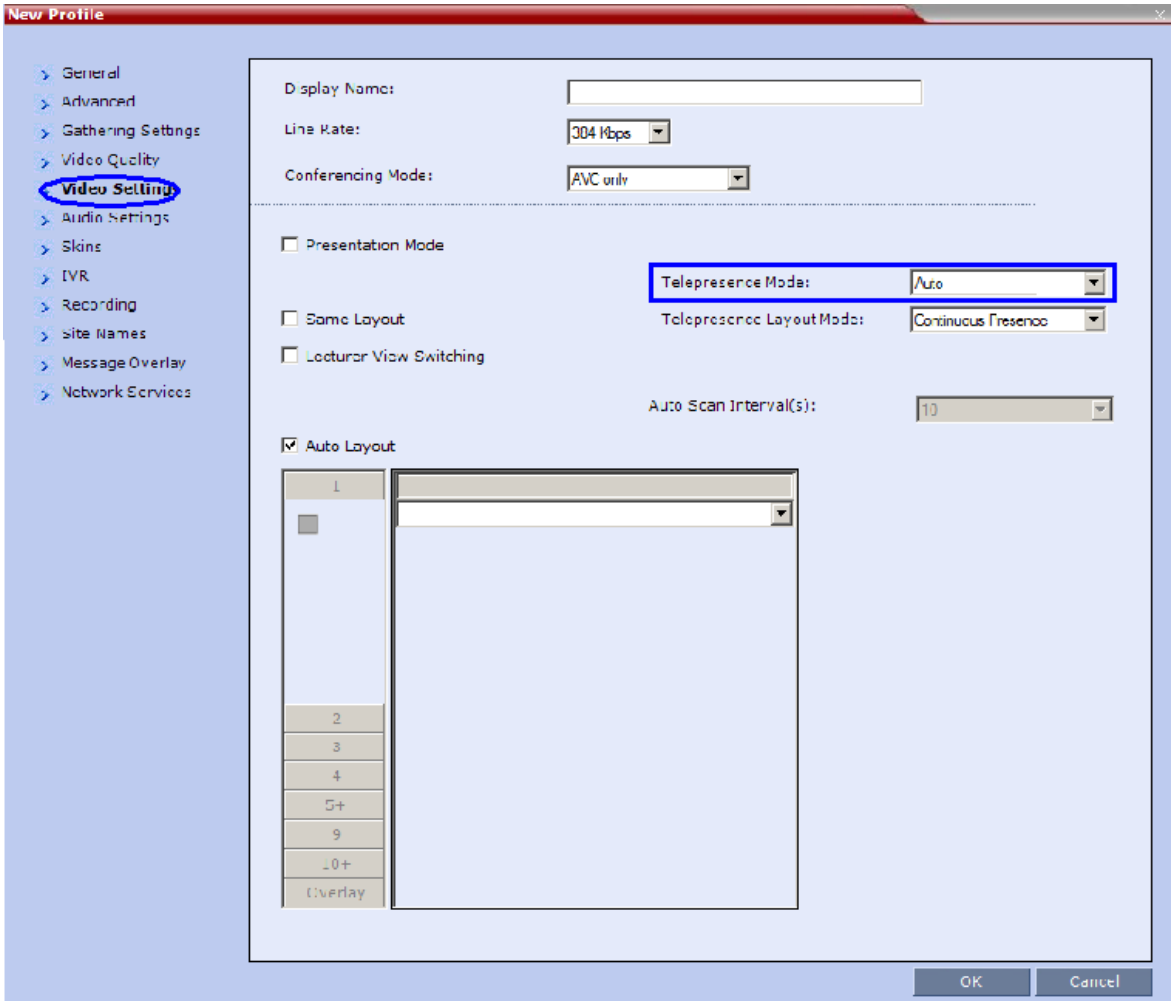
5 Open the **Video Quality** tab.



Content Settings is disabled if **TIP Compatibility** is set to **Prefer TIP** in the **Advanced** tab.

For more information on content in TIP environments, see Content Sharing Behavior.

6 Open the **Video Settings** tab.



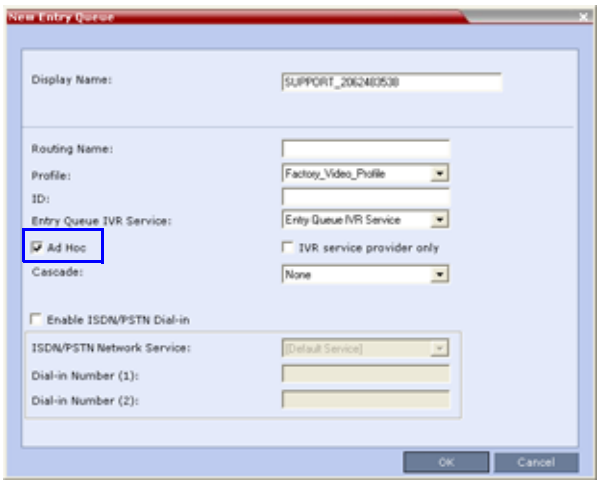
7 Set the **Telepresence Mode** to **Auto**.

8 Assign the New Profile to the Meeting Room. For more information see Creating a New Meeting Room.

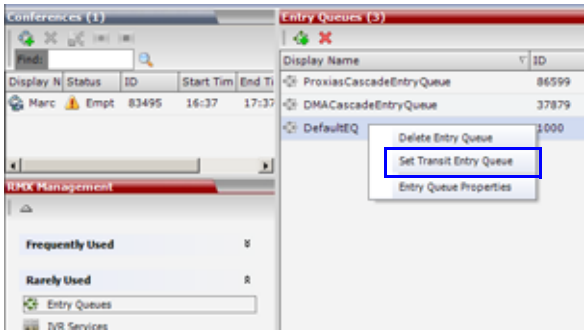
Procedure 5: Configuring an Ad Hoc Entry Queue on the Collaboration Server if DMA is not used

1 Create or select the **Entry Queue** as described in Entry Queues.

2 In the New Entry Queue or Entry Queue Properties dialog, ensure that **Ad Hoc** is selected.



3 Ensure that the Entry Queue is designated as the **Transit Entry Queue** as described in Transit Entry Queue.



Procedure 6: Configuring a Meeting Room on the Collaboration Server

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

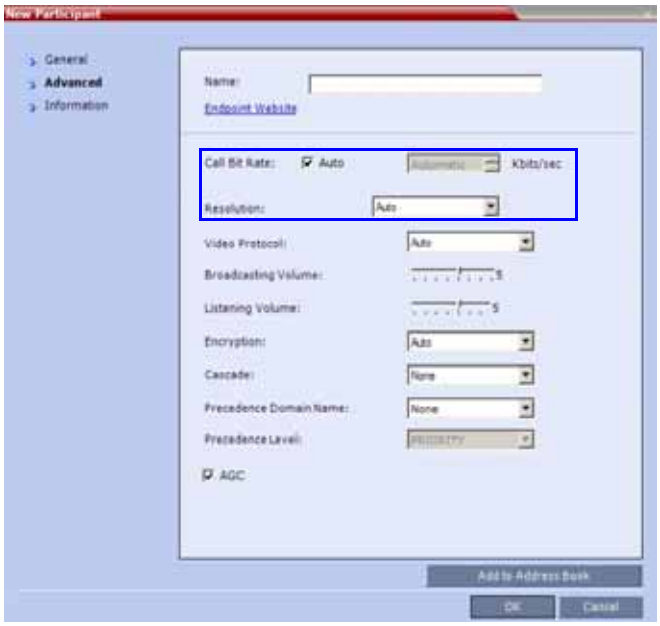
For more information see Creating a New Meeting Room.

Procedure 7: Configuring Participant Properties for Dial Out Calls

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

a Define the New Participant - General settings. For more information see Adding a Participant to the Address Book.

b Select the **Advanced** tab.



c Ensure that:

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

Collaboration with Microsoft and Cisco

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

The Collaboration Server natively inter-operates with Microsoft Lync and Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls between:

- Polycom Immersive Telepresence Systems (ITP) Version 3.1.1:
  - RPX 200
  - RPX 400
  - OTX 300
- Polycom video conferencing endpoints
  - Standalone HDX
  - Polycom 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 Polycom and Cisco Infrastructure - Polycom endpoints using SIP shows a company that has a mixture of Polycom, Cisco and Microsoft endpoints, room systems and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the Collaboration Server as the conference bridge.

This solution enables Polycom, 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 Polycom and Cisco Infrastructure - Polycom endpoints using SIP:

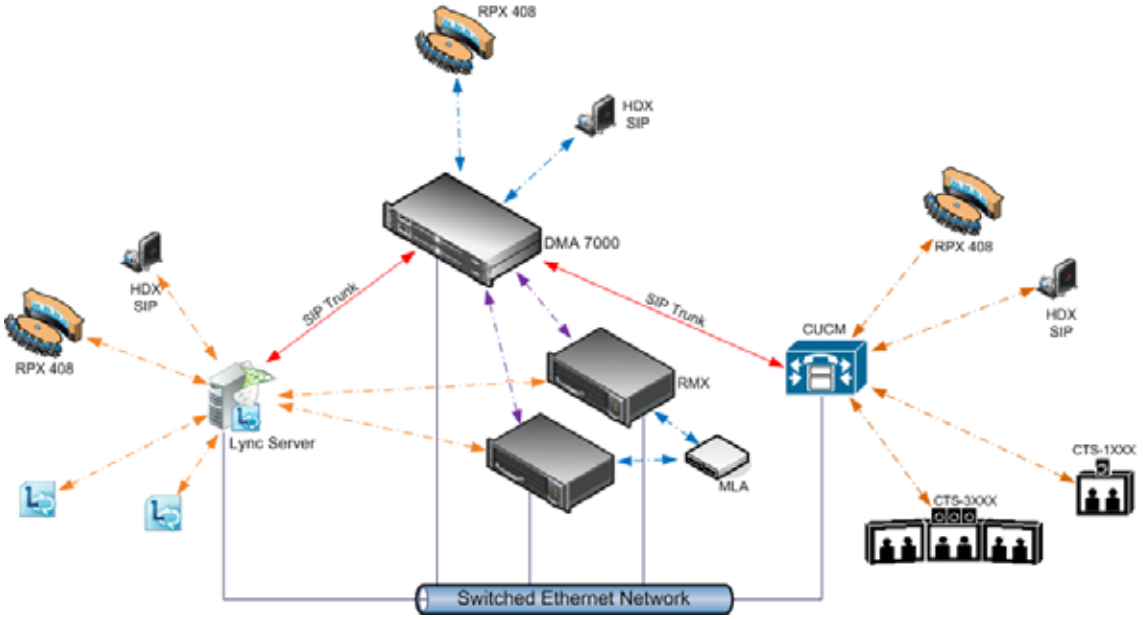
- DMA is required as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the DMA.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- Dial- out calls directly from the RMX are not supported.
- Lync Clients cannot share content with CTS
- SIP trunks are required to the DMA from:
  - MS Lync as a Static Route.
  - CUCM

Deployment Architecture

- DMA is required as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the DMA.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- Dial- out calls are not supported
- Lync Clients can not share content with CTS
- SIP trunks are required to the DMA from:
  - MS Lync as a Static Route.
  - CUCM

For more information, see Cisco TIP Support.

POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture



POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components

Component	Version
Polycom	
HDX	3.0.5
Polycom® RealPresence® Media Suite	1.7
DMA	5.0
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

POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components

Component	Version
Outlook 2010	14.0.6112.5000
Cisco	
CUCM	8.5, 8.6.2
Cisco Unified Personal 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

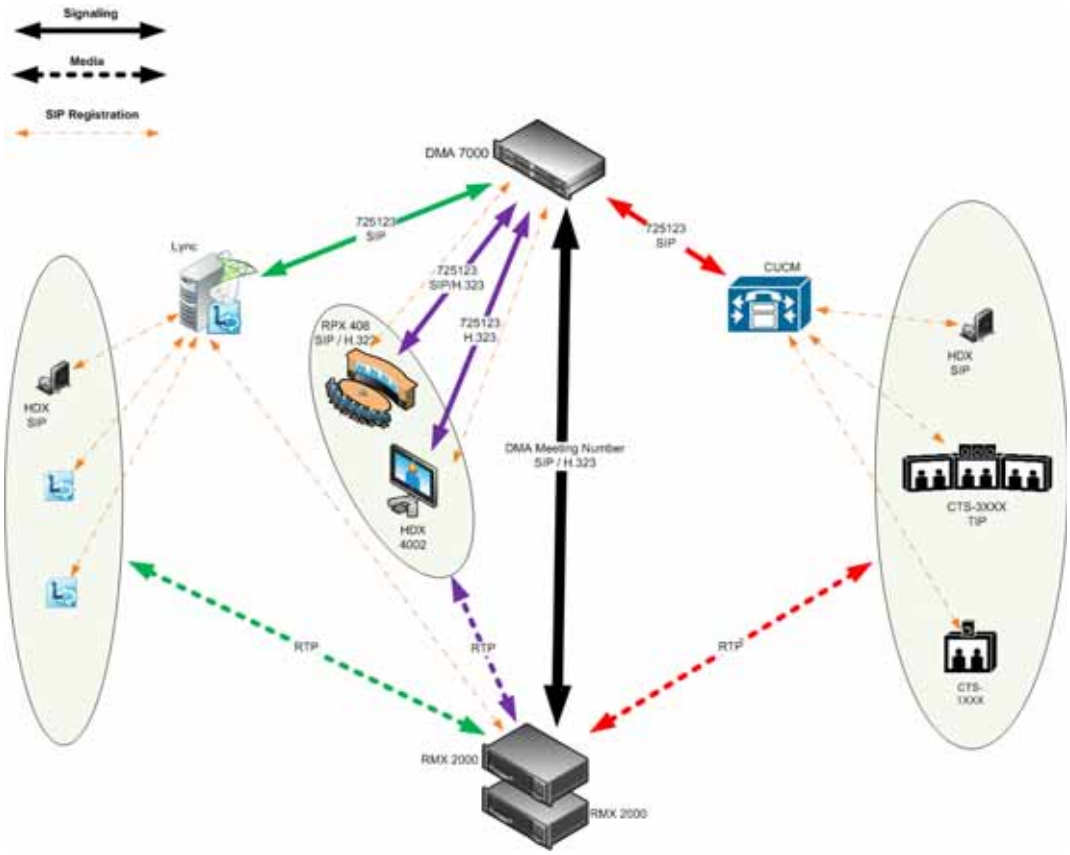
The following are not supported:

- 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 DMA

In this example:

- Endpoint registration: To either DMA, Lync or CUCM.
- DMA dial in Prefix: 72
- Virtual Meeting Room in DMA: 725123
- DMA Meeting Number: Generated by DMA



Administration

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

DMA

The DMA system can be configured 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 used as a SIP peer, the DMA system can host video calls between Cisco endpoints that are registered with the CUCM, Lync Clients that are registered with the Lync Server and Polycom endpoints that are registered with the DMA system.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Polycom DMA System as SIP Peer.

Microsoft Lync Server

Microsoft Lync Server manages Presence for each registered Polycom endpoint and enables video calls between Lync Clients and Polycom endpoints allowing Lync contacts to be called without needing to know their addresses.

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

CUCM

When Polycom SIP endpoints (voice and video) are registered 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 will be used in such cases.

For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*, Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants.

Solution Interoperability Table

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

Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	9.0.1	Cisco Unified Communication Manager: • CUCM must be configured to route calls to ASR/SBC. CUCM must be configured with a SIP trunk to the Service Provider's SBC. • All endpoints must register once with the CUCM • SIP trunks from CUCM to Polycom system components (eg. DMA) should be configured with Music on Hold disabled.
ASR (Cisco SBC)	100x	The Cisco Aggregation Services Routers (ASR) Series includes Cisco IOS XE 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.
Polycom Equipment		
DMA	6.0.0_ATT_Build_25	Polycom Distributed Media Application • DMA is an optional component but is essential if Content sharing is to be enabled. • All SIP endpoints register to DMA as a SIP Proxy. • DMA should be configured to route SIP calls (with CTS destination) to CUCM. • DMA can be configured with a VMR (Virtual Meeting Room). Incoming calls are then routed to the Collaboration Server.

Solution Architecture Components

Component	Version	Description
Collaboration Server	8.1.1 and up	MCU: • Functions as the network bridge for multipoint calls between H.323, SIP and TIP endpoints. • The Collaboration Server can be interfaced to CUCM using a SIP trunk, enabling CTS to join multipoint calls on Collaboration Server. Signaling goes through the CUCM while the media in TIP format goes directly between the CTS and Collaboration Server. • The Collaboration Server must be configured to route outbound SIP calls to DMA. • Collaboration Server must be configured 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 multi-screen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX or OTX systems.
HDX and ITP Endpoints	3.1.1.1	Telepresence, desktop and room systems. • Polycom SIP endpoints must register to DMA as SIP Proxy.
Microsoft		
Lync 2010	4.0.7577.183 CU4	
Lync 2010 client	4.0.7577.405 1 CU4	
Exchange 2007 R2 SP3	8.3.213.1	
Exchange 2010 SP2	14.2.247.5	
Outlook 2007	12.0.6557.50 01 SP2	
Outlook 2010	14.0.6112.50 00	

TIP Layout Support & Resource Usage

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

- OTX system - Works with three screens, therefore no adjustment is required and it should be set to work in room switch Telepresence Layout Mode (while avoiding zooming in/out)
- RPX 2xx - This endpoint works with two screens, therefore it will adjust to use only **one** screen.
- RPX 4xx - This endpoint works with four screens, therefore it will adjust 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 endpoint 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 is no one fully free media (ART) processor available.

The MCU will always try to fill up one media processor with up to three TIP-enabled endpoint 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 Polycom), virtual participants are used to indicate the additional screens in the in the Web Client. For example, if the endpoint has three screens, the system will display 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 Polycom Components

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

To configure the Microsoft, Cisco and Polycom components:

1. Configure a SIP Trunk connection between the Polycom DMA system and the Cisco Unified Communications Manager (CUCM).

   For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Polycom DMA System as SIP Peer.

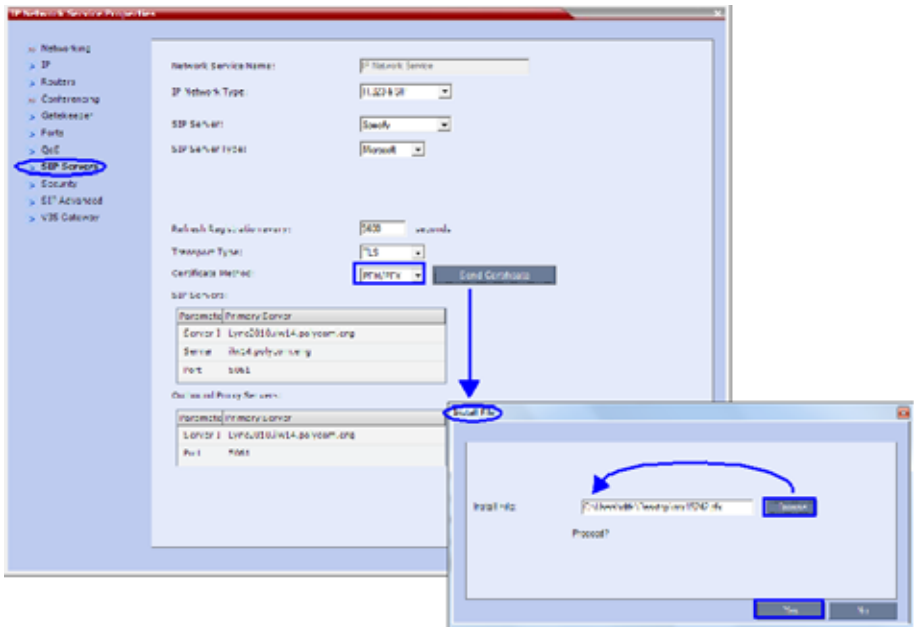
2. Register the Collaboration Server to the Lync Server
   a. Install a Security Certificate on the Collaboration Server.

      The Certificate is obtained from the System Administrator and saved on the Workstation.

   b. In the **SIP Servers** tab of the **IP Network Services Properties** dialog:
      i. Set **Certificate Method** to **PEM/PFX**.
      ii. Click **Send Certificate**.

         The I**nstall File** dialog is displayed.

      iii. Browse to the saved Certificate on the Workstation, and click **Yes** to install it.



For more information see:

- Deployment into Lync Environments.
- *Polycom Unified Communications Deployment Guide for Microsoft Environments*, Configuring Your Collaboration Server System for use with the Lync Server.

3 Register the 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.

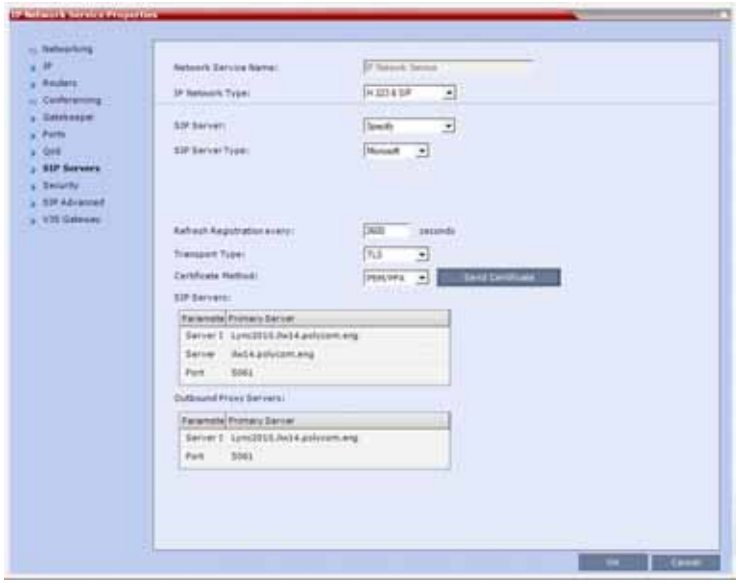
e If not selected by default, change the Transport Type to **TLS**.

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 f**.)

i In the Outbound Proxy Servers table, set Port to **5061** (the same value as in Step g).



For more information see *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

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 will reject calls at lower line rates, therefore the System Flag value must be **1024** or higher.

For more information see Modifying System Flags.

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 Polycom TIP-enabled endpoints connecting to the TIP-enabled Telepresence conference.

NO_FORCE - No forcing is applied, and Polycom TIP-enabled endpoints can connect to the TIP-enabled Telepresence conference at any line rate or resolution.

7 Reset the Collaboration Server.

8 Register the DMA to the Lync server

For more information see *Polycom Unified Communications Deployment Guide for Microsoft Environments*, Configure a DMA System SIP Peer for the Lync Server.

9 Register the ITP endpoints to the Lync server.

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, Deployment Process for Polycom Immersive Telepresence Systems.

10 Register Lync Clients to the Lync server.

For more information see the relevant Lync documentation.

11 Register DMA to the CUCUM server

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Using a Polycom DMA System in a Cisco Environment.

12 Register CTS1000 and CTS3000 endpoints to the CUCUM server

For more information see the relevant Cisco documentation.

13 Register ITP endpoints to the CUCM server.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, Direct Registration of Polycom Telepresence Systems with the Cisco Unified Communications Manager.

14 Register HDX endpoints to the DMA as Gatekeeper

For more information see the *Polycom® DMA™ 7000 System Operations Guide*.

15 Open MLA to configure ITP Layouts

MLA (Multipoint Layout Application) 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.

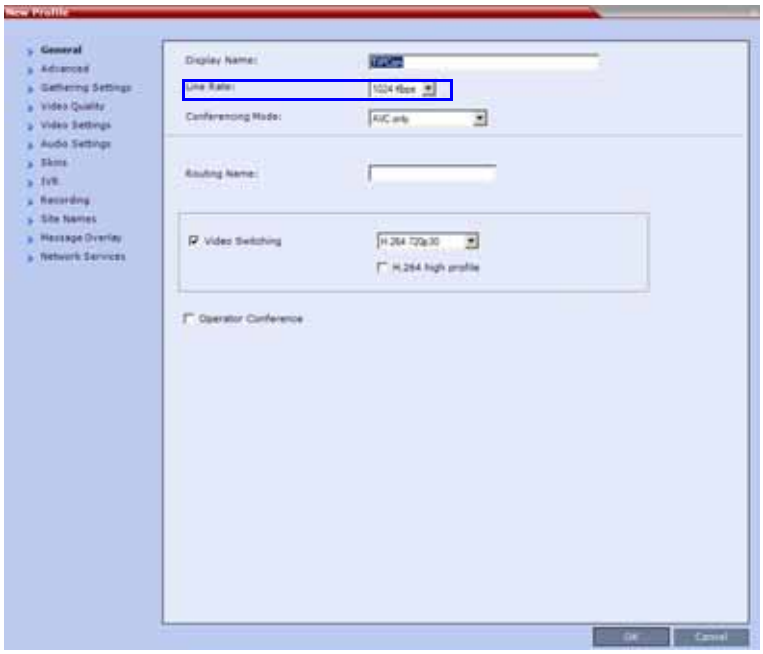
For more information see *Polycom Unified Communications Deployment Guide for Cisco Environments*.

16 Configure a TIP Enabled Profile on the Collaboration Server.

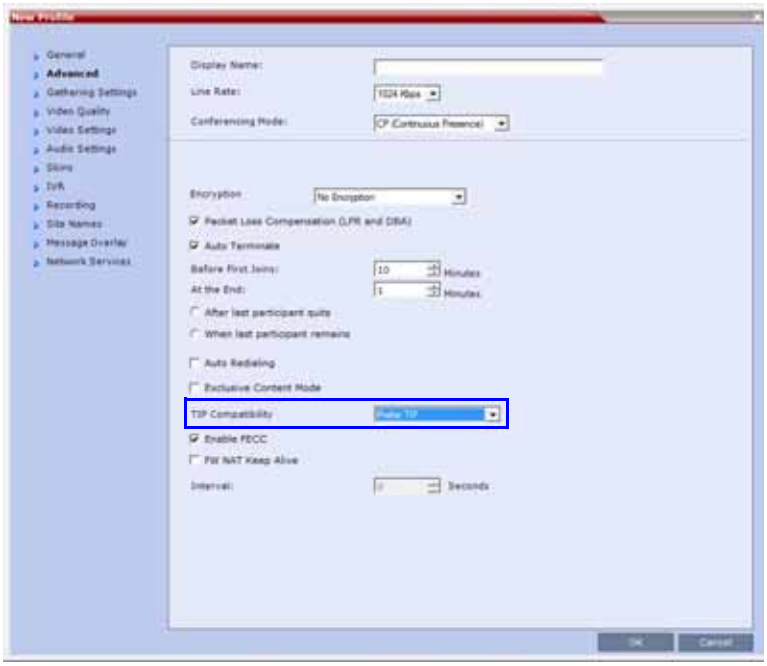
a Create a New Profile for the Meeting Room.

For more information see Defining New Profiles.

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. To view its behavior, see the Content Sharing Behavior table listed below.

Note: Feature Applicability in TIP Enabled Conferencing

When **Prefer TIP** is selected, **Video Switching**, Gathering Settings, Skins, Message Overlay, Site Names and Network Indications are disabled.

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

		Content Receiver		
None		**HDX / ITP**		**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		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.

In **Prefer TIP** mode, it is pre-requisite 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.

Encryption

Encryption between the 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 be encrypted using TLS. When upgrading, the Collaboration Server automatically creates a self-signed certificate to support encrypted communications with CISCO endpoints.

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

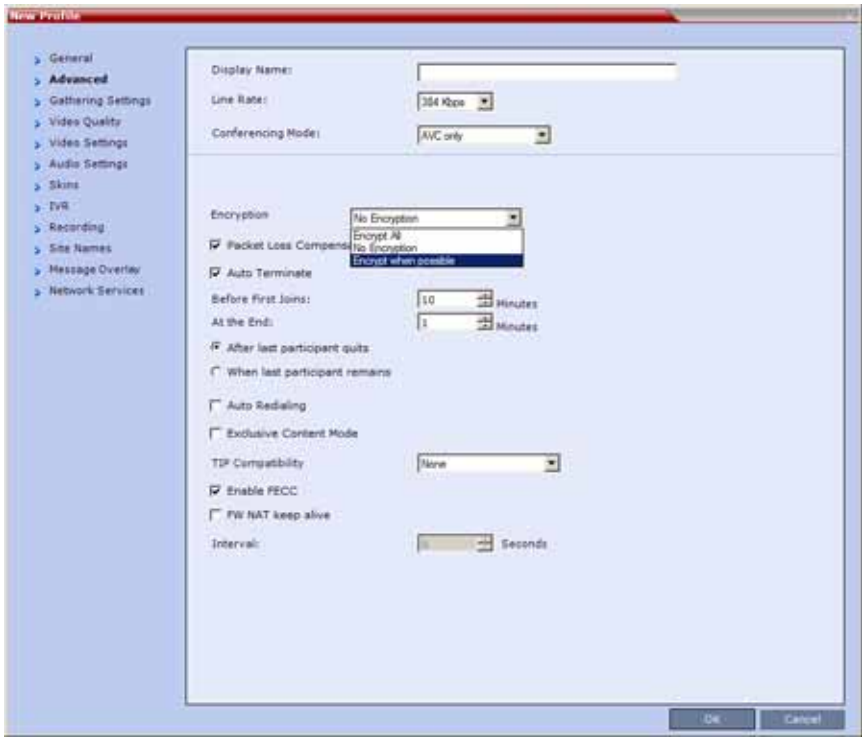
Guidelines

- This feature is not supported in Ultra Secure Mode.
- Voice activity metrics and RTP are not encrypted.
- In the event that DTLS negotiation fails, SIP will be encrypted using TLS if enabled in the IP Management Network properties, SIP Servers tab. DTLS negotiation does not require SIP TLS.
  - In a mixed CISCO and Microsoft Lync environment, in order 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, must have been issued by the same certificate authority that issued the certificates used by both the Microsoft Lync server and the CUCM server.
- The flag, **SIP_ENCRYPTION_KEY_EXCHANGE_MODE**, is used 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 was tested using the following CISCO components:

- Cisco CUCM Version 9.0
- Cisco TPC Version 2.3
- Cisco endpoints running Version 1.9.1
  - C20, C40, C60, and C90 running TC5
  - CTS500
  - CTS1310
  - CTS3010

To enable DTLS negotiation for content encryption:

1 In a new or existing **Profile**, open the **Advanced** tab.



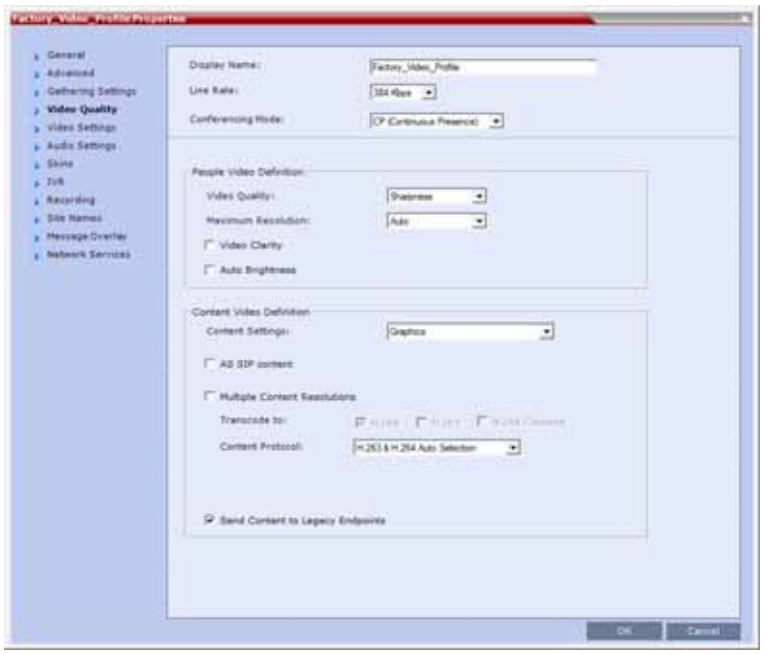
2 Set **Encryption** to either **Encrypt All** or **Encrypt when possible**.

3 Set **FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE** System Flag to NO

These setting will enable encrypted and non-encrypted H.323 participants to connect to encrypted or non-encrypted conferences.

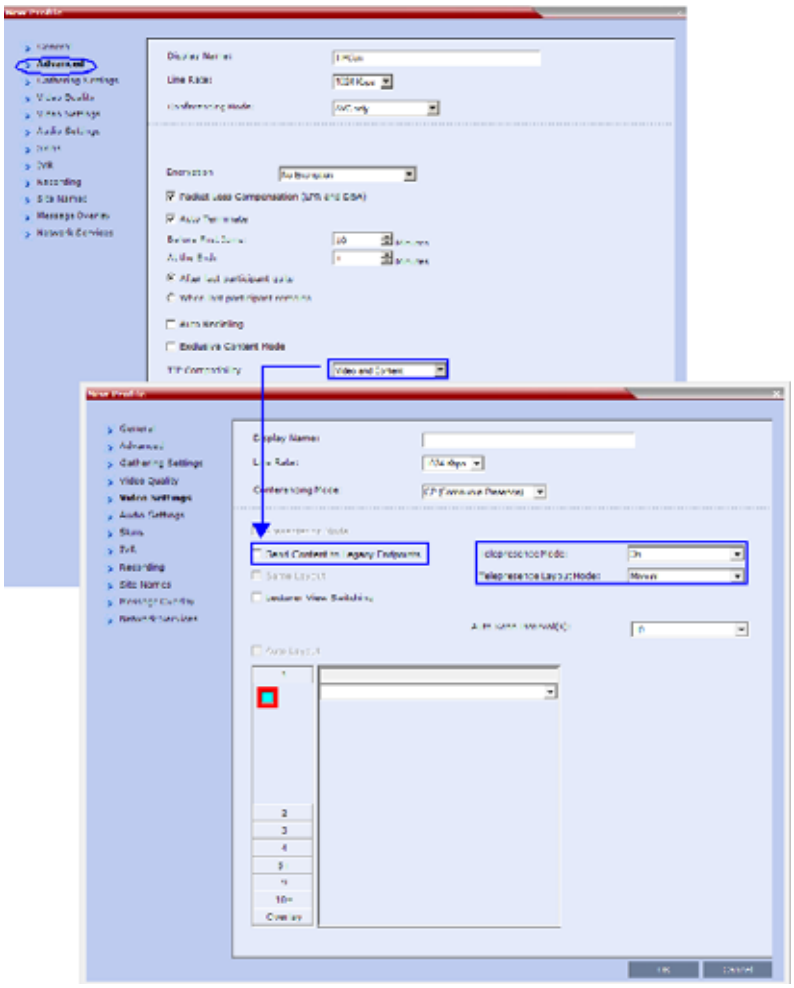
For more information see Encryption.

a Open the **Video Quality** tab.



Content Settings is disabled if **TIP Compatibility** is set to **Prefer TIP** in the **Advanced** 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**. For more information see Creating a New Meeting Room.

5 Configure a **Virtual Meeting Room (VMR)** on the DMA.

The procedures for configuring **DMA** are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Resolution Configuration

The resolution configuration dialog is not 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.

To register the various types endpoints:

1. Configure HDX endpoints to register to Lync Server.

   The procedures for configuring HDX endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

2. Configure H.323 endpoints to register to DMA as SIP Proxy

   The procedures for configuring SIP endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

3. Configure SIP endpoints to register to:
   - DMA as SIP Proxy
   - Lync Server as SIP Proxy
   - CUCM as SIP Proxy

   The procedures for configuring *SIP* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

4. Configure TIP endpoints to register to:
   - DMA
   - CUCM

For more information on the above, see *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Content

Endpoint Registration and Dialing Method affect the Video and Content Sharing characteristics of the conference as detailed in the table below.

Video and Content

Endpoint Registration	Lync	CUCM	DMA
Dialing Method	**ITP /HDX** RTV Key is required for HDX and ITP	**ITP /HDX** **TIP Key is required for HDX**	**ITP /HDX** **TIP Key is required for HDX**
HDX to 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 Collaboration Server	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints		
CTS to Collaboration Server	• HD1080p30 • TIP Content Sharing • Content: XGA,5fps		

Operations During Ongoing Conferences

Moving participants between TIP enabled meetings and non TIP enabled meetings is not possible.

Monitoring

CTS Participants

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

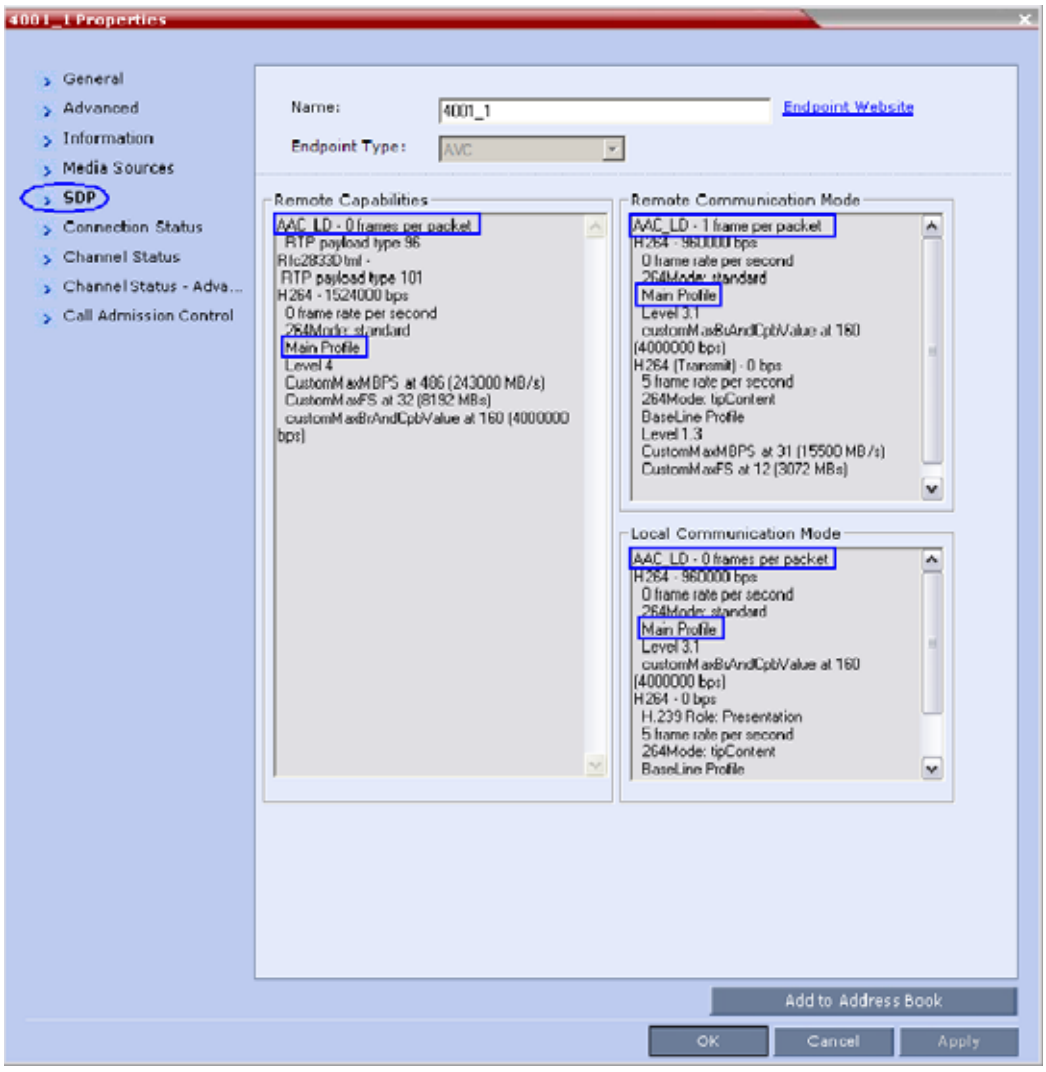
   The **Participant Properties - General** dialog box opens.

2. Select the **SDP** tab.

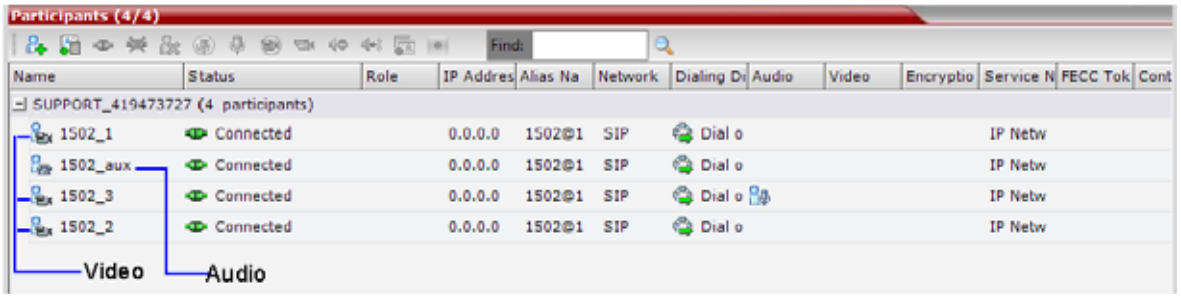
   The following are indicated in the **Remote Capabilities**, **Remote Communication Mode** and **Local Communication Mode** panes:

   - AAC_LD - Audio Protocol

- Main Profile - Video protocol



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. The **Participant** list below shows a connected CTS 3000, a 3-screen system.



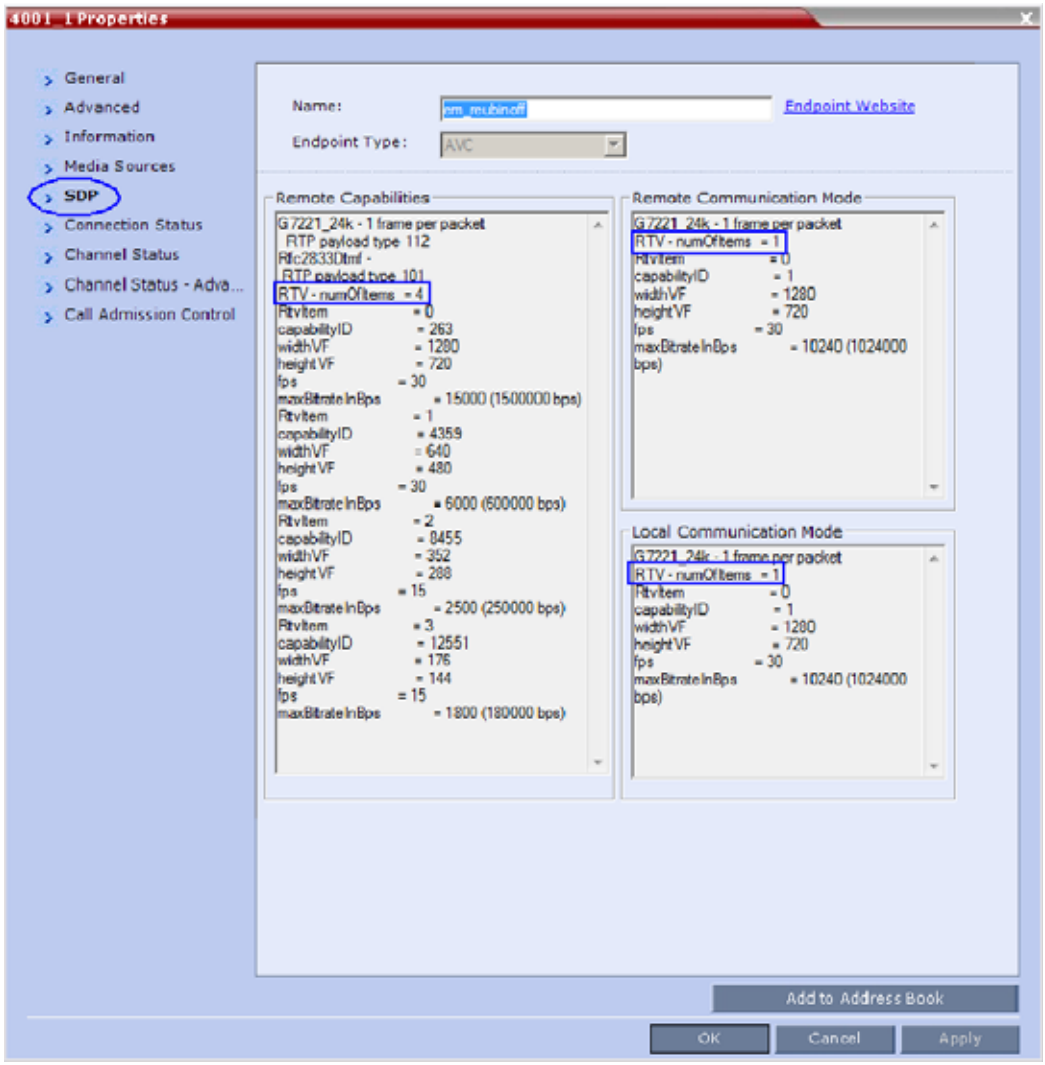
Lync Participants (RTV)

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

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

2 Open the **SDP** tab.

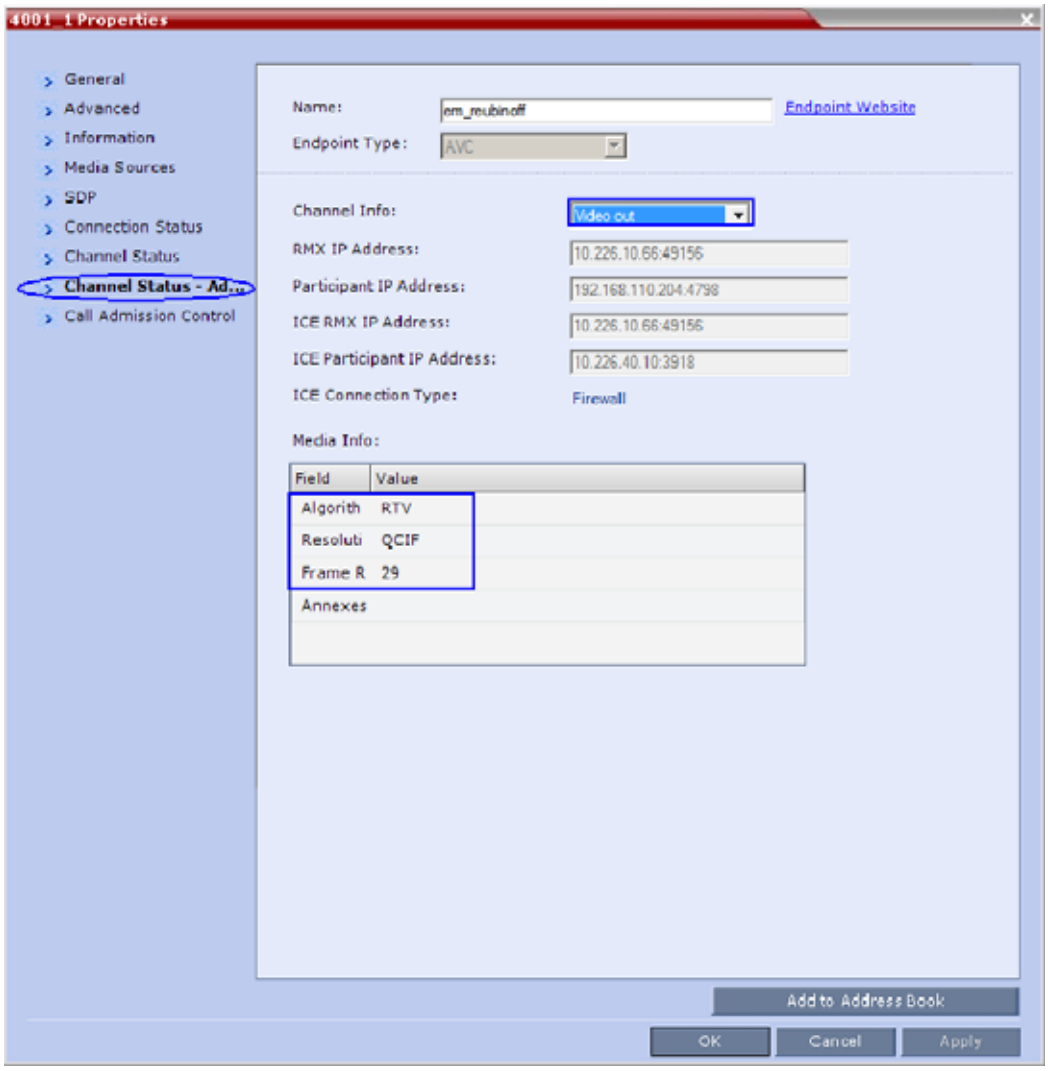
RTV is indicated in the **Remote Capabilities**, **Remote Communication Mode** and **Local Communication Mode** panes:



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 non-encrypted conferences.
- Auto Layout sometimes ignored for CTS and Lync Clients calling through DMA.

  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.

Appendix - Direct Connection to the RealPresence Collaboration Server

Direct connection to the RealPresence Collaboration Server 2000/4000/1800 is necessary to:

- Connect to and modify the RealPresence Collaboration Server Factory Default Management Network settings without using the USB memory stick.

  If you do not wish to use the USB memory stick method of modifying the RealPresence Collaboration Server Management Network parameters, you can establish a direct connection between a workstation and the RealPresence Collaboration Server to modify them.

- Connect to the RealPresence Collaboration Server Alternate Management Network for support purposes.

  While separate from all other networks, the Alternate Management Network has identical functionality to the Management Network although it cannot be reconfigured and it operates based on factory defaults only.

  Security Notes

  - Connection to the Alternate Management Network bypasses LAN and Firewall security. Strict control of access to LAN 3 port is recommended.
  - The Alternate Management Network is only available if Network Separation has not been performed. For more information, see Multiple Network Services.

  The Alternate Management Network cannot be configured and operates according to factory defaults.

- Connect to the RealPresence Collaboration Server via a modem.

Note that you cannot directly connect to the RealPresence Collaboration Server, Virtual Edition and you cannot directly connect to a RealPresence Collaboration Server when it is in Ultra Secure Mode.

Establish a Direct Connection to the RealPresence Collaboration Server

To establish a direct connection to the RealPresence Collaboration Server you must:

- Configure the Connecting Workstation
- Cable the Workstation Connection to the RealPresence Collaboration Server
- Connect to the MCU with the RMX Web Client

Configure the Connecting Workstation

Before connecting directly to a RealPresence Collaboration Server, use the Windows New Connection Wizard to configure the IP Address, Subnet Mask and Default Gateway settings of the connecting workstation to be compatible with either the RealPresence Collaboration Server Default Management Network or Alternate Management Network.

See the documentation for the workstation operating system for specific information about how to configure these network values.

The addresses required for connection to either the RealPresence Collaboration Server Default Management Network or Alternate Management Network are listed in the table below.

Reserved IP Addresses

	IP Address	
Network Entity	**Management Network (Factory Default)**	**Alternate Network**
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

Follow these guidelines:

- The workstation's IP address must be in the same network neighborhood as the RealPresence Collaboration Server Control Unit IP address. None of the reserved IP addresses listed in Reserved IP Addresses list above should be used for the IP Address.
- The Subnet mask and Default gateway addresses should be the same as those for the RealPresence Collaboration Server Management Network.

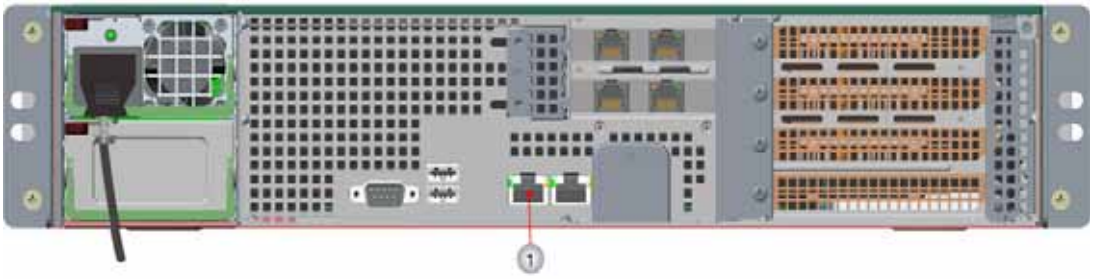
Cable the Workstation Connection to the RealPresence Collaboration Server

Direct connect to the RealPresence Collaboration Server is achieved by correct cabling.

To connect directly to the RealPresence Collaboration Server:

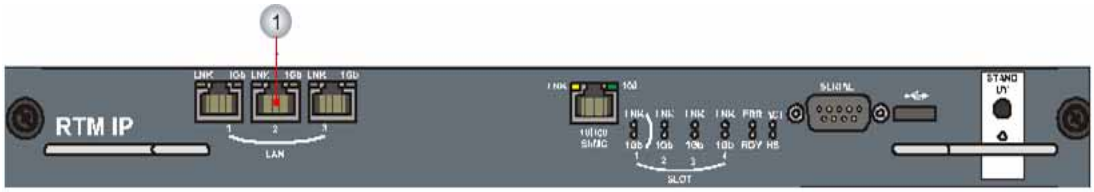
1. Using a LAN cable, connect the workstation:
   - To the LAN 1 Port on the RealPresence Collaboration Server (RMX) 1800 back panel.
   - To the LAN 2 Port on the RealPresence Collaboration Server (RMX) 2000/4000 back panel.

RealPresence Collaboration Server (RMX) 1800



Reference Number	Description
1	LAN 1 port

RealPresence Collaboration Server (RMX) 2000



RealPresence Collaboration Server (RMX) 4000

Reference Number	Description
1	LAN 2 port

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.

To connect to the MCU with the RMX Web Client:

1 Open a Microsoft 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 *Polycom RealPresence Collaboration Server Getting Started Guide*.

Configure the Primary Management Network

To configure the primary management network:

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 Collaboration Server's back panel.

4 Connect LAN 2 Port on the 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 Collaboration Server Web Client Login screen, enter the default **Username** (POLYCOM) and **Password** (POLYCOM) and click **Login**.

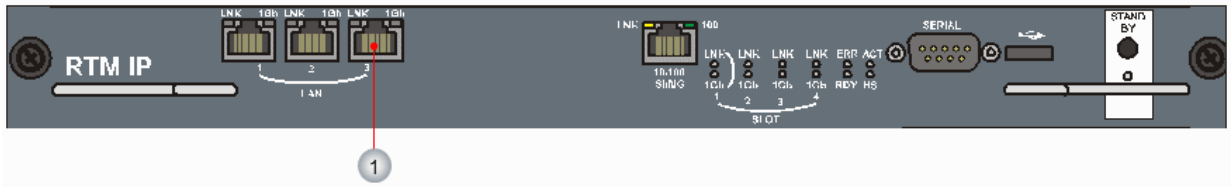
Connect the Alternate Management Network (2000/4000)

The Alternate Management Network enables direct access to the RealPresence Collaboration Server for support purposes. The Alternate Management Network cannot be configured and operates on factory defaults.

The Alternate Management Network is only accessible using a LAN cable, connecting the pre-configured 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

RealPresence Collaboration Server (RMX) 2000



RealPresence Collaboration Server (RMX) 4000

To connect to the Alternate Management Network:

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 is displayed.
3. Enter the administrator's **Username** and **Password**, and click **Login**.

   The RMX Web Client starts and the Collaboration Server can be managed in the same manner as if you had logged on to the Management Network.

Connecting the Collaboration Server via Modem (2000/4000)

Remote access to the Collaboration Server's *Alternate Management Network* is supported via an external PSTN <=> IP modem.

To connect via modem to the Alternate Management Network perform the following procedures:

1. **Install the RMX Manager** – The web client enables direct access to the Collaboration Server for support purposes.
2. Configure the modem – Assign the modem an IP address on a specific subnet in the Alternate Management Network.
3. Create a dial-up connection – Using Windows **New Connection Wizard**.
4. **Connect to the Collaboration Server** – Via the RMX Manager.

Configure the Modem

Configure the modem with the following settings.

- IP address – near 169.254.192.nn

- Subnet Mask – 255.255.240.0

Create a Dial-up Connection

Using the This procedure is performed once. Only the **Dial** field in the **Connect** applet (see step 11) is modified for connection to different modems.

To create a dial-up connection:

1. In Windows, navigate via the **Control Panel** to the **Network Connections** applet and select Create a new connection.
2. When the **New Connection Wizard** is displayed, click **Next**.
3. In the **Network Connection Type** dialog, select **Connect to the Internet** and click **Next**.
4. In the **Getting Ready** dialog, select **Set up my connection manually** and click **Next**.
5. In the **Internet Connection** dialog, select **Connect using dial-up modem** and click **Next**.
6. In the **Connection Name** dialog, enter a **Name** for the modem connection (e.g**. Modem Connection**) and click **Next**.
7. In the **Phone Number to Dial** dialog, enter the Phone Number for the modem and click Next.
8. In the **Connection Availability** dialog, select Anyone's use and click Next.
9. In the **Internet Account Information** dialog, complete the **Username**, **Password** and **Confirm Password** fields, and click Next.
10. The **Connection** applet is displayed with the field values filled in as specified by the **New Connection Wizard.**
11. Click Dial to establish a connection to LAN 3 Port via the modem.

    The **Windows – Network Connections** applet displays **Connected** status for the new connection.

Appendix - Homologation for Brazil

This section describes how the RealPresence Collaboration Server meets homologation requirements for import into Brazil.

H.323 & SIP Protocol Flag Options

Using a set of system flags, the user has the ability to select either Polycom proprietary or H.323/SIP standard protocol settings.

H.323 & SIP Flag Settings

Three flags are enabled on the RealPresence Collaboration Server, allowing the user to define and select either standard or proprietary H.323 and SIP protocol settings.

Flag name: SIP_TIMERS_SET_INDEX

Description: SIP Timer type timeout settings according to standard or proprietary protocol.

Flag section: CS_MODULE_PARAMETERS

Possible Values: either 0 or 1.

0 - Polycom standard (flag default setting)

1 - SIP Standard recommendation. For homologation and certification testing, this flag must be set to 1.

For use as a reference, the following table lists the SIP timer types for each flag setting and their corresponding timeout values in milliseconds.

SIP Timer Types

	Value (in milliseconds)	
SIP TIMER Types	**POLYCOM (flag default)**	**Standard Recommended**
T1	50000	500
T2	20000	4000
TimerB	35000	32000
TimerC	35000	60000
TimerD	32000	32000

SIP Timer Types

SIP TIMER Types	Value (in milliseconds)	
	POLYCOM (flag default)	**Standard Recommended**
TimerF	35000	32000
TimerH	35000	32000
TimerI	5000	5000
TimerJ	32000	32000
TimerK	5000	5000

Flag name: H323_TIMERS_SET_INDEX

Flag description: Enables or disables H.323 index timer according to standard or proprietary H.323 protocol.

Section CS_MODULE_PARAMETERS

Possible values:

0 - Sets the H.323 index timer to Polycom proprietary (flag default setting)

1 - Sets the H.323 index timer based on the H.323 Standard recommendation. For homologation and certification testing, this flag must be set to 1.

Flag name: DISABLE_DUMMY_REGISTRATION

Flag description: Enables or disables SIP dummy registration on the domain.

Flag Section: MCMS_PARAMETERS_USER

Possible values:

NO - Disables SIP dummy registration (flag default setting).

YES - Enables SIP dummy registration. For homologation and certification testing, the flag must be set to **YES**.