Version **8.1.4.J** | January 2014 | DOC2713A

Polycom® RealPresence® Collaboration Server (RMX) 1500/2000/4000 Release Notes for Maximum Security Environments

Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

This software has achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 8.1.4.J software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

Regulatory Notices

Warning

- No user-serviceable parts inside. Do not open.
- The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device
- This equipment must be earthed. Do not power this equipment if the integrity of themains earthing conductor cannot be verified
- Only trained and qualified personnel should be allowed to install, replace, service or repair this equipment
- To prevent system overheating do not operate in an ambient temperature exceeding 40° C / 104° F
- Installation of this equipment must comply with local and national electrical codes.

Environmental

This product is compliant with the requirements of the recast RoHS Directive 2011/65/EU. Information can be obtained from Polycom Ltd, 270 Bath Road, Slough, Berkshire, SL1 4DX, UK or via: **RoHSinformation@polycom.com**

Information on recycling can be found at: **www.polycom.com/WEEE**

Disposal of this equipment should be carried out in accordance with local environmental guidelines and regulations for waste. For further information please contact: **TakeBack@polycom.com**

Batteries

Below is a listing of batteries that could be present in the product:

Description:Internal CMOS battery

Type:CR2032 Lithium Coin Cell

Weight:3.3g

Batteries used in this product are in compliance with EU Battery Directive 2006/66/EC.

Batteries in this product are not based on mercury, lead or cadmium technologies.

Batteries in this product are not intended to be replaced or removed by the user

Additional information on the safe use and recycling of batteries can be found at: **www.polycom.com/batteries**

United States Federal Communication Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Modifications: Any modifications made to this device that are not approved by Polycom, Inc. may void the authority granted to the user by the FCC to operate this equipment.

Industry Canada (IC)

This Class [A] digital apparatus complies with Canadian ICES-003

Cet appareil numerique de la classe [A] est conforme a la norme NMB-003 du Canada

European Economic Area (EEA)	
Česky [Czech]:	Polycom (UK) Ltd tímto prohlašuje, že tento Polycom RMX je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]:	Undertegnede Polycom (UK) Ltd erklærer herved, at følgende udstyr Polycom RMX overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]:	Hiermit erklärt Polycom (UK) Ltd, dass sich das Gerät Polycom RMX in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]:	Käesolevaga kinnitab Polycom (UK) Ltd seadme Polycom RMX vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English:	Hereby, Polycom (UK) Ltd. Declares that this Polycom RMX is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Por medio de la presente Polycom (UK) Ltd declara que el Polycom RMX cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]:	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Polycom (UK) Ltd ΔΗΛΩΝΕΙ ΟΤΙ Polycom RMX ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]:	Par la présente Polycom (UK) Ltd déclare que l'appareil Polycom RMX est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]:	Con la presente Polycom (UK) Ltd dichiara che questo Polycom RMX è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Íslenska (Icelandic):	Hér með lýsir Polycom (UK) Ltd yfir því að Polycom RMX er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC
Latviski [Latvian]:	Ar šo Polycom (UK) Ltd deklarē, ka Polycom RMX atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šiuo Polycom (UK) Ltd deklaruoja, kad šis Polycom RMX atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]:	Hierbij verklaart Polycom (UK) Ltd dat het toestel Polycom RMX in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]:	Hawnhekk, Polycom (UK) Ltd, jiddikjara li dan Polycom RMX jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]:	Alulírott, Polycom (UK) Ltd nyilatkozom, hogy a Polycom RMX megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]:	Polycom (UK) Ltd erklærer herved at utstyret Polycom RMX er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]:	Niniejszym Polycom (UK) Ltd oświadcza, że Polycom RMX jest zgodne z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1999/5/WE.
Português [Portuguese]:	Polycom (UK) Ltd declara que este Polycom RMX está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]:	Polycom (UK) Ltd týmto vyhlasuje, že Polycom RMX spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovensky [Slovak]:	Polycom (UK) Ltd týmto vyhlasuje, že Polycom RMX spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]:	Polycom (UK) Ltd vakuuttaa täten että Polycom RMX tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]:	Härmed intygar Polycom (UK) Ltd att denna Polycom RMX står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
A full copy of the Declaration of Conformity can be obtained from Polycom Ltd, 270 Bath Road, Slough, Berkshire, SL1 4DX, UK.	

China CCC EMC statement
警告 此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对干 扰采取切实可行的措施。

Taiwan BSMI EMC statement

声　明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Japan VCCI EMC statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　　VCCI－A

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Worldwide EMC statement

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Optional ISDN interface card

If the above is fitted to the system then the following statements also apply;

United States Federal Communication Commission (FCC)

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the ISDN card itself is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

The following USOC, FIC and SOC codes are applicable to this equipment;

USOC Jacks: RJ48S

Service Order Code: 6.0N

Facility Interface Code: 04DU9.DN, 04DU9.BN, 04DU9.1KN, 04DU9.1SN

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact Polycom Inc in the U.S.A. 1-888-248-8294. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Table of Contents

Version 8.1.4.J - New Security Features

Table 1 *New Security Features*

#	Category	Feature Name	Description
1	Security	MLPP (Multi Level Precedence and Preemption)	Precedence is the method by which a call is assigned a priority level. The RMX supports two separately defined and configurable Precedence Domains.
2	Security	IEEE 802.1X Authentication	Provides enhanced security of wireless local area networks that follow the IEEE 802.11 standard.
3	Security	White List Access	Provides for enhanced security of web access to the RMX, by using a White List containing the addresses of all IP devices permitted to connect to the RMX.
4	Security	NTP	Beginning with this version, the RMX will use only the RTM-IP card as the NTP client to the NTP server. The clock setting can be maintained by the battery on the RTM-IP card in the event of system restart or shutdown. In previous versions both the RMX CPU and the RTM-IP card were clock sources. Support has been added for IPv6 addressing and depending on the RMX's selected IP addressing mode, both IPv4 and IPv6 addressing modes can be used.
5	Security	Alternative Network Address Types (ANAT)	Alternative Network Address Types (ANAT) is supported allowing a mixture of IPv4 and IPv6 addressing to be specified by the Session Description Protocol (SDP).
6	Security	Support of Previously Blocked Features	The following previously blocked features are supported: • SIP • SIP TLS • SIP Digest • SNMP • Recording Link • *AS SIP Content* is supported.
7	Security	DNS per IP Network Service	A *DNS* can be defined for each *IP Network Service* defined.
8	Security	Internet Control Message Protocol (ICMP)	The following *System Flags* have been added to enable the administrator to control *ICMP Redirect* and *Destination Unreachable* messages: • ENABLE_ACCEPTING_ICMP_REDIRECT • ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE

Table 1 *New Security Features*

#	Category	Feature Name	Description
9	Security	New Flag: SIP_TCP_TLS_TIMERS (Module: CS)	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: <1,5, 4,500000,5>
10	Interoperability: Redcom	New Flags: REDUCE_CAPS_FOR_REDCOM_SIP	To accommodate deployments where some devices have limits on the size of the SDP payload in SIP messages (such as LSCs from Redcom running older software versions), when the flag value = YES, the *SDP* size is less than 2kb and includes only one audio and one video media line. Default: NO
11	Interoperability: Redcom	*SIP_FORMAT_GW_HEADERS_FOR_REDCOM*	Controls whether the *RMX* adds 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. It is recommended to set this flag to YES whenever the *RMX* is deployed such that it registers its conferences to a *SIP* call server. Range: YES, NO Default: NO

Version 8.1.4.J - Changes to Existing Security Features

Table 2 *Changes to Existing Security Features*

#	Category	Feature Name	Description
1	Security	ULTRA_SECURE_MODE System Flag	From Version 8.1.4.J this *System Flag* is hidden. It was visible in all previous versions, up to and including Version 7.8. The flag must be manually added to the System Configuration before its value can be modified.

Table 2 *Changes to Existing Security Features*

#	Category	Feature Name	Description

2	Security	SIP TLS Encryption Key Length	*TLS* certificates can be generated using the following methods: *CSR*, *PFX* and *PEM*.
			Encryption Key length (bits):
			• SIP Signaling:
			  • *CSR* - 2048 (Generated by RMX)
			  • *PFX* / *PEM* - 1024 or 2048 (Generated by User)
			• Management / *LDAP*:
			  • *CSR* - 2048 (Generated by RMX)

3	Security	Additional Certificate Fields	• *Subject Alternative Name (SAN):* Allows the optional inclusion of *Domain Name* (of the *802.1X Authentication Server*), *FQDN, Short DNS,* or *IP Address* information during certificate creation.
			• *Hash Method*: Allows the selection of the output value for the *Secure Hash Algorithm.*
			  • SHA-256 the output value is 256 bits.
			  • SHA-1 the output value is 160 bits.

4	Security	Password Encryption - Migration from SHA-1 to SHA-256	Beginning with this version, SHA-256 (Secure Hash Algorithm) becomes mandatory for: • Application login passwords. • Linux operating system passwords • CSRs (Certificate Signing Requests)
5	Security	PKI	The PKI feature set has been enhanced and expanded to include: • Option to disable PKI in Ultra Secure Mode (Certificate Validation Option) • Online Certificate Status Protocol (OCSP) • PKI Self-signed Certificate
6	Security	SIP TCP Keep-Alive	The NAT Keep Alive method has been enhanced according to IETF RFC 5626 and RFC 6223.
7	Security	Media Encryption and Authentication	In compliance with UC_APL_SEC_0013, the RMX supports an additional Privacy Protocol the AES_CM_128_HMAC_SHA1_32, in addition to AES_CM_128_HMAC_SHA1_80
8	General	SNMP	SNMP enables managing and monitoring of the MCU status by external managing systems, such as HP OpenView or through web applications.

Version 8.1.4.J - New Features

Table 3 *New Features*

#	Category	Feature Name	Description
1.	Video	New Video Resolution 1080p 60	This version adds the option of *HD1080p* resolution at 60 fps for improved resolution of motion video.
2	Conferencing	Layout Overlays	*Layout Overlays* allow additional participant endpoints to be displayed in 1x1 conference *Video Layout*s.
3	Conferencing	Non-encrypted Conference Message	When mixing encrypted and non-encrypted endpoints in a conference using the "*Encrypt When Possible*" encryption option in the *Conference Profile* the encryption status of the conference can change as encrypted and non encrypted participants connect and disconnect.
4	Conferencing	Multiple Cascading Links	This version adds support for *Multiple Cascade Links* between RMXs hosting conferences that include *Immersive Telepresence Rooms* (*ITP*) such as Polycom's OTX and RPX Room Systems.
5	Conferencing	Speaker Change Threshold	The amount of time a participant must speak continuously until becoming the speaker is now configurable.
6	Conferencing	Exclusive Content Mode	*Exclusive Content Mode* allows the administrator to limit Content broadcasting to one participant, preventing other participants from interrupting the Content broadcasting while it is active.
7	Conferencing	FECC Control	FECC can be enabled and disabled for individual conferences in the Conference Profile.
8	Conferencing	Mute Participants Except Lecturer	All participants in the conference except for the lecturer can be automatically muted upon connection to the conference, preventing interruption of the lecture, accidentally or by participants with noisy connections.
9	Conferencing	Network Quality Indication	A *Network Quality Indicator* is displayed for each participant in the CP layout indicating the quality of the participants' video channels.
10	Conferencing	Content at HD1080p Resolution	Endpoints that support H.264 can now receive H.239 Content at the following resolutions: • HD720p at 30fps • HD1080p at 15fps
11	General	System Flag - SIP RTCP Flow Control	You can modify the *TMMBR* parameter (*Temporary Maximum Media Stream Bit Rate*) by adding the following flags: RTCP_FLOW_CONTROL_TMMBR_ENABLE Enables/disables the SIP RTCP flow control parameter. Default: YES RTCP_FLOW_CONTROL_TMMBR_INTERVAL *System Flag* and setting its value as required. Range: 5 - 999 (seconds) Default: 180

Table 3 *New Features (Continued)*

#	Category	Feature Name	Description
12	General	System Flag - SIP RTCP_FIR_ENABLE	RTCP_FIR_ENABLE When set to YES, the Full Intra Request (FIR) is sent as INFO (and not RTCP). Default = YES
13	General	Exporting and Importing Conference Templates	Conference Templates can be exported from one MCU and imported to multiple MCUs in your environment. Additionally, you can export Conference Templates and their associated Conference Profiles simultaneously.
14	General	Exporting and Importing Conference Profiles	Conference Profiles can be exported from one MCU and imported to multiple MCUs in your environment, enabling you to copy the Conference Profiles definitions to other systems.
15	General	Exporting and Importing System Configuration files	System Flags can be exported from one MCU and imported to multiple MCUs in your environment.
16	General	Managing Noisy Content	The system can identify participants who send frequent requests to refresh their content display, subsequently causing the content display of the conference to refresh and degrade the viewing quality. These participants are tagged as noisy content participants. The system can identify participants who send frequent requests to refresh their Content display, subsequently causing the Content display of the conference to refresh and degrade the viewing quality. These participants are tagged as Noisy Content participants. This process is controlled by the following system flags: • MAX_INTRA_REQUESTS_PER_INTERVAL_CONTENT • MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_CONTENT • CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS
17	General/IP	Direct IP dialing	For RMXs registered to a gatekeeper, the RMX 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.
18	Partners: Microsoft Certification	Lync 2013 Client Support	The RMX interoperability level with Lync 2013 is identical to Lync 2010. The following supported Lync 2010 feature set is supported with Lync 2013: • RTV • FEC support • ICE over TCP • Media over TCP • Network Error Recovery • SIP Dialog Recovery • Additional meeting room presence mode • Connecting an RMX meeting room to an AV-MCU conferences
19	Partners: POCN	Collaboration with Microsoft and Cisco	The *POCN* solution, enables *Polycom*, *Microsoft* and *Cisco* users, each within their own environment, to participate in the same conference running on an *RMX*.

Table 3 *New Features (Continued)*

#	Category	Feature Name	Description
20	Partners; Avaya, Redcom, NEC-Sphere	LSC Interoperability	Basic SIP proxy / server interoperability is supported for Local Session Controllers.
21	Network	NAT (Network Address Translation) Traversal	NAT Traversal is a set of techniques enabling participants behind firewalls to use *Session Border Controllers* (*SBC*) to connect to conferences, hosted on the RMX, remotely using the internet. This version includes support for an additional *Business to Business Connection*.
22	Network	BFCP Over UDP	• *BFCP* over *UDP* improves interoperability with *SIP Clients* that share *Content* using this protocol. • *AS SIP Content* is supported
23	Network	ICE - Multiple Network Services	One *Network Service* including *ICE* can be configured per media card installed in the *RMX*.
24	Management	Troubleshooting	If a *Browser Environment Error* occurs, the user is given the options of running the *Automatic Troubleshooting Utility* or performing the *Troubleshooting Procedures* manually.

Version 8.1.4.J - Changes to Existing Features

Table 4 *Changes to Existing Features (Continued)*

#	Category	Feature Name	Description
1	Conference	Address Book - Multi-level Address Book	The RMX *Address Book* can be organized into a multi-level hierarchical structure. It can be used to mirror the organizational layout of the enterprises and it is especially suitable for large-scale enterprises with a considerable number of conference participants, organizational departments, and divisions.
2	Conference	Address Book - Obtaining Display Name from the Address Book	The MCU can be configured to replace the name of the dial-in participant as defined in the endpoint (site name) with the name defined in the address book.
3	Conference	Interactive Video Forcing	Participants in ongoing conferences can be interactively forced to a Video Window in the conference layout by using Drag and Drop.
4	Conference	Participant Connection Status	The Participants list header displays real-time connection status information of Endpoints and Cascade Links in the selected conference.
5	Conferencing	Disconnect Last Invited Participant	A new *DTMF* code allows you to disconnect the last *Invited Participant*. The *DTMF* code is configurable: **#72** is recommended.
6	Conferencing	Customized Content Rate	*Customized Content Rate* is an additional *Content Setting* that allows manual definition of the *Conference Content Rate*.
7	General	System Flags - IVR	The following *System Flags* no longer require a system reset in order for flag changes to take effect: • IVR_MESSAGE_VOLUME • IVR_MUSIC_VOLUME • IVR_ROLL_CALL_VOLUME
8	General	Fast Configuration Wizard	Two additional dialog boxes in the *Fast Configuration Wizard* enable *RMX Time* and a new *Administrator User* (*Default User* replacement) to be defined. The two active alarms related to these system requirements are no longer displayed when setting up a new system. • *RMX Time* parameters are described in the *RMX Administration and Utilities* chapter section of the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide.* • *Default User* deletion and replacement are described an the end of the *Fast Configuration Wizard* section in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide.*
9	General	Active Alarms Reduction	Several of the *Active Alarms* have been moved to the *Faults List, reducing* the number of *Active Alarms* generated by the *RMX.*

Table 4 *Changes to Existing Features (Continued)*

#	Category	Feature Name	Description
10	General	Reduced Logger Messages	Process improvements have been made to the log file output and a reduction in the logger messages has been implemented. Messages have been reduced by condensing the number of messages, and log message texts have been revised.
11	General	Conference IVR Service	A new message type, *Blip on Cascade Link*, was added to the *Conference IVR Service - General* dialog box. The message/tone *.wav file assigned to this message type is played when the link to the cascaded conference is connected successfully.
12	General	RMX Support for Microsoft Lync 2013 Clients	The RMX interoperability level with Lync 2013 is the same as the interoperability level with Lync 2010.
13	General	Packet Loss Compensation (LPR and DBA)	The LPR (Lost Packet Recovery) check box in the New Profile - Advanced and Profile Properties - Advanced dialog boxes has been renamed Packet Loss Compensation (LPR and DBA).
14	General	Cascading Conferences	The RMX can be defined as Master on Level 1 and the MGC can be defined as Slave in levels 2 and 3.
15	General	CDR Changes: - Multi-part CDR - Event 34 - Additional Columns - Unformatted files	By default, the maximum CDR (Call Data Record) file size is limited to 1MB. When a CDR file reaches a size of 1MB the file is saved and further call data recording is stopped and the additional data is lost. The RMX can be configured to keep recording the data in multiple CDR file set of 1MB each. Multi-Part CDR ensures that conference call data from long duration or permanent conferences is recorded and not lost. A new event (34) was added to the CDR file. It includes information of the maximum line rate, maximum resolution and maximum frame rate used by H.323 or SIP participant during the conference. In the CDR List, two new fields have been added: • *GMT Start Time* • *File Retrieved* In unformatted CDR files the *GMT Offset* and *GMT Offset Sign* fields are now supported.
16	General	User Authorization Level	A new User *Authorization Level*, *Administrator - Read Only*, has been added to this version.
17	General	RMX 1500Q Video/Voice Port Configuration (Slider) Change	On the RMX 1500Q, when a video license of 25 ports is purchased, the Video/Voice Port Configuration (Slider) uses a different formula based on the license information to calculate the conversion ratio between audio and video ports.
18	Network	Gateway Redial	Additional *Redial* options and *IVR* messages have been included for *Gateway Calls* to numbers that are wrong, adding functionality to the *RMX's Gateway* capabilities when used in conjunction with communication servers (*H.323, SIP, ISDN*) such as *Polycom's CMA* and *DMA*.
19	Network	SIP Digest	SIP digest now supports the following methods: • SERVICE - for edge server credentials and for publishing presence. • REFER - in call transfer.

Table 4 *Changes to Existing Features (Continued)*

#	Category	Feature Name	Description
20	Network	SIP Registration	*RMX*'s registering to *SIP* servers, when *SIP* registration is not enabled in the conference profile, will each register with an *URL* derived from its own signaling address. This unique *URL* replaces the non-unique *URL*, dummy_tester, used by all *RMX*s in previous versions.
21	Network	Changes to the Management Network dialog box	The *Secured Communications* check box has been moved to the *Management Network - Security* tab from the *Management Network - IP* tab. In the M*anagement Network - Security* dialog box, the *Request Peer Certificate* check box has been renamed to *Skip certificate validation for user logging session*.
22	Network	New Euro ISDN Switch type	A new T1 Switch Type has been added: EURO ISDN for Taiwan.
23	Network	Set Default ISDN/ PSTN Network	In the *ISDN/PSTN Network Services* pane, the *Set Default ISDN/ PSTN Network Services* icon has been changed to the following: 
24	Network	Default flag value: LAN_REDUNDANCY	The default value of the **LAN_REDUNDANCY** *System Flag* has been changed to **NO**. If the flag value is set to **YES** and either of the LAN connections (LAN1 or LAN2) experiences a problem, an active alarm is raised stating that there is no LAN connection, specifying both the card and port number.
25	Partners	IBM	For *IBM SameTime Unified Telephony Lite* (*SUT*) clients, *RTCP-FB* replaces the use of *SIP INFO* messages when the *RMX* issues an *INTRA* request or other flow control commands to change the video rate.
26	Partners	Microsoft	Registration with Presence has increased up to 100 conferencing entities to a single SIP Server.
27	RMX Manager	Add MCU Dialog Box	Auto Reconnection options have been added to the Add MCU dialog box.
28	System Configuration	New flag for KeepAlive Requests interval	The flag **CPU_TCP_KEEP_INTERVAL_SECONDS** was added to the system configuration. This flag indicates the interval in seconds between the KeepAlive requests. Default value: **75** seconds. Range: 10-720 seconds.
29	System Configuration	New flag for clock drift	The flag **MUX_DATA_FLUSHING_FREQUENCY** was added to the system configuration. This flag indicates the number of additional data flushes to be performed. Default value: 2 Range: 0-6 This is for use when the RMX has a clock drift from external ISDN clock source (ISDN switch). The threshold for the drift is 20 milliseconds per 30 second interval. If clock drift is detected, depending on the flag value, the RMX performs additional data flushes to the external MUX in each 30 second interval in order to avoid losing synchronization, avoiding disconnection, video freezes or breaks in audio.

Table 4 *Changes to Existing Features (Continued)*

#	Category	Feature Name	Description
30	System Configuration	New flag for KeepAlive Request	The flag **CPU_TCP_KEEP_ALIVE_TIME_SECONDS** was added to the system configuration. This flag indicates when to send the first KeepAlive indication to check the TCP connection. Default value: **7200** seconds (120 minutes) Range: 600-18000 seconds When there are NAT problems, this default may 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.
31	System Configuration	Flag Name Change	The **MAX_CONF_PASSWORD_REPEATED_CHAR** *System Flag* has been renamed to **MAX_CONF_PASSWORD_REPEATED_DIGITS**
32	Video	Video Preview	H.264 High Profile is supported with Video Preview.
33	Video	Content - Legacy Endpoints	The *Send Content to Legacy Endpoints* check box has been moved to the *Profiles - Video Quality* tab from the *Profiles - Video Settings* tab.

Version 8.1.4.J - Interoperability

Devices

The following table lists the devices with which Version 8.1.4.J was tested.

Table 2-1 *Version 7.7 Device Interoperability Table*

Device	Version
Gatekeepers/Proxies	
Polycom Netgear WGR614 (VBP AP and H460)	V11.2.x
Polycom VBP5300 E/ST	V11.2.x
Polycom CMA	6.2.0.ER22
Polycom RealPresence Resource Manager (XMA)	7.3.0,7.1.1
Polycom PathNavigator	
Polycom SE200	
Polycom RMX Gateway	8.1.6
Cisco (Tandberg) VCS	X7.2.2
Cisco (Tandberg) Gatekeeper	N6.1
Cisco (Tandberg) Gateway	G3.2
Cisco 3241 Gateway	2.1(1.43)p
Cisco 3745 Gatekeeper	
Radvision ECS gatekeeper	7.1.2.12
Radvision Scopia P10 Gateway	5.7.2.0.25
Microsoft OCS Server	
Microsoft Lync Server	4.0.7577.183 (CU5version)
Microsoft Lync Server W15	Lync Server 2013- 5.0.8308.0
Broadsoft Proxy	R18SP1
Vidyo GW	
RPAD	2.1
Recorder	
Polycom RSS 2000	8.5
Polycom RSS 4000	8.5

Table 2-1 *Version 7.7 Device Interoperability Table (Continued)*

Device	Version
MCUs, Call Managers Network Devices and Add ins	
Polycom MGC 25/50/100 and MGC+50/100	9.0.4.3
Polycom RMX 1000	2.1.2
Polycom DMA 7000	6.0.2
LifeSize MCU	
BlueJeans MCU	
Radvision Scopia Elite	
Avaya Communication MGR	R016x.02.0.823.0 Patch 20199
Avaya Aura Session Manager	V6.3.0.0.630039
Avaya Aura Communication Manager as Evolution Server	R016x.02.0.823.0 Patch 20199
Cisco Call Manager	9.0/9.1
Cisco (Tandberg) Codian 4505 MCU	4.4(3.49)
Cisco Telepresence Server	
IBM WebSphere Application Server	7.0.0.15 (Network Deployment) plus required WebSphere iFixes.
Siemens Server	V7.00.01.ALL.07_PS0010.E11
Acme Packets SBC	SBC ACME Net-Net 3820 Firmware SCX6.2.0 MR-8 Patch 4 (Build 1005)
Endpoints	
Polycom HDX Family	3.1.1.3, 3.1.2
Polycom GS Family	4.1.1
Polycom Telepresence (ITP) Systems	3.1.1.3, 3.1.2
Polycom VSX and V-Series Family	9.0.6.2
Polycom Viewstation Family	7.5.4 or higher
Polycom Viewstation FX/EX/4000	6.0.5 or higher
Polycom CMA Desktop	5.2.4
Polycom CMA Desktop for MAC	5.2.4
Polycom QDX6000	4.0.3
Polycom Real Presence Desktop	3
Polycom RealPresence Mobile iPad	3

Table 2-1 *Version 7.7 Device Interoperability Table (Continued)*

Device	Version
Polycom RealPresence Mobile Android	3
Polycom m100	1.0.5
Polycom VVX1500	4.0.4
Polycom VVX500	4.1.3
Polycom VVX600	4.1.3
Polycom PVX	8.0.16
Polycom iPower 9000	6.2.x
Polycom Sound Point 601 SIP	3.1.7
Polycom SoundPoint 650 SIP	4.0.3
Polycom SoundStation IP4000 SIP	3.1.7
Polycom SoundStation IP7000	4.0.3
Polycom HDX Touch Controller	1.7
Avaya IP Softphone	
Avaya one-X Communicator	v6.1.8.06-SP8-40314
Avaya 1000 series endpoint	v4_8_3_24
Avaya Desktop Video endpoint	v 1.1.2.020002
LifeSize Desktop client	2.0.2.191
LifeSize Express 220	4.11.13
LifeSize Passport	4.11.13
LifeSize Room	4.7.22
LifeSize Team 200	4.7.22
LifeSize Team 220	4.11.13
Cisco (Tandberg) 150 MXP	L6.1
Cisco (Tandberg) 1700 MXP	F9.3.1
Cisco (Tandberg) 6000 MXP	F9.3.1
Cisco (Tandberg) Edge95 MXP	F9.3.1
Cisco (Tandberg) 6000 B	B10.3
Cisco (Tandberg) 6000 E	E5.3
Cisco C20	6.0.1, 6.1.1
Cisco C90	6.0.1, 6.1.1
Cisco C60	5.1

Table 2-1 *Version 7.7 Device Interoperability Table (Continued)*

Device	Version
Cisco E20	4.1.2
Cisco EX90	6.0.1, 6.1.1
Cisco SX20	6.0.1, 6.1.1
Cisco CTS3010 (Telepresence)	1.9.3/1.10.1
Cisco CTS1300 (Telepresence)	1.8.1/1.9.3
Cisco CTS500 (Telepresence)	1.8.1
Radvision Scopia XT1000	2.5.416
Radvision Scopia XT5000	3.1.1.37
Aethra X7	12.1.7
Sony PCS –1	3.42
Sony PCS –G50	2.72
Sony PCS –TL50	2.42
Sony PCS-G90	2.22
Sony PCS-XG80	2.36
CSS Server	1.1.0.504
Addon client	1.1.0.37260
Microsoft OC client R2	
Microsoft Lync 15 client	15.0.4420.1017
Microsoft Lync 14 client	4.0.7577.4356
Siemens Client	V7R0.0.6
Siemens OpenStage Desktop Voice	V3_R1_31_0
IBM DB2 Database Server	9.7
IBM Lotus Domino® Enterprise Server	V8.5.2
IBM Lotus Notes client	V8.5.2
IBM Lotus Sametime Media Manager	V8.5.2 IFR 1
IBM Lotus Sametime System Console	V8.5.2 IFR 1
IBM Lotus Sametime Community Server	V8.5.2 IFR 1
IBM Lotus Sametime Proxy Server	V8.5.2 IFR 1
IBM Lotus Sametime Meeting Server	V8.5.2 IFR 1

For more information about partner product interoperability, refer to the partner deployment guides.

Polycom RMX and Avaya Interoperability

For questions and support on the Polycom - Avaya integrated solution, please contact your Avaya Authorized Service Provider.

Polycom RMX 4000, RMX 2000 and RMX 1500 can call and receive calls with current generally available versions of Avaya one-X Communicator H.323 video soft clients (R5.2) on Aura Communication Manager R5.2.1, R6.0, and R6.1.

RMX Web Client

The following table lists the environments (Web Browsers and Operating Systems) with which the *RMX Web Client* was tested.

Table 3 *Version 7.0 Environment Interoperability Table*

Web Browser	Operating System
Internet Explorer 7	Windows XP™
	Windows Vista™
Internet Explorer 8	Windows 7, Windows 8
Internet Explorer 9	

For single core cpu workstations: It is not recommended to run *RMX Web Client* and *Polycom CMAD* applications simultaneously on the same workstation.

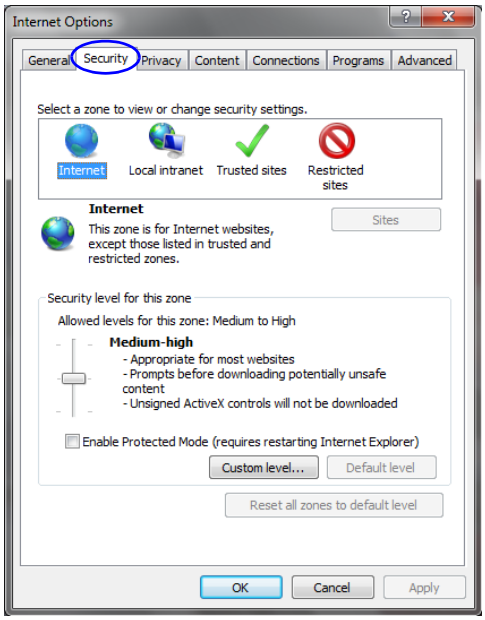
Windows 7™ Security Settings

If *Windows 7* is installed on the workstation, *Protected Mode* must be disabled before downloading the software to the workstation.

To disable Protected Mode:

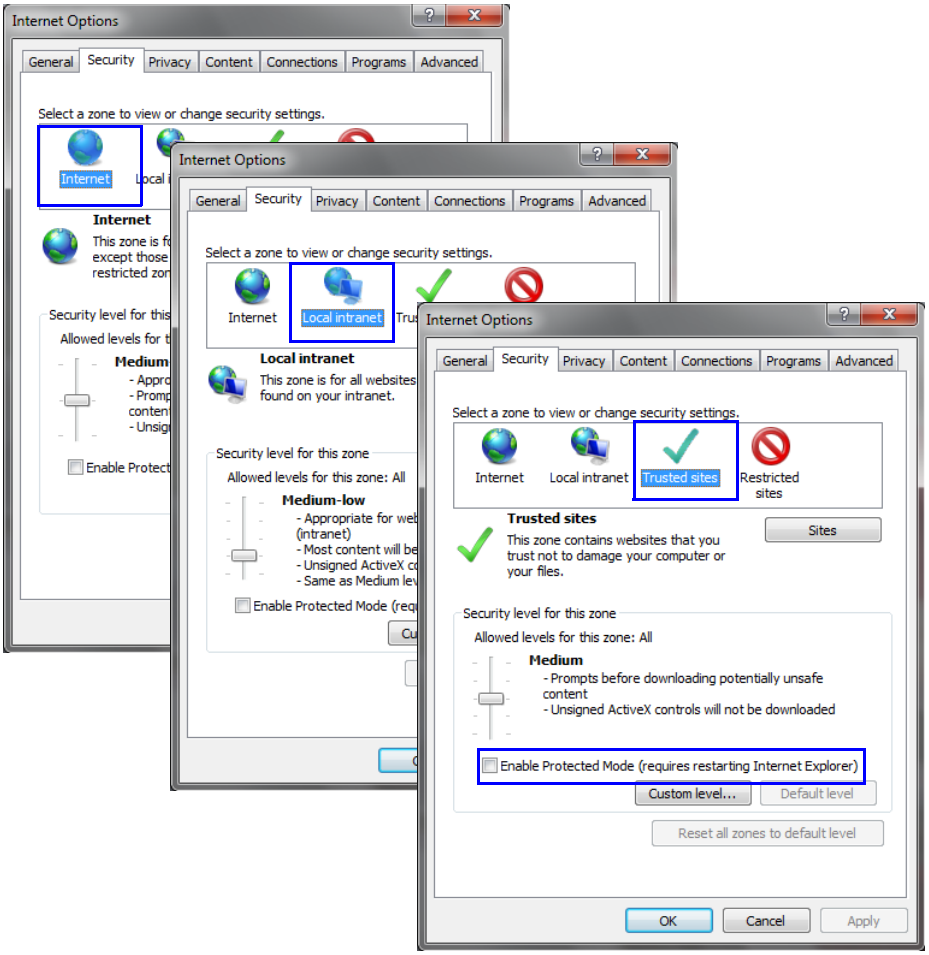
1 In the *Internet Options* dialog box, click the **Security** tab.

The **Security** tab is displayed.



2 Clear the *Enable Protected Mode* check box for each of the following tabs:

— *Internet*
— *Local intranet*
— *Trusted sites*



3 After successful connection to RMX, the *Enable Protected Mode* check boxes can be selected to enable *Protected Mode* for the following tabs:

— *Internet*
— *Local intranet*

Internet Explorer 8 Configuration

When using *Internet Explorer 8* to run the *RP Collaboration Server Web Client* or *RMX Manager* applications, it is important to configure the browser according to the following procedure.

To configure Internet Explorer 8:

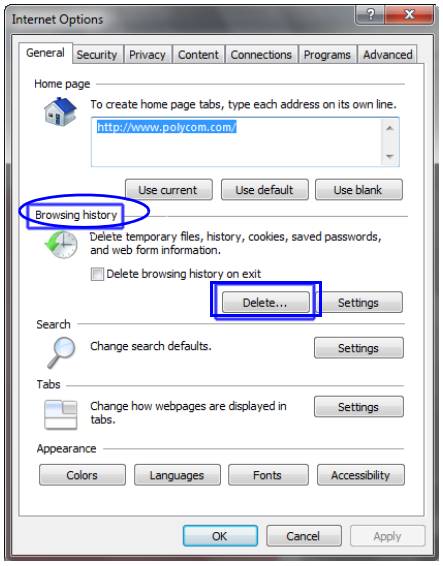
1 Close **all** browsers running on the workstation.

2 Use the *Windows Task Manager* to verify that no *iexplore.exe* processes are running on the workstation. If any processes are found, use the **End Task** button to end them.

3 Open *Internet Explorer* but do **not** connect to the MCU.

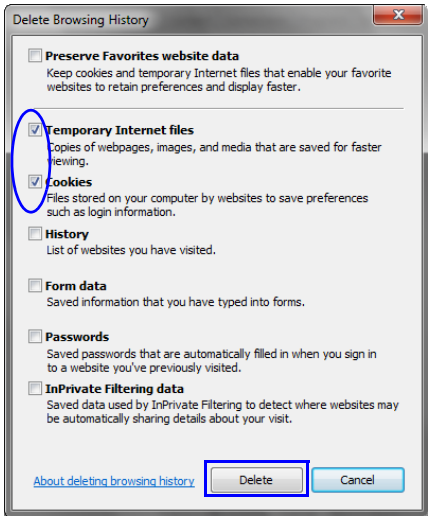
4 In the *Internet Explorer* menu bar select **Tools >> Internet Options**.

The *Internet Options* dialog box is displayed with *General* tab open.



5 In the *Browsing history* section, click the **Delete** button.

The *Delete Browsing History* dialog box is displayed.



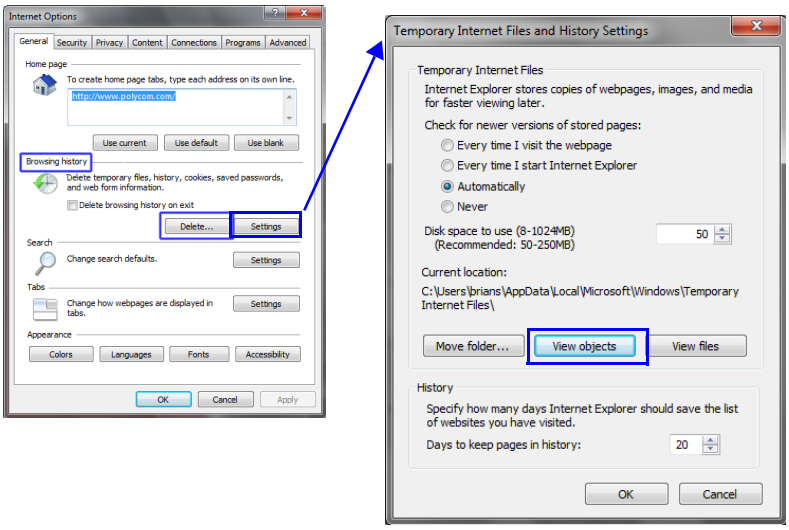
6 Select the **Temporary Internet** files and **Cookies** check boxes.

7 Click the **Delete** button.

8 The *Delete Browsing History* dialog box closes and the files are deleted.

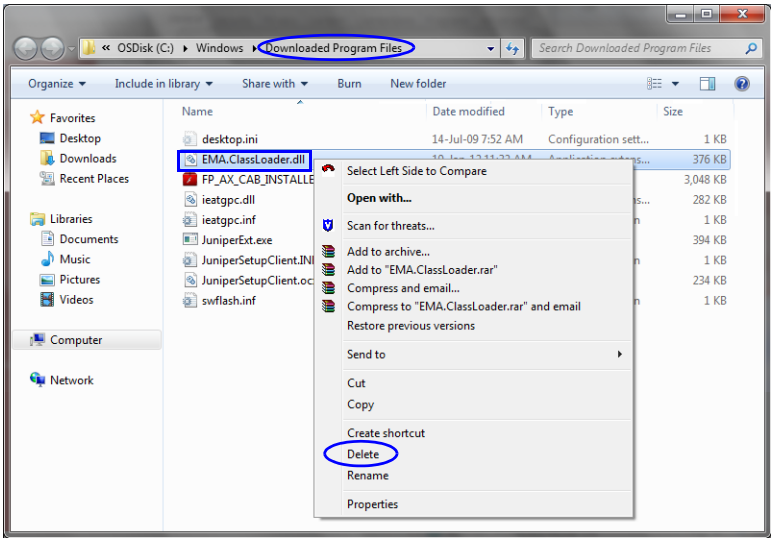
9 In the *Internet Options* dialog box, click the **Settings** button.

The *Temporary Internet Files and History Settings* dialog box is displayed.



10 Click the **View objects** button.

The *Downloaded Program Files* folder containing the installed *Program Files* is displayed.



11 Select the **EMAClassLoader.dll** file and press the **Delete** key on the workstation or right-click the *EMA.ClassLoader.dll* file and then click **Delete**.

12 Close the *Downloaded Program Files* folder and the *Temporary Internet Files and History Settings* dialog box.

13 In the *Internet Options* dialog box, click the **OK** button to save the changes and close the dialog box.

Polycom Solution Support

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

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Version 8.1.4.J - Upgrade Package Contents

The Version 8.1.4.J upgrade package must be downloaded from the Polycom Resource Center and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Manager installation files
- RMX Documentation
  - RealPresence Collaboration Server (RMX) 1500/2000/4000 Version 8.1.4.J Release Notes
  - RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments
  - RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide
  - RealPresence Collaboration Server (RMX) 1500/2000/4000 Hardware Guides
  - RealPresence Collaboration Server (RMX) 1500/2000/4000 Quick Installation Booklets
  - Installation Quick Start Guide for RMX 1500/2000/4000
  - RMX Third Party Licenses
- External DB Tools
  - RMX 1500/2000/4000 External Database API Programmer's Guide
  - Sample Scripts
- RMX XML API Kit Version 8.1
  - RMX 1500/2000/4000 XML API Version 8.1.0 Release Notes
  - RMX 1500/2000/4000 XML API Overview
  - RMX 1500/2000/4000 XML API Schema Reference Guide
  - MGC to RMX XML API Conferencing Comparison
  - Polycom XML Tracer User's Guide
  - XML Schemas
  - Polycom XML Tracer application

Where to Get the Latest Product Information

To view the latest Polycom product documentation, visit the **Support** section of the Polycom website at http://support.polycom.com

Upgrade Procedures

Version 8.1.4.J does not support MPM+ cards.

Only MPMx cards are supported.

DO NOT upgrade to Version 8.1.4.J if *MPM+* cards are installed in the RealPresence Collaboration Server (RMX) system.

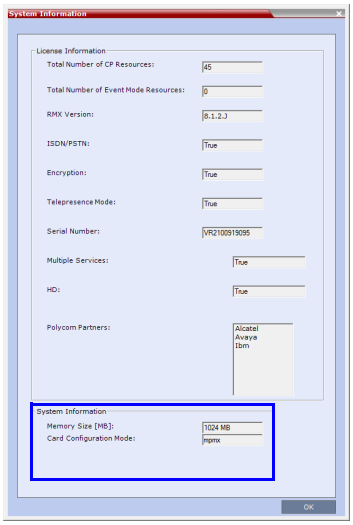
Contact *Polycom Support* for more information.

If the upgrade process includes upgrading the *Media* cards, refer to the *RealPresence Collaboration Server 2000/4000 MPMx Migration Procedure* documentation.

Guidelines

- Ensure that the *Control Unit* memory size is at least 1024MB. If memory size is 512MB, **DO NOT** perform the upgrade procedure. Contact *Polycom Support* for more information.

  To check the MCU's Memory size: In the RMX Web Client/RMX Manager go to **Administration > System Information.**



- If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *RealPresence Collaboration Server* software to the workstation. For more information see "*Windows 7™ Security Settings*" on page **2-15**.
- To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each *LAN* connection.
- If the default **POLYCOM** user is defined in the *RMX Web Client*, an *Active Alarm* is created and the *MCU* status changes to **MAJOR** until a new Administrator user is created and the default user is deleted.

- When upgrading from a version in which the *Profiles* dialog box did not include the *Gathering Phase* option: To enable the *Gathering Phase* in the existing *Profiles*, you must modify the *Profiles* assigned to these conferencing entities. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide for Maximum Security Environments*, "*Gathering Settings*".
- When upgrading from a version in which the *Profiles* dialog box did not include the *SIP Registration* option: To keep the conferencing entities registered with the *SIP Server* defined in the *IP Network Service*, registration must be enabled in the *Profiles* assigned to these conferencing entities. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide for Maximum Security Environments*, "*Media Encryption*".
- SHA-256 (Secure Hash Algorithm) Password Encryption - When upgrading to *Version 8.1.4.J*, user passwords will be hashed with *SHA-256* on *Login* and *SHA-1* hashed *Login* passwords will be deleted. New passwords are stored in SHA-256 format.

  The RMX configuration, including users and passwords, should be backed up before upgrading or downgrading. Table 2-10 summarizes the system behavior with regard to passwords and certificates when upgrading to or downgrading from this version.

Table 2-1 *Version Change - Password and Certificate Compatibility*

Version Change	Behavior	
	Passwords	**Certificates**
Upgrade from old version to new version	On user login: • All **new**-**user** passwords are hashed and saved using *SHA-256*. • **Existing** user passwords remain saved using the SHA-1 signature, however: • On first login after the upgrade the *SHA-1* hashed password is automatically replaced with *SHA-256* hashed password. **Note:** After an upgrade to version *8.1.4.J* there will be still passwords saved with the *SHA-1* signature. In order not to rely on automatic password signature conversion and replacement, and to ensure that the system only has *SHA-256* hashed passwords saved, the administrator should: Either: • Ensure that all the users login to the system at least once to ensure automatic replacement of *SHA-1* hashed passwords with *SHA-256* hashed passwords. Or: • Delete and recreate all users.	The new version accepts certificates issued with *SHA-1* hashing.

Table 2-1 Version Change - Password and Certificate Compatibility (Continued)

Version Change	Behavior	
	Passwords	**Certificates**

Downgrade *from new version to old version*	Before the downgrade procedure begins, the administrator receives a popup warning message "Passwords will change to factory default would you like to proceed?"
	All users *and SHA-256* hashed passwords are deleted.
	The administrator's *User Name* and *Password* reverts to the *Factory Default:* POLYCOM / POLYCOM.
		The old version accepts certificates issued with *SHA-1* hashing.
		
		For certificates issued with *SHA-256* hashing:
		• The administrator receives a popup warning message "TLS certificate will be deleted and the system will switch to non-secured connection, would you like to proceed?"
		• For each certificate that is hashed with SHA-256:
		  • *RMX Web Client / RMX Manager* connections to the RMX are switched to non-secured mode.
		  • LDAP services are changed from 636 to port 389.
		  • *SIP TLS* sessions are changed to *SIP UDP*.
		  • The certificate is deleted.

Although *SVC Conferencing Mode* options are available in *Conference Profiles*, it is advised that they not be used with *Version 8.1.4.J*.

Upgrade Paths to Version 8.1.4.J

The upgrade options from previous versions to Version 8.1.4.J are summarized in Table 2-2.

Table 2-2 Upgrade Paths to Version 8.1.4.J

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		New Version	
	Version	**Key**	**Version**	**Key**	**Version**	**Key**
7.5.1.J / 7.5.2.J	N/A		N/A		**8.1.4.J**	Yes
7.5.0.J	N/A		N/A		7.5.1.J	No
7.0.2	N/A		N/A		7.5.0.J	Yes
5.0.2	7.0.2	Yes	N/A		7.5.0.J	Yes

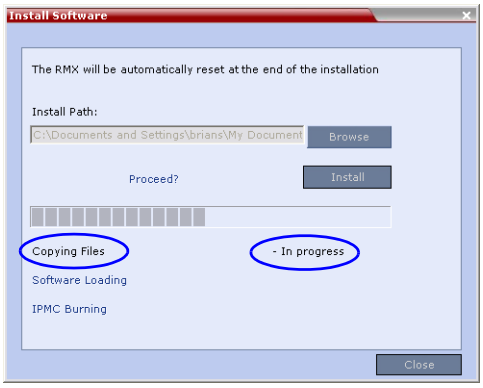
Table 2-2 Upgrade Paths to Version 8.1.4.J

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		New Version	
	Version	Key	Version	Key	Version	Key
5.1	5.0.2	Yes	7.0.2	Yes	7.5.0.J	Yes

Upgrading from Version 7.5.1.J / 7.5.2.J to Version 8.1.4.J.

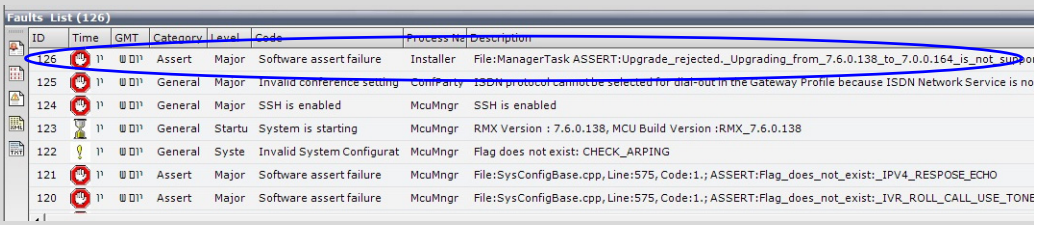
1. Download the Version 8.1.4.J software from the *Polycom Resource Center* web site.
2. Obtain the Version 8.1.4.J *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RealPresence Collaboration Server (RMX)1500/2000/4000 Deployment Guide for Maximum Security Environments*, "*Obtain Product Activation Key for the RMX*" on page **1-25**.
3. Backup the configuration file. For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide for Maximum Security Environments*, "*Software Management*".
4. Install *MCU* Software *Version 8.1.4.J*.
   On the *RMX* menu, click **Administration> Software Management > Software Download**.
5. Browse to the *Install Path,* selecting the **Version 8.1.4.J.x.x.bin** file in the folder where *Version 8.1.4.J* is saved and click **Install**.

The *Install Software* information box that the file *Copying files* is *In progress*.



- When an incorrect or non viable version upgrade/downgrade is attempted, an alarm and fault are activated on the RMX.

Click **OK**. The RMX software installation procedure is aborted and a system alert activates in the Faults List as shown below.



- During any upgrade or downgrade software version installation when the *Safe Software Version Installation* warning has been activated your current browser session will block any new installation attempt. As a workaround close and then re-open a new browser session, which will enable you to start a new software version installation.

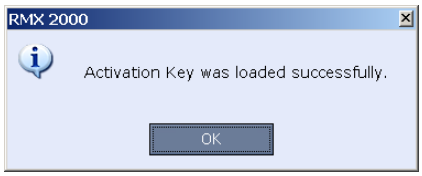
At the end of the *Coping Files* process the system displays an indication that the software copying procedure is *Done* and a new *Activation Key* is required.

6 Click the **OK** button.

The *Product Activation* dialog box is displayed with the serial number field completed.

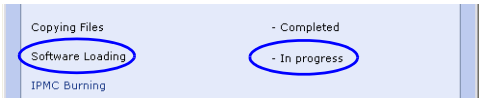
7 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

At the end of the *Product Activation* process the system displays an indication that the *Product Activation Key* was successfully installed.

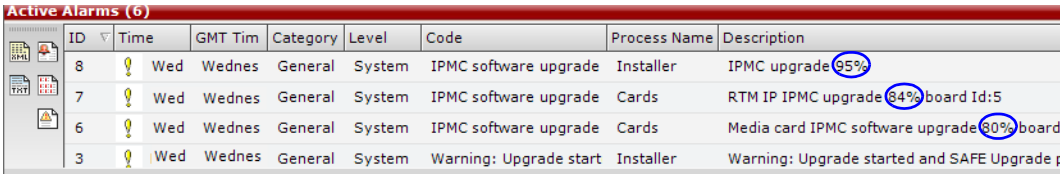


8 Click the **OK** button.

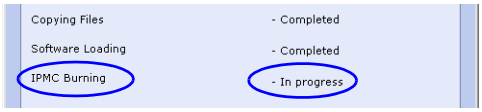
The *Install Software* information box indicates that *Software Loading* is in progress.



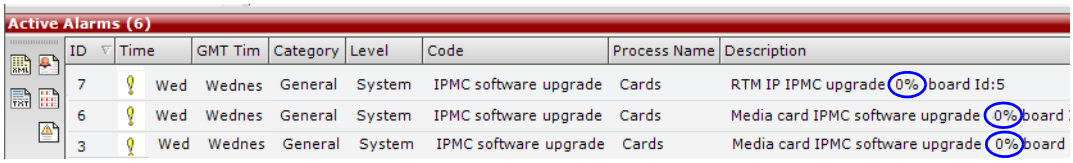
A series of *Active Alarms* are displayed indicating the progress of the upgrade process.



The *Install Software* information box indicates that *IPMC Burning* is in progress.

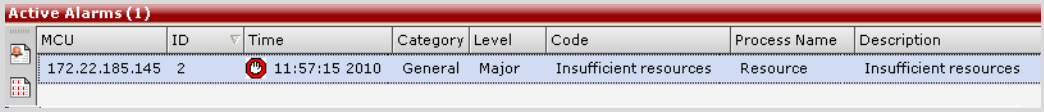


A further series of *Active Alarms* are displayed indicating the progress of the upgrade process.



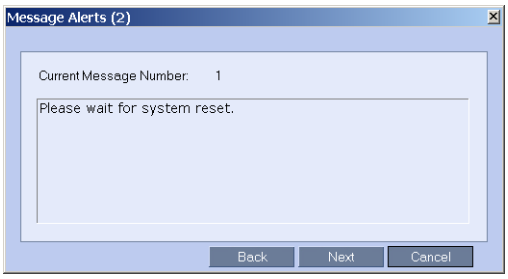
The upgrade procedure takes approximately **20** minutes.

Sometimes, when updating the *Version 8.1.4.J* license key, the system displays the following active alarm:



Ignore this Active Alarm and complete this installation procedure.

A system message alert may appear, if so then click **Next/Cancel**.



Connection to the *RealPresence Collaboration Server* is terminated and you are prompted to reopen the browser.

9 Approximately 10 minutes after receiving this message, close and reopen the browser.

10 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RealPresence Collaboration Server*.

If the browser displays a message indicating that it cannot display the requested page, close and reopen the browser and connect to the RealPresence Collaboration Server.

The version number in the *Welcome* screen has changed to *8.1.4.J*.

11 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

If the error "Browser environment error. Please close all the browser sessions" appears, close all the browser sessions, and reconnect to the RealPresence Collaboration Server. If the error message appears again, either run the automatic troubleshooter utility or manually preform the suggested troubleshooting procedures. For more details, see the *RealPresence Collaboration Server (RMX)1500/2000/4000 Deployment Guide for Maximum Security Environments "Troubleshooting"* on page A-1.

In the *Main Screen* an *MCU State* indicator displays a progress indicator 

showing the time remaining until the system start-up is complete.

To use the new features such as *Operator Assistance* and *Gateway Sessions* the IVR Services must be updated. For more details, see *"Additional/Optional System Updates After Upgrading"* on page 36.

The upgrade to Version 8.1.4.J is complete.

Upgrading from Version 7.5.0.J to Version 7.5.1.J.

1 Download the required software *Version 7.5.1.J* from the *Polycom Resource Center* web site.

2 Optional. If the system has *Entry Queues* and *Meeting Rooms* defined that are protected by *Conference* or *Chairperson Passwords*, in *Ultra Secure Mode*, that are less than 9 characters in length, increase these passwords to a length of at least 9 characters before continuing with the upgrade to *Version 7.5.1.J*.

3 Backup the configuration file. For more information, see the *RealPresence Collaboration Server 1500/2000/4000 Administrator's Guide for Maximum Security Environments, "Software Management"* on page **17-71**.

4 Install *MCU* Software *Version 7.5.1.J*
On the *RMX* menu, click **Administration> Software Management > Software Download**.

5 Browse to the *Install Path,* selecting the **Version 7.5.1x.bin** file in the folder where *Version 7.5.1.J* is saved and click **Install**.

— The installation begins.

At the end of the installation process the system displays an indication that the software was successfully downloaded.

— The upgrade procedure begins.

The upgrade takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RealPresence Collaboration Server resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*

6 After about **30** minutes, **close and reopen the browser** and connect to the RealPresence Collaboration Server.
If the browser was not closed and reopened, the following error message is displayed: *Browser environment error. Please reopen the browser.*

7 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator 

showing the time remaining until the system start-up is complete.

Upgrading from Version 7.0.2 to Version 7.5.0.J

1 Download the *Version 7.5.0.J* software from the *Polycom Resource Center* web site.

If *Windows7*™ is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 7.5.0.J* software to the workstation.
For more information see "*Windows 7™ Security Settings"* on page **15**.

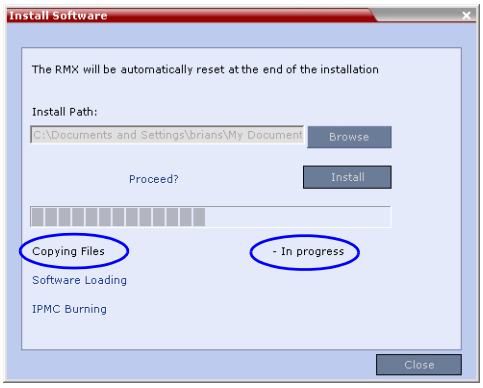
2 Obtain the Version 7.5.0.J *Product Activation Key* from the *Polycom Resource Center* web site.

3 Backup the configuration file.

4 Install *MCU* Software *Version 7.5.0.J.*
On the *RMX* menu, click **Administration> Software Management > Software Download**.

5 *Browse* to the *Install Path,* selecting the **Version 7.5.0.J.x.x.bin** file in the folder where *Version 7.5.0.J* is saved and click **Install**.

The *Install Software* information box that the file *Copying files* is *In progress*.

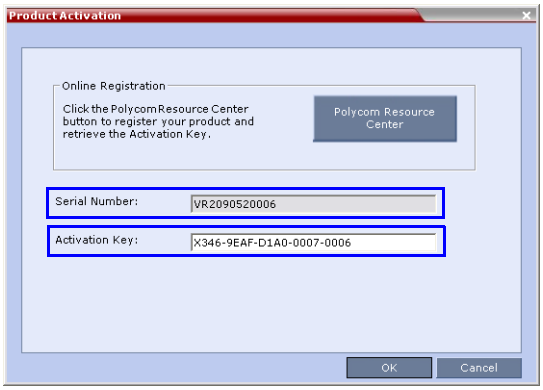


At the end of the installation process the system displays an indication that the software copying procedure is *Completed* and that a new *Activation Key* is required.

6 Click the **OK** button.

7 On the *RMX* menu, click **Setup > Product Activation**.

The *Product Activation* dialog box is displayed with the serial number field completed.

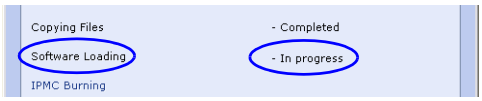


8 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

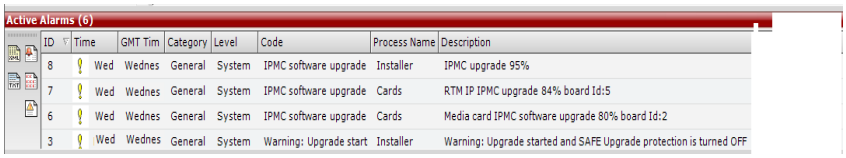
At the end of the *Product Activation* process the system displays an indication that the *Product Activation Key* was successfully installed.

9 Click the **OK** button.

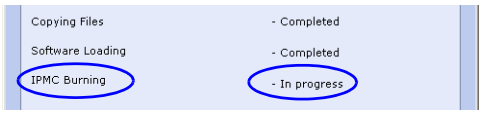
The *Install Software* information box indicates that *Software Loading* is in progress.



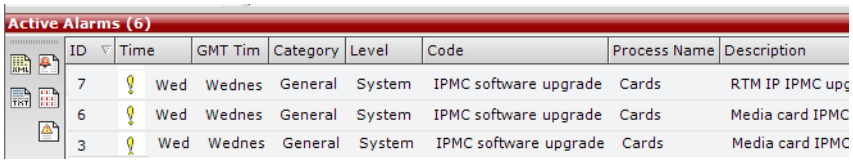
A series of *Active Alarms* are displayed indicating the progress of the upgrade process.



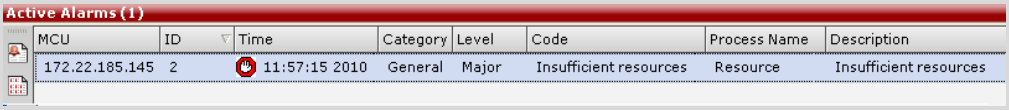
The *Install Software* information box indicates that *IPMC Burning* is in progress.



A further series of *Active Alarms* are displayed indicating the progress of the upgrade process.



Sometimes, when updating the *Version 7.x* license key, the system displays the following active alarm:



Ignore this Active Alarm and complete this installation procedure.

The upgrade procedure takes approximately **20** minutes.

Connection to the *RealPresence Collaboration Server* is terminated and you are prompted to reopen the browser.

10 Approximately 5 minutes after receiving this message, close and reopen the browser.

11 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RealPresence Collaboration Server*.

If the browser displays a message indicating that it cannot display the requested page, close and reopen the browser and connect to the RMX.

12 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator 

showing the time remaining until the system start-up is complete.

- If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.
- If the upgrade process fails, please contact Polycom support.

To use the new features such as *Operator Assistance* and *Gateway Sessions* the *IVR Services* must be updated.

Upgrading from Version 5.0.2 to Version 7.5.0.J

This upgrade requires an intermediate upgrade from *Version 5.0.2* to *Version 7.0.2* followed by an upgrade to *Version 7.5.0.J*.

Intermediate Upgrade from Version 5.0.2 to Version 7.0.2

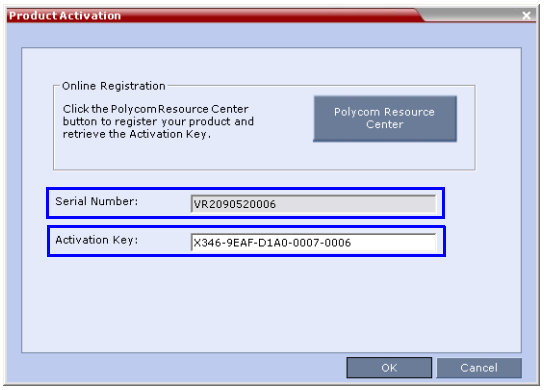
1. Download the software Version 7.0.2 software from the *Polycom Resource Center* web site.

If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 7.0.2* software to the workstation.
For more information see "*Windows 7™ Security Settings"* on page **15**.

2. Obtain the Version 7.0.2 *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RealPresence Collaboration Server (RMX)1500/2000/4000 Deployment Guide for Maximum Security Environments*, *"Download and Install the RMX Manager Onto a Workstation"* on page **1-25**.
3. Backup the configuration file. For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide for Maximum Security Environments, "Software Management"*.
4. Install *MCU* Software Version 7.0.2.
   On the *RMX* menu, click **Administration > Software Management > Software Download**.
5. *Browse* to the *Install Path,* selecting the **Version 7.0.2xx.bin** file in the folder where **Version 7.0.2**. is saved and click **Install**.

   At the end of the installation process the *Install Software* dialog box indicates that the installed software is being checked. The system then displays an indication that the software was successfully downloaded and that a new activation key is required.
6. On the *RMX* menu, click **Setup > Product Activation**.

The *Product Activation* dialog box is displayed with the serial number field completed.



7 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

At the end of the *Product Activation* process the system displays an indication that the *Product Activation Key* was successfully installed.

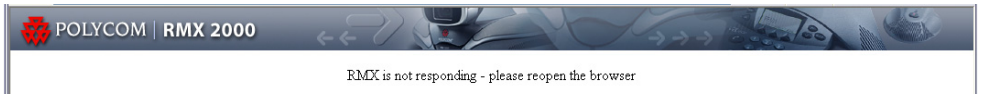
8 When prompted whether to reset the *RealPresence Collaboration Server*, click **Yes** to reset the *RealPresence Collaboration Server*.

Sometimes when upgrading from version 5.0.2 to version 7.0.x the reset process fails. In such a case, you can try to connect to the *MCU* via the Shelf Management and reset the *MCU* from the Hardware Monitor or you can "hard" reset the *MCU* by turning the Power off and on again.

9 When prompted to wait while the *RealPresence Collaboration Server* resets, click **OK**.

The upgrade procedure takes approximately 30 minutes.

Connection to the *RealPresence Collaboration Server* is terminated and you are prompted to reopen the browser.



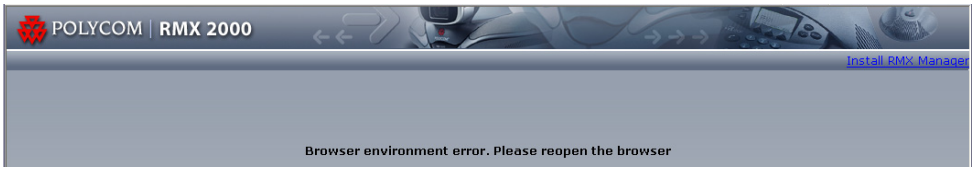
10 After approximately 30 minutes close and reopen the browser.

11 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RealPresence Collaboration Server*.

The browser displays a message indicating that it cannot display the requested page.

12 Refresh the browser periodically until connection to the *RealPresence Collaboration Server* is established and the *Login* screen is displayed.

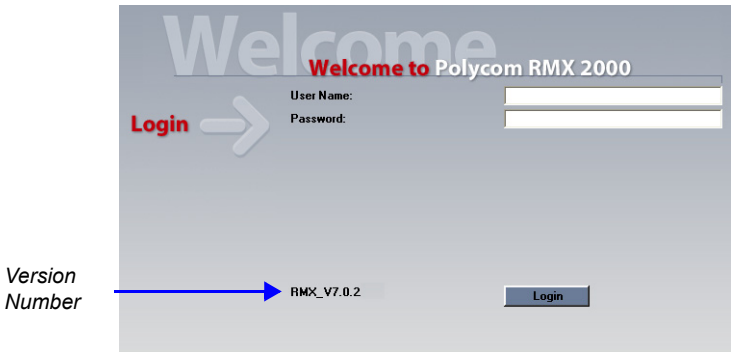
You may receive a message stating *Browser environment error. Please reopen the browser.*



13 **Optional.** Close and reopen the browser.

14 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RealPresence Collaboration Server*.

The *Login* screen is displayed. The version number has changed to *7.0.2*.



15 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator Sta ting up (15:25) showing the time remaining until the system start-up is complete.

- If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.
- If the upgrade process fails, please contact Polycom support.

Upgrade from Version 7.0.2 to Version 7.5.0.J

>> Continue with the upgrade from *Version 7.0.2* to *Version 7.5.0.J* as described starting on page 29.

Upgrading from Versions 5.1.0.G to Version 7.5.0.J

This upgrade requires the following intermediate upgrade procedures followed by an upgrade to *Version 7.5.0.J*:

1 Upgrade from *Version 5.1.0.G* to *Version 5.0.2*.

2 Upgrade from *Version 5.0.2* to *Version 7.0.2*.

Intermediate Upgrade from Version 5.1.0.G to Version 5.0.2

Ultra Secure Mode must be disabled before this upgrade can be performed.

1 Download the required software *Version 5.0.2* from the *Polycom Resource Center* web site.

If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 5.0.2* software to the workstation.
For more information see "*Windows 7™ Security Settings*" on page **15**.

2 Backup the configuration file. For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide for Maximum Security Environments, "Software Management"*.

3 Install *MCU* Software *Version 5.0.2*.
On the *RMX* menu, click **Administration> Software Management > Software Download**.

4 *Browse* to the *Install Path*, selecting the **Version 5.0.2xx.bin** file in the folder where *Version 5.0.2* is saved and click **Install**.

At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.

5 Click **Close** to close the *Install Software* dialog box.

6 When prompted whether to reset the *MCU*, click **Yes** to reset the *MCU*.

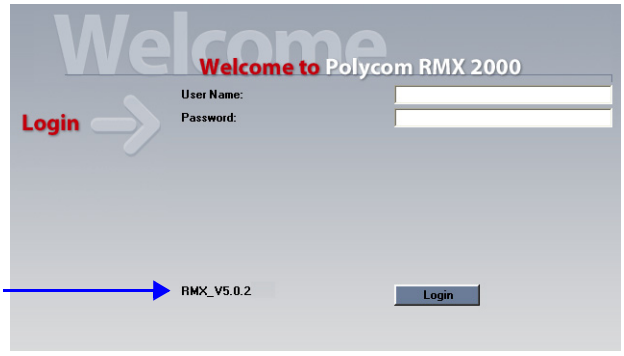
At the end of the installation process the system displays an indication that the software was successfully downloaded.

The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RealPresence Collaboration Server resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP*.

7 After about **30** minutes, **close and reopen the browser** and connect to the RealPresence Collaboration Server.
If the browser was not closed and reopened, the following error message is displayed: "Browser environment error. Please reopen the browser".

The version number in the *Welcome* screen has changed to *5.0.2*.



8 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator 

showing the time remaining until the system start-up is complete.

Intermediate Upgrade from Version 5.0.2 to Version 7.0.2

>> Continue with the upgrade from *Version 5.0.2* to *Version 7.0.2* as described starting on page 32.

Upgrade from Version 7.0.2 to Version 7.5.0.J

>> Continue with the upgrade from *Version 7.0/7.0.1/7.0.2* to *Version 7.5.0.J* as described starting on page 29.

Additional/Optional System Updates After Upgrading

IVR Services Update

DTMF Codes added in versions later than the version being upgraded are not automatically added to the *Conference IVR Service*. These *DTMF Codes* must be added manually.

To modify the Conference IVR Service:

1 In the IVR Services list, double-click the service to modify or right click the service and select Properties.

2 To add the gateway voice messages and dial tones, click the **General** tab and select the appropriate *.wav files.

3 To modify the DTMF codes, click the **DTMF Codes** tab.

4 Modify the DTMF codes as follows:

Table 2-3 *DTMF Code Changes (Continued)*

Action	Existing DTMF Code	New DTMF Code
Enable Roll Call	*32	*42
Disable Roll Call	#32	#42
Roll Call Review Names	*33	*43
Roll Call Stop Review	#33	#43
Start/Resume Recording	*73	*3
Stop Recording	*74	*2
Pause Recording	*75	*1
Request Private Assistance		*0
Request Assistance for the conference		00
PCM (for ISDN participants only)		##
Invite Participant		*72
Disconnect Last Invited Participant		#72

5 To add the Operator Assistance options, click the **Operator Assistance** tab and select the appropriate options and messages.

For details on modifying the IVR Services, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide for Maximum Security Environments*, *"Defining a New Conference IVR Service"*.

Media Encryption

When upgrading from a version prior to 7.6.1 the ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF *System Flag* is replaced by a value in the Conference *Profile*. Therefore, it is essential that the encryption settings of all existing conference Profiles are verified, and if necessary, modified to meet local encryption requirements through the new encryption options according to Table 3.

Table 3 *System Flag and Profile Settings in Version 7.6.1 and Earlier*

Encryption Setting			
Versions prior to 7.6.1		**Version 7.6.1 and Later**	
Parameter	**Value**	**Parameter**	**Value**
Profile Encryption Setting	**YES**	Profile Encryption Setting	**Encrypt All**
Profile Encryption Setting	**NO**	Profile Encryption Setting	**No Encryption**
System Flag	**ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF=YES**	FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE	**YES**

DMA Compatibility

If a Polycom DMA system is installed in the environment, the value of the flag, **MAX_PASSWORD_REPEATED_CHAR,** must be set to **4** to maintain compatibility between the *RealPresence Collaboration Server* and the DMA.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Administrator's Guide* "*Modifying System Flags*" on page **1-1**.

SHA-256 (Secure Hash Algorithm) Password Encryption

When upgrading to *Version 8.1.4.J*, user passwords will be hashed with *SHA-256* on *Login* and *SHA-1* hashed *Login* passwords will be deleted. New passwords are stored in SHA-256 format.

After an upgrade to version *8.1.4.J* there will be still passwords saved with the *SHA-1* signature. In order not to rely on automatic password signature conversion and replacement, and to ensure that the system only has *SHA-256* hashed passwords saved, the administrator should **either** ensure that all the users login to the system at least once to ensure automatic replacement of *SHA-1* hashed passwords with *SHA-256* hashed passwords **or** delete and recreate all users.

DNS per IP Network Service

The version includes support for a *DNS* to be configured for each *IP Network Service* that is defined. When upgrading from a version that does not support a *DNS* per *IP Network Service*, the *DNS* configured for the *Management Network Service* will be automatically be used in the *IP Network Service*. If required, modify the *DNS* settings in the *IP Network Service Properties* dialog box.

LAN Redundancy

In this version the default value of the **LAN_REDUNDANCY** *System Flag* has been changed to **NO**.

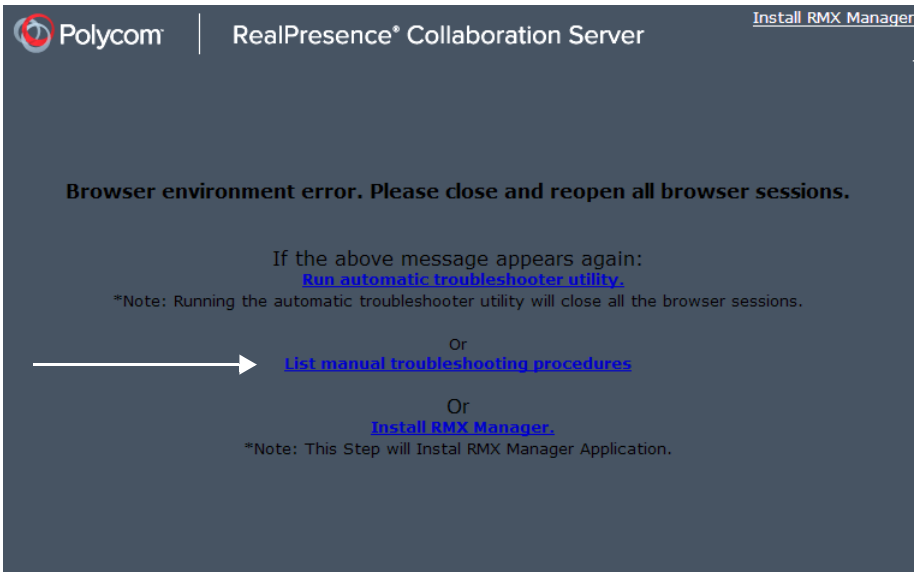
If *LAN Redundancy* is a system requirement, the **LAN_REDUNDANCY** *System Flag* must be added to *system.cfg* and its value set to **YES**.

For more information see the *RealPresence Collaboration Server 1500/2000/4000 Administrator's Guide*, "*Manually Adding and Deleting System Flags*" on page **22-18**.

If the flag value is set to **YES** and either of the LAN connections (LAN1 or LAN2) experiences a problem, an active alarm is raised stating that there is no LAN connection, specifying both the card and port number.

Troubleshooting

If a *Browser Environment Error* occurs, close and re-open the browser. If the problem persists, you can either run the *Automatic Troubleshooting Utility* or perform the *Troubleshooting Procedures* manually.



For more information see "*Troubleshooting Instructions*" on page **255**.

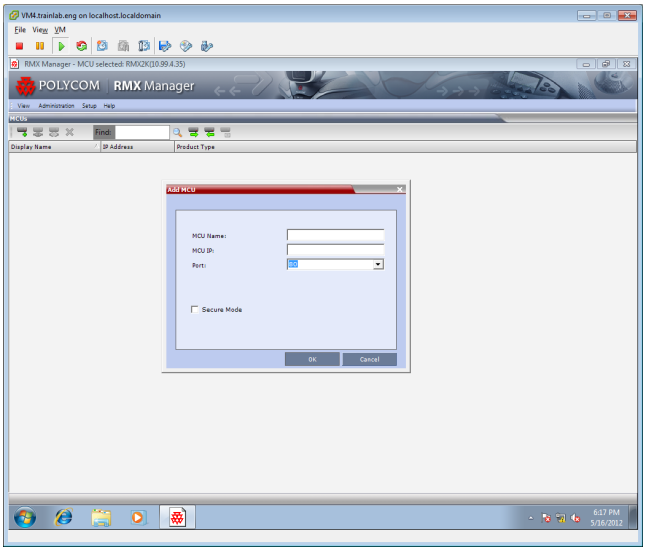
Upgrading the RMX Manager Application.

The *RMX Manager* specific to version 8.1.4.J must be used.

The *RMX Manager* specific to version 8.1.4.J can be downloaded from the *Support* section of the *Polycom* website at http://www.polycom.com/forms/rmx-sw-fed-thankyou.html

To upgrade the RMX Manager:

1. Back up the *RMX Manager* configuration.
   For more information, see the *RealPresence Collaboration Server 1500/2000/4000 Administrator's Guide*, "*Import/Export RMX Manager Configuration*".
2. Obtain the *RMX Manager* specific to *Version 8.1.4.J* from the *Polycom Software Distribution* website.
3. Install the *RMX Manager* on the workstation:
   a. Using *Windows*, navigate to the folder where the downloaded *RMX Manager* has been saved.
   b. Double-click on the downloaded install file and follow the on-screen instructions to complete the installation.
4. When the install of the *RMX Manager* is completed, launch the *RMX Manager* using the *Windows Start* menu.)



5. Import the backed up *MCUs* list using the *Import RMX Manager Configuration* option.
   For more information, see the *RealPresence Collaboration Server 1500/2000/4000 Administrator's Guide*, "*Import/Export RMX Manager Configuration*".
6. **Optional.** If needed, add the *MCU* to the *RMX Manager's MCUs* list.
   a. Right-click in the *RMX Manager* window.
   b. Select **Add MCU**.
   c. Enter the *MCU Name*.
   d. Enter the *IP Address* of the *MCU*.
   e. Leave the port as *Port 80* until such time that the *RMX* is placed into *Secure Mode*.

Version 8.1.4.J Detailed Description - New Security Features

MLPP (Multi Level Precedence and Preemption)

In compliance with *UC APL* requirements, *Quality of Service* (*QoS*) can be more accurately modified to suit local needs with the addition of *Multi Level Precedence* and *Preemption* methods for call prioritizing and call handling.

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

- Latency
- Low packet throughput
- Average delay between packets
- Jitter (variation in delay)
- Transmission error rate
- Order of packet delivery

Precedence is the method by which a call is assigned a priority level. The *RMX* supports two separately defined and configurable *Domains*, each having its own *Precedence* policy.

For a full description of *Precedence* see *IETF RFC 2474.*

One of the following *Precedence Levels* is assigned to all calls:

Table 2-1 *Precedence Levels*

Highest Priority	FLASH-OVERRIDE-OVERRIDE (Classified Networks only)
	FLASH-OVERRIDE
	FLASH
	IMMEDIATE
	PRIORITY
Lowest Priority	ROUTINE

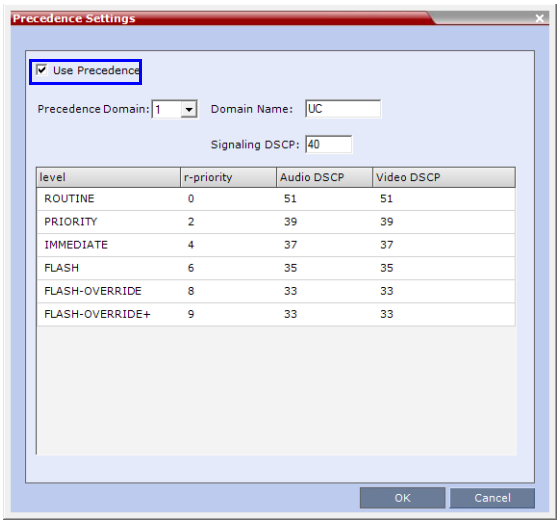
Conferences can have a mix of participants from different *Precedence* domains and network domains.

Precedence is supported for both IPv4 and IPv6.

Preemption is the method whereby, when system resources are insufficient, lower priority calls are terminated and their resources assigned to higher priority calls. *Preemption* is typically a function of network components such as the *Local Session Controller (LSC*). To the *RMX*, a preempted call appears as a disconnected call.

Enabling Precedence

Precedence is disabled by default. It is enabled by using the **Setup > Precedence Settings** menu to display the *Precedence Settings* dialog box. *Precedence* is enabled by selecting the **Use Precedence** check box.



See "*Configuring and Modifying Precedence Domains and DSCP Values*" on page **2-45**.

When *Precedence* is enabled, all other *QoS* system settings are overridden by the parameters sent in the *SIP Message*. For more information about *QoS*, see the *RealPresence® Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Network Services*" on page **1-1**.

SIP Message

A *SIP Message* is a request or a response between network entities that communicate using the SIP protocol. The *SIP Message* header contains *Precedence* and *Resource Priority* (*r-value*) information and an optional *Require* tag for each call.

For a full description of *SIP Messages* see *IETF RFC 3261*.

For a full description of *Resource Priority (DSCP)* see *IETF RFC 2474*.

For a full description of SIP *r-priority* see *IETF RFC 4412*.

Dial-in calls

If the *Use Precedence* check box in *Precedence Settings* is selected:

- The RMX uses the information in the *SIP Message* header to match the call to a *Precedence Domain* and a *Precedence Level*. Table 2-2 summarizes of the default values.

Table 2-2 *Precedence Domain and Resource Priority - DSCP Default Values*

Resource Priority	Precedence Level	DSCP Value	
		Audio	Video
9	*FLASH-OVERRIDE-OVERRIDE*	33 (0x21)	33 (0x21)
8	*FLASH-OVERRIDE*	33 (0x21)	33 (0x21)

Table 2-2 *Precedence Domain and Resource Priority - DSCP Default Values (Continued)*

Resource Priority	Precedence Level	DSCP Value	
		Audio	Video
6	*FLASH*	35 (0x23)	35 (0x23)
4	*IMMEDIATE*	37 (0x25)	37 (0x25)
2	*PRIORITY*	39 (0x27)	39 (0x27)
0	*ROUTINE*	51 (0x33)	51 (0x33)
NONE	No Resource Priority header for backward compatibility		

- *SIP Dial in* participants, both defined and undefined, do not inherit *Precedence* or *Domain* characteristics from the *Participant's Address Book*. (Additional fields, added to the *Participant's Properties - Advanced* and *Address Book - Advanced* dialog boxes are used to enter and modify *Precedence* or *Domain* characteristics for *SIP Dial-out* participants.)
- For backward compatibility, calls received with a *SIP Message* header that contains no *Precedence Domain* and the *Resource Priority* information, are assigned ROUTINE priority in the first defined *Precedence Domain*.
- Incoming calls are accepted or rejected depending on the:
  - Value of the **REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME** *System Flag*.
  - Match or mismatch of the *Precedence Domains,* set in the *RMX* and contained in the incoming *SIP Message r-value*.
    - The *r-value* is of the following format:

      r-value = `<domain name>-<subdomain>.<r-priority>`

  Table 2-3 shows an example of calls accepted or rejected assuming:
  - *Domain Name* = **UC**
  - *Sub Domain* = **000000**
  - *r-priority* = **2**

Table 2-3 *Example - Call Acceptance by System Flag Value and Precedence Domain Matching*

<table>
<tr><th colspan="4">Call Acceptance</th></tr>
<tr><th colspan="2">Precedence Domain</th><th colspan="2">Flag Value:
REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME</th></tr>
<tr><th>RMX</th><th>Incoming SIP Message</th><th>YES</th><th>NO (Default)</th></tr>
<tr><td>UC</td><td>UC</td><td rowspan="6">Call Accepted</td><td rowspan="9">Call Accepted
and
assigned ROUTINE priority</td></tr>
<tr><td>UC</td><td>UC.00001</td></tr>
<tr><td>UC</td><td>UC.00002</td></tr>
<tr><td>UC-00000</td><td>UC-00000</td></tr>
<tr><td>UC-00000</td><td>UC-00001</td></tr>
<tr><td>UC-00000</td><td>UC</td></tr>
<tr><td>UC</td><td>UC00002</td><td rowspan="3">Call Rejected</td></tr>
<tr><td>UC</td><td>UCC</td></tr>
<tr><td>UCC</td><td>UC</td></tr>
</table>

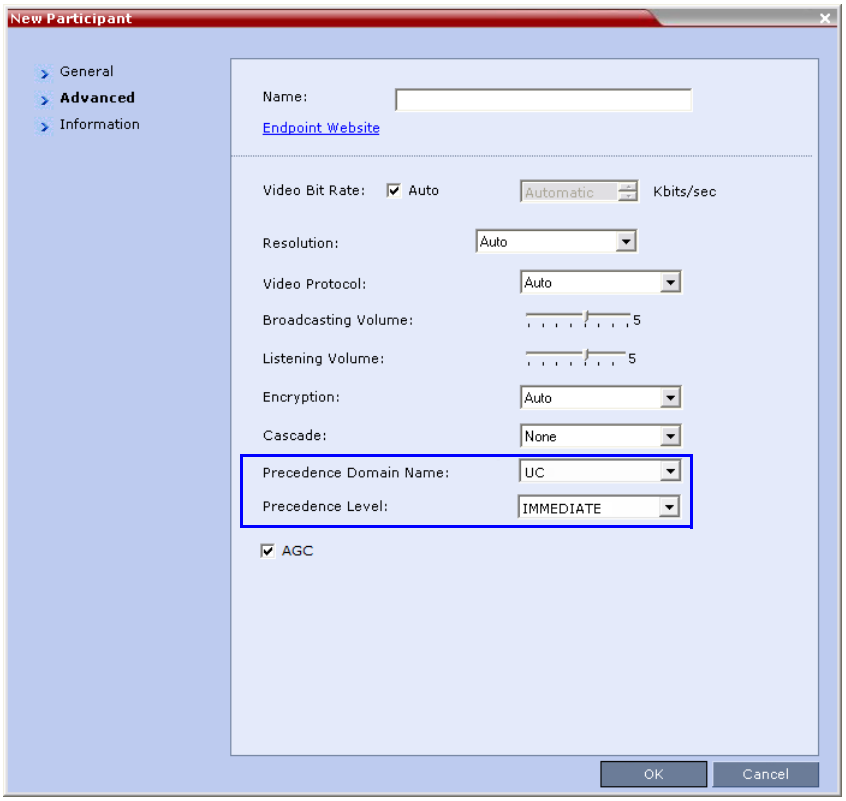
- Rejected calls receive a *417 Error* response.
- If the *Require* tag is null, the call is connected and assigned *ROUTINE* priority in the first defined *Precedence Domain*
- If the *Use Precedence* check box in *Precedence Settings* is cleared, the RMX will not reject such calls. The LSC is responsible for rejecting such calls.

Dial-out calls

For *Dial-out* calls, the *SIP Message* header information for the *Precedence Domain* and *Resource Priority* (*r-priority*) of the call is configurable.

Additional fields in the *Participant's Properties - Advanced* and *Participant's Address Book - Advanced* dialog box are used to modify these parameters:

- *Precedence Domain Name*
- *Precedence level*



Precedence Level Change

The *Precedence Level* of all calls can only be changed by the *LSC* sending a *Re-Invite* or similar *SIP Message* to the RMX.

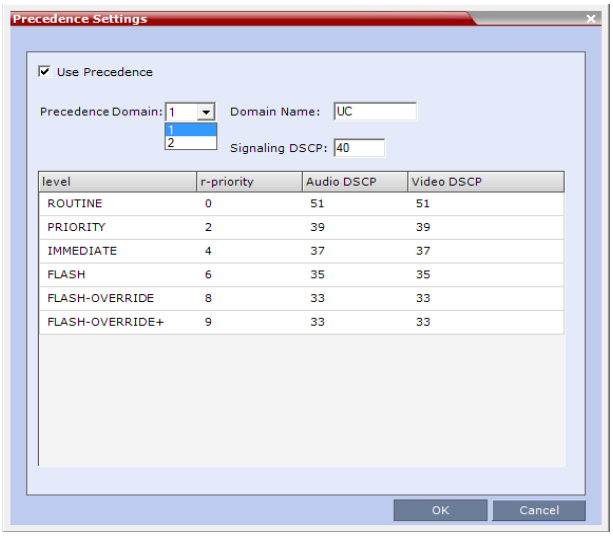
Configuring and Modifying Precedence Domains and DSCP Values

The *Precedence Domains* and *DSCP* values for each *Precedence Domain* can be configured and modified per *MCU*.

To configure Precedence Settings:

1 On the RMX menu, click **Setup** > **Precedence Settings**

The *Precedence Settings* dialog box is displayed.



2 **Optional:** Modify the values if required.

Table 2-4 *Precedence Settings - Domains, Levels and DSCP Values*

Field	Description
Use Precedence	Select or clear the check box to enable or disable *Precedence*. **Default:** Cleared (*Precedence* disabled)
Precedence Domain	Select the *Precedence Domain* to be modified, 1 or 2, from the drop-down menu. **Possible Values:** 1 / 2
Domain Name	Enter the required *Domain Name*.
Signaling DSCP	Modify the *DSCP* value of the *Signaling DSCP*. A single *Signaling Proxy* is used for all *Precedence Levels*. **Default:** 40 **Range:** 0 - 63
Level	*r-priority, Audio DSCP* and *Video DSCP* values can be modified for each of the six *Precedence Levels*: • ROUTINE • PRIORITY • IMMEDIATE • FLASH • FLASH-OVERRIDE • FLASH-OVERRIDE+

Table 2-4 Precedence Settings - Domains, Levels and DSCP Values (Continued)

Field	Description
r-priority	Modify the *r-priority* value for the *Level*. **Range:** 0 - 255. **Default:** ROUTINE - 0, PRIORITY - 2, IMMEDIATE - 4, FLASH - 6, FLASH-OVERRIDE - 8, FLASH-OVERRIDE+ - 9
Audio/Video DSCP	Modify the *DSCP* value for the *Audio/Video DSCP.* **Range:** 0 - 63. **Default:** ROUTINE - 51, PRIORITY - 39, IMMEDIATE - 37, FLASH - 35, FLASH-OVERRIDE - 33, FLASH-OVERRIDE+ - 31

3 Click **OK**.

System Flags

Changes to Existing Flags

The default value of the following flags have been changed:

Table 2-5 Flags - Old vs New Default Values

Flag name	Old Default Value (hex)	New Default Value (hex)
QOS_IP_VIDEO	0x88	0x31
QOS_IP_AUDIO	0x88	0x31
QOS_IP_SIGNALING	0x00	0x28
RTCP_QOS_IS_EQUAL_TO_RTP	NO	YES

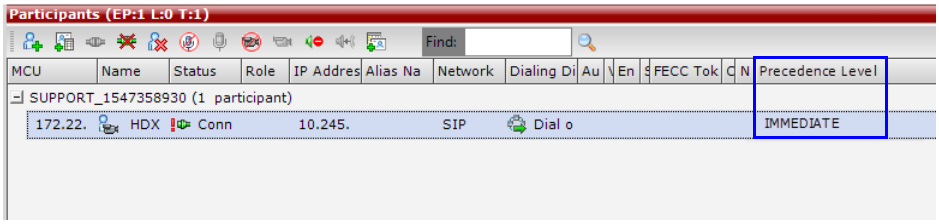
New Flags

The following *System Flags* must be added to *system.cfg* if their values are to be modified:

- **QOS_MANAGEMENT_NETWORK** - the overall hex value of the DiffServ field (not just the value of the DSCP portion) is used as the *DSCP* value for the *RMX Management Network*.
  - **Default:** 0x10
  - **Range:** 0x00 - 0xFC
- **REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME** - see "*Dial-in calls"* on page **2-41** (above) for a description of this flag.
  - **Default:** NO
  - **Range:** YES / NO

Monitoring Precedence Level

The *Precedence Level* of each connected participant is listed in the *Participants* list pane.



IEEE 802.1X Authentication

In compliance with *UC APL* requirements for enhanced security of wireless local area networks that follow the *IEEE 802.11* standard, support for *802.1X Authentication* has been included in this version.

802.1X Authentication requires that the *RMX* registers with a *802.1X Authentication Server and* is supported on *RMX 1500/2000/4000* The authentication protocol is applied to each the following *Network Interface Controllers* (*NICs*):

- Management
- Signaling
- Media

- For RMX 2000, *Network Separation* must be implemented before configuring *802.1X Authentication.*
- *802.1X Authentication* is not supported in *Microsoft* environments.

The following *802.1X Authentication* methods are supported:

- EAP-MD5
- EAP-TLS
- PEAPv0
- MSCHAPv2

Certificate Repository

Implementation of *802.1X Authentication* requires a certificate, which is obtained from the *Certificate Repository*.

- Either one *TLS* certificate is retrieved for all *IP* services and their associated *NICs,*
  - — If one certificate is retrieved for all *NICs,* the RMX will use the *Management Certificate* for all the *NICs.*

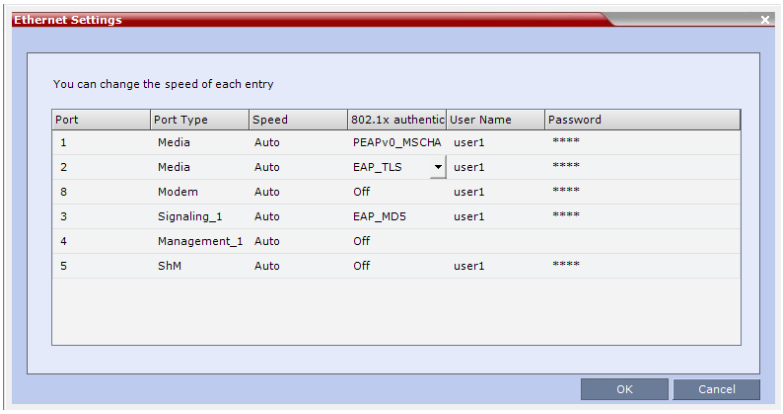
  or
- A *TLS* certificate for each *IP* service and their associated *NICs* is retrieved from the *Certificate Repository*:
  - — If several different *TLS* certificates are retrieved, each *NIC* will use the certificate of the service that it is associated with.
    - In a system configured with *Multiple Network Services* each *IP* service will use its own certificate.

- A *NIC* that does not have its own certificate will first attempt to use the *Management Certificate* before using a self-signed certificate.

Enabling and Configuring 802.1X Authentication

802.1X Authentication for each *NIC* is enabled or disabled in the **Setup > Ethernet Settings** dialog box. The following additional table columns are used to modify these parameters:

- *802.1X Authentication*
- *User Name*
- *Password*

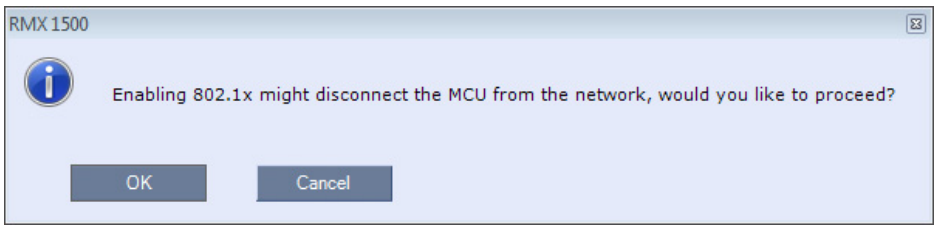


Modify the *Ethernet Settings* table fields as set out in Table 2-6:

Table 2-6 *802.1X Authentication - Configuration*

Field	Description
802.1x Authentication	For each *NIC*, click the arrow to open the drop-down menu and select (or disable) the *802.1X Authentication* method: • Off • EAP-MD5 • EAP-TLS • PEAPv0 • MSCHAPv2
User Name	Enter the *User* name that the RMX will use to register with the *802.1X Authentication Server*. This must be the RMX's *DNS* name and can be up to 256 characters. **Note:** If the *Domain Name (DC)* field was completed in the *Certificate Request*, the *User* must be: `<Common Name (DNS)>@<Domain Name (DC)>` as set out in the *Certificate Request*.
Password (EAP-MD5, PEAPv0 and MSCHAPv2 only)	Enter the *Password*, that the RMX will use to register with the *802.1X Authentication Server*. Up to 256 Unicode characters can be used. The *Password* is always displayed as four asterisks.

Enabling *802.1X Authentication* can result in the RMX being disconnected from the network and a warning message is displayed:



System Flags

The following system flags are used to manage the *802.1X Authentication* process. They must be manually added to *system.cfg* if their default values need to be modified.

Table 2-7 *New Flags*

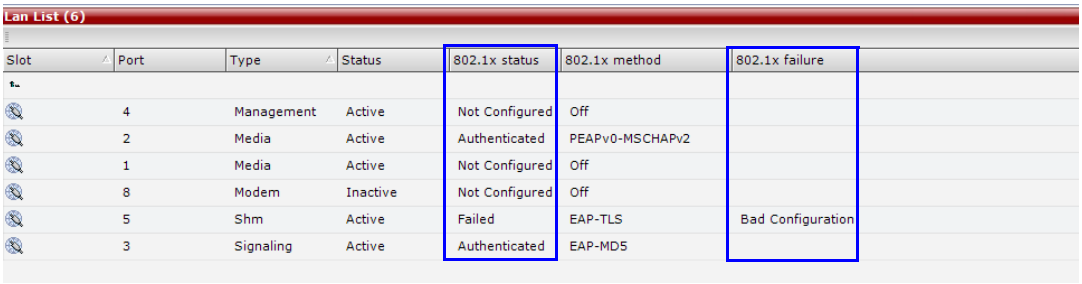
Flag name	Description
802_1X_CERTIFICATE_MODE	Determines whether one *TLS* certificate is retrieved from the *Certificate Repository* for all *IP* services or if multiple certificates will be retrieved, one for each *IP* service. **Range:** ONE_CERTIFICATE, MULTIPLE_CERTIFICATE **Default:** ONE_CERTIFICATE.
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. **Range:** YES, NO. **Default:** YES.
802_FIPS_MODE	If the flag value is YES, the availability of the MD5 Authentication Protocol will neither be displayed as selectable option nor supported. **Range:** YES/NO. **Default:** NO

Disabling 802.1X Authentication

Switching to *http* mode from *https* mode by inserting a USB key containing a file named **RestoreFactorySecurityDefaults.txt** into the *RTM-IP USB* port disables *802.1X* functionality

Ethernet Monitoring

802.1x Status is displayed in the *Hardware Monitor - LAN List*.



Lan List (6)

Slot	Port	Type	Status	802.1x status	802.1x method	802.1x failure
	4	Management	Active	Not Configured	Off	
	2	Media	Active	Authenticated	PEAPv0-MSCHAPv2	
	1	Media	Active	Not Configured	Off	
	8	Modem	Inactive	Not Configured	Off	
	5	Shm	Active	Failed	EAP-TLS	Bad Configuration
	3	Signaling	Active	Authenticated	EAP-MD5	

The following *802.1X Statuses* are possible:

- *Authenticated*
- *Not Configured*
- *Failed*

The following *802.1X Failure* reasons are possible:

- *Bad Configuration*
- *Link Status not Detected*

White List Access

In compliance with *UC APL* requirements for enhanced security of web access to the RMX, a *White List* containing the addresses of *IP Networking Entities* permitted to connect to the *RMX's Management Network* is implemented - *Networking Entities* such as *Network Hosts, Control Workstations, Gatekeepers SIP/ DNS Servers*, etc.

Guidelines

- Only administrators can access and modify the *White List*.
- During *First Time Installation and Configuration*, when enabling the *White List*, the *IP* address of the workstation used to run the *RMX Web Client* is automatically added to the *White List*.
- The last *White List* entry cannot be deleted to prevent lock out. Any attempt to enable an empty *White List* results in the display of an error message: *WhiteList is empty please add IP's to the list if you want to enable WhiteList*.
- Both *IPv4* and *IPv6* are supported.
- Web access to the RMX for *http* and *https* is through ports *80* and *443* respectively.
- The *White List* can hold up to 100 entries. An error message is displayed when exceeding this limit.
- Access is blocked at the firewall for devices with *IP* addresses not listed in the *White List*.
- The *White List* is saved during *Backup*, *Restore* and *Upgrade* processes.
- Changes to the *White List* are written to the *Auditor Event File*.
- Alterations to the *White List* do not require a system reset.

Enabling, Disabling and Modifying the White List

The use of *White List* in the environment can be enabled or disabled in the *Management Network Service - White List* dialog box.

To enable, disable, view or modify the White List:

1 In the *RMX Management* pane, click the **IP Network Services**.

The *IP Network Services* pane is displayed.

2 In the *IP Network Services* list pane, double-click the **Management Network** entry.

The *Management Network* dialog box is displayed.

3 Click the **WhiteList** tab.

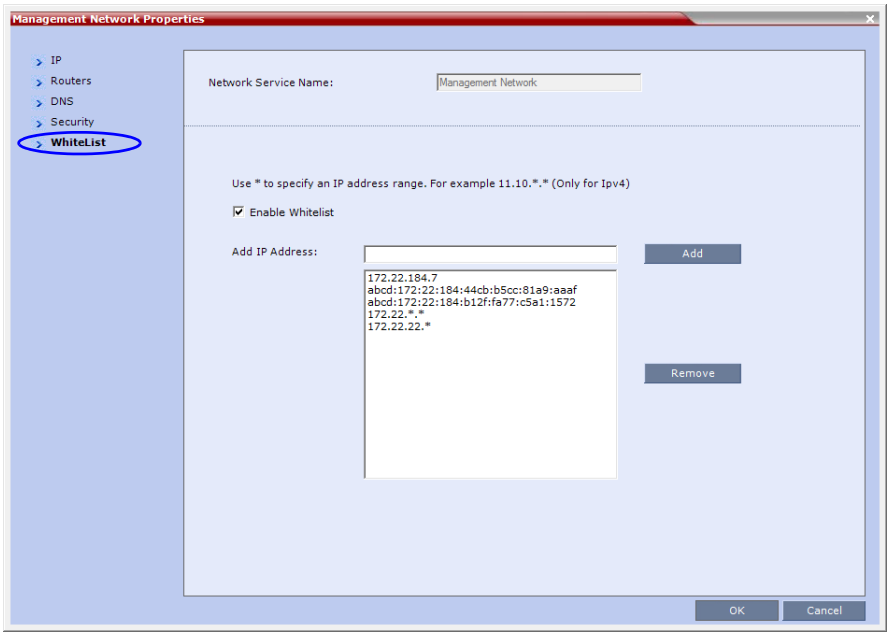
The *WhiteList* dialog box is displayed.

— If there are no entries in the *White List,* it is disabled to prevent lock out.

— If the *White List* is disabled none of the *IP* addresses in the list are displayed.

— The *Add* and *Remove* buttons are only active if the *Enable Whitelist* check box is selected.

4 Select the **Enable Whitelist** check box.



All *IP* addresses in the list are displayed and the *Add* and *Remove* buttons become active.

5 Modify the *White List*.

Both *IPv4* and *IPv6* addresses are supported and the system will only allow an entry of the type of *IP* addresses for which the *Management Network Service* is configured according to Table 2-8.

Table 2-8 *IP Address Modes*

IP Address Modes	
RMX	**Workstation / Device**
IPv4	IPv4
	IPv4 & IPv6
IPv6	IPv6
	IPv4 & IPv6
IPv4 & IPv6	IPv4
	IPv6
	IPv4 & IPv6

— If the system changes its *IP* addressing mode (e.g. from *IPv4* only to both *IPv4 &6*) while the *White List* is enabled, the *White List* is disabled and a message, *White list has been disabled please reconfigure*, is displayed.

— *IPv4* addresses can be added as a range by using the wildcard character, *, to substitute the 3rd and 4th dotted decimal numbers of the *IP* address, e.g. 11.10.*.*

a To **Add** *IP* addresses:

For each *IP* address to be added to the *White List*:

i) In the *Add IP Address* field enter an *IP* address to be added to the *White List* and click the **Add** button.

If an invalid *IP* address is entered, an error message is displayed and the administrator is prompted to enter a correct IP address.

If a duplicate *IP* address is entered, a message: *Duplicate IP's are not allowed in WhiteList* is displayed.

ii) When all the *IP* addresses have been added, click **OK**.

A message is displayed: *Applying white list will limit RMX web access to the configured IP list, are you sure you want to continue?*

iii) Click **Yes** to apply the modified *White List*.

b To **Remove** *IP* addresses:

For each *IP* address to be removed from the *White List*:

i) In the *White List*, click to select an *IP* address to be removed from the *White List*.

ii) Click the **Remove** button.

ii) When all the *IP* necessary addresses have been removed, click **OK**.

A message is displayed: *Applying white list will limit RMX web access to the configured IP list, are you sure you want to continue?*

iii) Click **Yes** to apply the modified *White List*.

Alternative Network Address Types (ANAT)

In compliance with *UC_APL_NET_0007 Alternative Network Address Types* (*ANAT*) is supported.

When the RMX is configured for *IPv4* and *IPv6 Addressing*, the addition of the s*dp-anat option tag* in the *SIP Require* and *SIP Supported* headers allows a mixture of *IPv4* and *IPv6 addressing* to be specified by the *Session Description Protocol* (*SDP*).

For a full description of *ANAT* see *IETF RFCs 4091* and *4092*.

Guidelines

- *BFCP* over *TCP* is not supported in *Ultra Secure Mode*. It's associated *Content* channel is not available.
- *BFCP* over *UDP* is supported in *Ultra Secure Mode*.
- If the RMX is configured for both *IPv4* and *IPv6*, *IPv4* addressing is given preference when establishing the connection.
- If an *Outbound Proxy* is configured, its transport type is used.
- If an *Outbound Proxy* is not configured, the *SIP Server's* (*Registrar*) transport type is used.

  The *Outbound Proxy* and the *SIP Server* must be configured with one type only either according to the *IP* address type or according to the *DNS Resolution* type. However, if the RMX is configured for *IPv4&IPv6* then the *SIP Contact* field will contain both *IPv4* and *IPv6* addresses.

System Flag

The *ANAT Protocol* selection is controlled by the **ANAT_IP_PROTOCOL** *System Flag*. To modify it, manually add it to *system.cfg* and set its value as described in Table 2-9.

Range: DISABLED, AUTO, PREFER_IPv4, PREFER_IPv6

Default:

— If the **ULTRA_SECURE_MODE** *System Flag* is set to **NO**: **DISABLED**.

— If the **ULTRA_SECURE_MODE** *System Flag* is set to **YES**: **AUTO**.

Table 2-9 *ANAT_IP_PROTOCOL System Flag Values for Dial in Dial out*

Value	Behavior - Dial in and Dial out
DISABLED	*sdp-anat* does not appear in *SIP* headers and the *SDP* does not contain a mixture of IPv4 and IPv6. If an endpoint requests *ANAT* (sends the *Require: sdp-anat* tag) the RMX will accept the call.
AUTO	*sdp-anat* appears in *SIP* headers. **Dial in:** The *IP Version* preference is according to the *SDP* priority. **Dial out:** *IPv4* is advertised first.
PREFER_IPv4	*sdp-anat* appears in *SIP* headers. **Dial in:** *IPv4* is the *IP Version* preference. **Dial out:** *IPv4* is advertised first.
PREFER_IPv6	*sdp-anat* appears in *SIP* headers. **Dial in:** *IPv6* is the *IP Version* preference **Dial out:** *IPv6* is advertised first.

BFCP Over UDP – AS-SIP Content

In compliance with *UCR 2008 Change 3*, *AS-SIP* (*Assured Services-Session Initiation Protocol*) *Content* flow has been included in this version. *AS-SIP* is an implementation of *SIP* that utilizes *SIP's* built in security features.

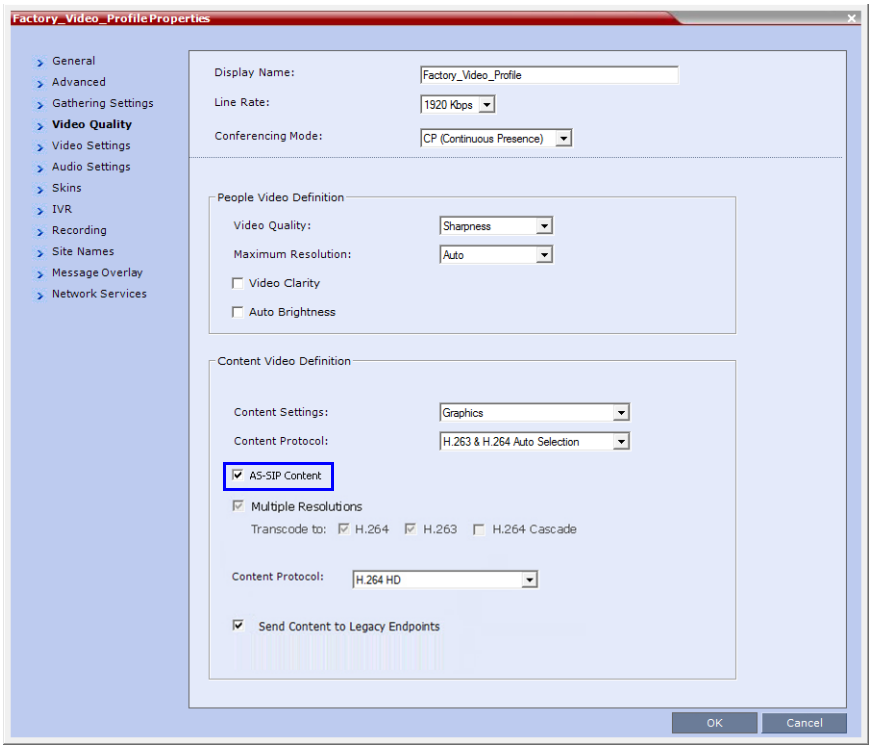
When using *AS-SIP Content*, the *media line* of the content channel is not sent as part of the initial *SDP Offer/Answer* message sequence. The *media line* of the *Content* channel is only sent to the *MCU* when an endpoint wanting to share *Content* initiates *Content* sharing. The RMX (RMX) then sends the *Content media line* to all conference participants using an *SDP Re-invite*.

Guidelines

- *AS-SIP Content* is shared using *Multiple Resolutions (Content Transcoding)* and is not supported in any other *Content* sharing mode such as *H.263 Content* and *H.264 Cascade and SVC Optimized Content Protocol*.
- *Multiple Resolutions* consumes system video resources. If sufficient system video resources are not available, a conference with *AS-SIP Content* enabled in its *Profile*, will not be created. An error: *Conference could not be created due to lack of Content DSP resources*, is displayed.
- The *SIP BFCP UDP* application line is included in *SDP Offer/Answer* message sequence.
- An endpoint declaring *SIP BFCP TCP* is connected with *video* and *audio* but without *Content*. The *SIP BFCP TCP* channel will not be connected.
- The following resolutions are supported with *H.264 HD Content* protocol. Only when *H.264 HD* is selected, these resolutions are enabled for selection:
  - *HD 720p5*
  - *HD 720p30*
  - *HD 1080p15*
- Endpoints that do not support receiving *H.264 Content* at a resolution of *HD 720p5* or greater are considered *Legacy Endpoints* and will receive *Content* using the people video channel.
- Endpoints that do not support transmitting *H.264 Content* at a resolution of *HD 720p5* or greater are considered *Legacy Endpoints* and will transmit *Content* using the people video channel. Depending on the endpoint type, these endpoints may not be able to transmit *Content* at all - this is dependent on the endpoint and is not controlled by the *RMX*.
- A mixture of older, non *AS-SIP* compliant and *AS-SIP* compliant endpoints are supported in the same conference and are able to share *Content*.
- An endpoint connecting during a *Content* session is immediately sent an *SDP Re-invite* that includes the connect media line and will receive *Content*.
- An endpoint connecting after *Content* started and was stopped will receive the *SDP Re-invite* and the content media line only after a new *Content* request is sent.
- Once *Content* has been initiated by one of the endpoints, the *Content* channel will be opened to all endpoints and remain open even if the *Content* sharing endpoint stops sharing *Content*.

Enabling AS-SIP Content

AS-SIP Content is enabled in the *New Profile / Profile Properties - Video Quality* tab.



When the *AS-SIP Content* check box is selected the following are automatically enabled and cannot be disabled:

- *Send Content to Legacy Endpoints*
- *Multiple Resolutions*

System Flag

The time that the *RMX* waits for endpoints to respond to its *SDP Re-invite* is determined by a timer. The timer duration, in seconds, is controlled by the **AS_SIP_CONTENT_TIMER** *System Flag*. Its default value is 10 seconds. To modify the timer value, manually add this flag to *system.cfg* and modifying its value as required:

Range: 1 - 60 seconds. (Values outside this range are rejected and an error message is displayed.)

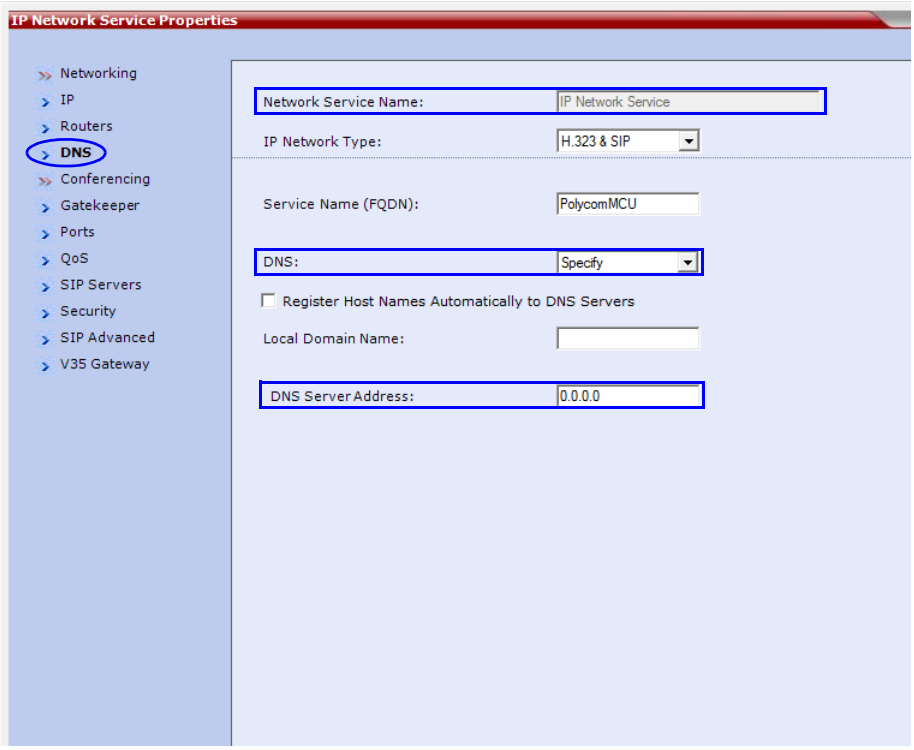
DNS per IP Network Service

In both *Standard Security* and *Ultra Secure Modes:*

- A *DNS* can be configured for the *Management Network Service* that is defined and the *IP Network Service*.
- If a *Multiple Services Licence* is installed, a *DNS* can be configured for each additional *IP Network Service* that is defined.

To configure a DNS per IP Network Service:

1 In the *New IP Network Service / IP Network Service Properties* dialog box, click the **DNS** tab.



2 In the *DNS* field select **Specify**.

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

4 Continue configuring the *IP Network Service* or click **OK** to save your changes.

Guidelines

- If the *DNS* field in the *IP Network Service* is set to **Specify** and the *DNS* is not configured or disabled, the *DNS* configured for the *Management Network* will be used.
- When upgrading from a version that does not support a *DNS* per *IP Network Service*, the *DNS* configured for the *Management Network* will be used.

Internet Control Message Protocol (ICMP)

ICMP (*Internet Control Message Protocol*) is used to send messages between networked entities. It is typically used to send and receive information concerning:

- Communications errors in network applications
- Remote host reachability and availability
- Network congestion (latency)
- Traffic redirection

Malicious devices can however use these capabilities in order to divert, intercept, detect, network traffic.

The following *System Flags* have been added to enable the administrator to control *ICMP Redirect* and *Destination Unreachable* messages:

- **ENABLE_ACCEPTING_ICMP_REDIRECT**
- **ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE**

By setting the value of these flags to **NO** the risk of malicious behavior can be mitigated.

For a full description of *ICMP* see *RFC 792*.

Guidelines

- Both flags apply to all *MCU* platforms: *RealPresence Collaboration Server* (*RMX*) 1500/2000/4000/*RealPresence Collaboration Server* (*RMX*) 1800/*RealPresence Collaboration Server 800s*).
- Both flags apply to all *Ethernet* connections: *Management*, *Signaling*, *Media*, *Modem*, etc.

System Flag: ENABLE_ACCEPTING_ICMP_REDIRECT

This *System Flag* enables the administrator to control whether the RMX accepts or rejects *ICMP Redirect Messages (ICMP* message type #5*)*, typically used to instruct routers to redirect network traffic through alternate network elements.

- **Range: YES / NO**
- **Default**:
  - **Ultra Secure Mode: NO** - Redirect messages or ignored.
  - **Default Security Mode: YES -** Redirect messages are accepted.

System Flag: ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE

This *System Flag* enables the administrator to control whether the RMX sends *ICMP Destination Unreachable Messages (ICMP* message type #3*)*.

Destination Unreachable Messages are sent when the RMX receives a *UDP* packet on a port configured for *TCP,* or receives a *UDP* packet on a port configured for TCP, or when, in real time, a packet is not processed in the prescribed time interval. For detailed timestamp information see *RFC 792*.

The *Destination Unreachable Message* may also be sent when *Network* or *Host* is unreachable (sent by the router) or the *Port* is unreachable (sent by the RMX).

- **Range: YES / NO**
- **Default**:
  - **Ultra Secure Mode: NO** - *Destination Unreachable Message* is never sent.
  - **Default Security Mode: YES -** *Destination Unreachable Message* is sent when needed.

Modifying the flag values

To modify the *System Flags* values, the flags must first be manually added to *system.cfg*. For more information about *System Flags*, see "*Manually Adding and Deleting System Flags*" in the *Administrator's Guide*.

Version 8.1.4.J - Changes to Existing Security Features

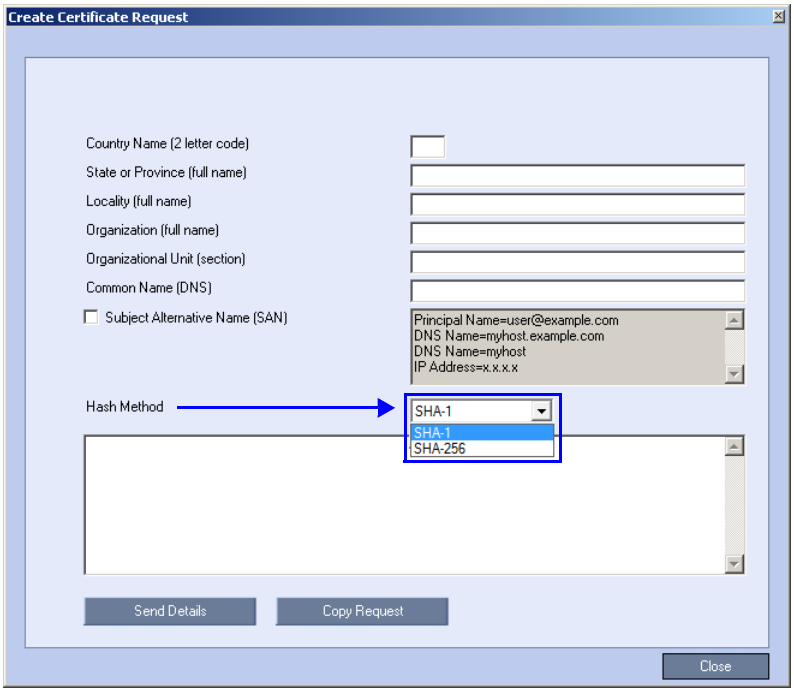
Password Encryption - Migration from SHA-1 to SHA-256

In compliance with *UC APL, FIPS 140-2* the *SHA-256* (*Secure Hash Algorithm)* becomes mandatory for:

- Application login passwords.
- Linux operating system passwords.
- CSRs (Certificate Signing Requests).

The output value for SHA-256 is 256 bits whereas for SHA-1 the output value is 160 bits.

For backward compatibility with previous versions, either *SHA-1* or *SHA-256* can be selected as the hash algorithm used in the creation of *CSRs*.



Upgrade / Downgrade Guidelines

The RMX configuration, including users and passwords, should be backed up before upgrading or downgrading.

Table 2-10 summarizes the system behavior with regard to passwords and certificates when upgrading to or downgrading from this version.

Table 2-10 *Version Change - Password and Certificate Compatibility*

Version Change	Behavior	
	Passwords	**Certificates**
Upgrade from old version to new version	On user login: • All **new-user** passwords are hashed and saved using *SHA-256*. • **Existing** user passwords remain saved using the SHA-1 signature, however: • On first login after the upgrade the *SHA-1* hashed password is automatically replaced with *SHA-256* hashed password. **Note:** After an upgrade to version *8.1.4.J* there will be still passwords saved with the *SHA-1* signature. In order not to rely on automatic password signature conversion and replacement, and to ensure that the system only has *SHA-256* hashed passwords saved, the administrator should: Either: • Ensure that all the users login to the system at least once to ensure automatic replacement of *SHA-1* hashed passwords with *SHA-256* hashed passwords. Or: • Delete and recreate all users.	The new version accepts certificates issued with *SHA-1* hashing.

Table 2-10 *Version Change - Password and Certificate Compatibility (Continued)*

Version Change	Behavior	
	Passwords	**Certificates**

Downgrade *from new version to old version*	Before the downgrade procedure begins, the administrator receives a popup warning message “Passwords will change to factory default would you like to proceed?”
	All users *and SHA-256* hashed passwords are deleted.
	The administrator’s *User Name* and *Password* reverts to the *Factory Default:* POLYCOM / POLYCOM.
		The old version accepts certificates issued with *SHA-1* hashing.
		
		For certificates issued with *SHA-256* hashing:
		• The administrator receives a popup warning message "TLS certificate will be deleted and the system will switch to non-secured connection, would you like to proceed?”
		• For each certificate that is hashed with SHA-256:
		  • *RMX Web Client / RMX Manager* connections to the RMX are switched to non-secured mode.
		  • LDAP services are changed from 636 to port 389.
		  • *SIP TLS* sessions are changed to *SIP UDP*.
		  • The certificate is deleted.

Non-hashed Passwords

All non-hashed passwords are stored encrypted as set out in Table 2-11.

Table 2-11 *Non-hashed Passwords - Encryption*

Connection	Storage type	Previous Versions	From Version 8.1
SNMPv3 *Two passwords:* *Authentication / Privacy*	Community permissions which are not the PW to connect to SNMP are not Saved Encrypted	Non encrypted	AES 256
Exchange	Non encrypted – Feature disabled in Ultra Secure Mode	Non encrypted	AES 256
RV v.35 serial ports – password for login	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256
H.323 authentication – password	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256
SIP digest – password	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256

PKI Online Certificate Status Protocol OCSP

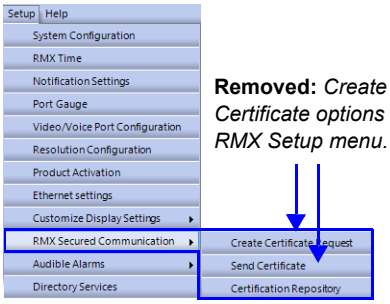
In compliance with *UC APL* requirements, the *PKI* feature set has been enhanced and expanded.

Beginning with this version:

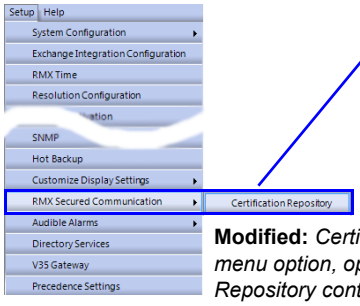
- A single *Certificate Repository* is maintained for:
  - The *Management Network Service.*
  - *SIP TLS* Personal Certificates for each defined *IP Network Service*.
  - Trusted (*CA*) certificate for all *TLS* connections.
  - *CRL* for all *TLS* connections.
- *SIP TLS* certificates are validated against the *CA*.
- *SIP TLS* certificates are managed using *CRL* and *Online Certificate Status Protocol* (OCSP).
  - Certificate revocation mode, whether by *OCSP* or *CRL* is managed using the i setting of the *Management Network*.
  - *SIP TLS* is managed using the *General TLS* setting.

Changes to the RMX Web Client and RMX Manager

Certificate creation and management is enhanced by the following changes to the *RMX Web Client* and *RMX Manager*.

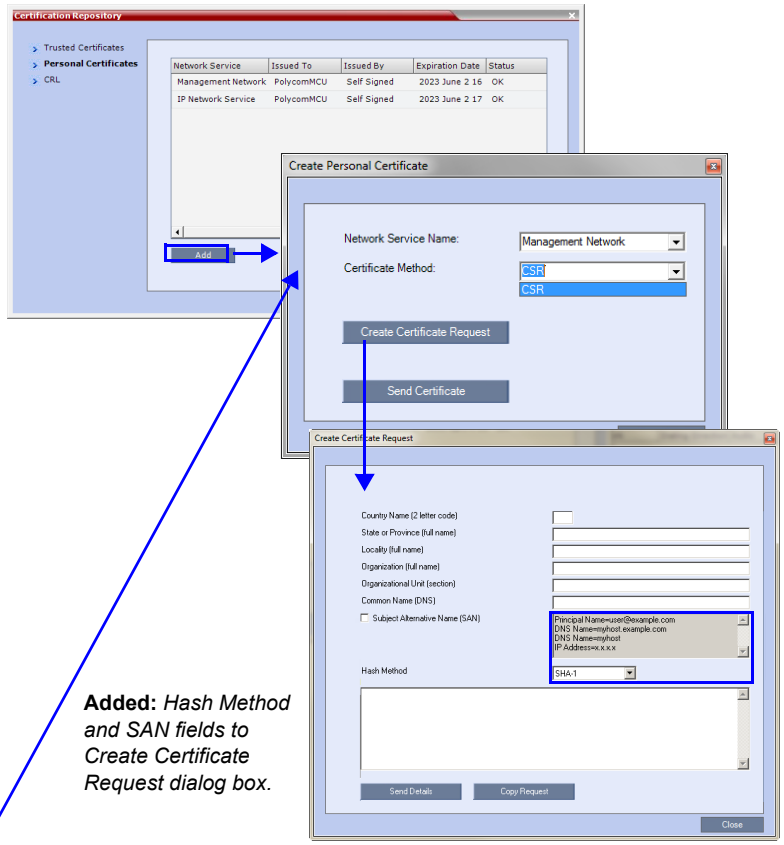


Removed: *Create / Send Certificate options in the RMX Setup menu.*



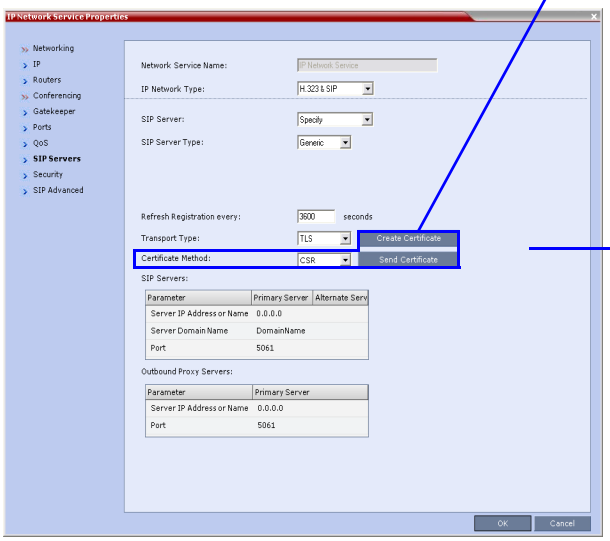
Modified: *Certification Repository menu option, opens Certification Repository containing Create / Send Certificate options.*

Added: *Certification Repository management dialog box, containing a Create Certificate Request and Send Certificate dialog box.*

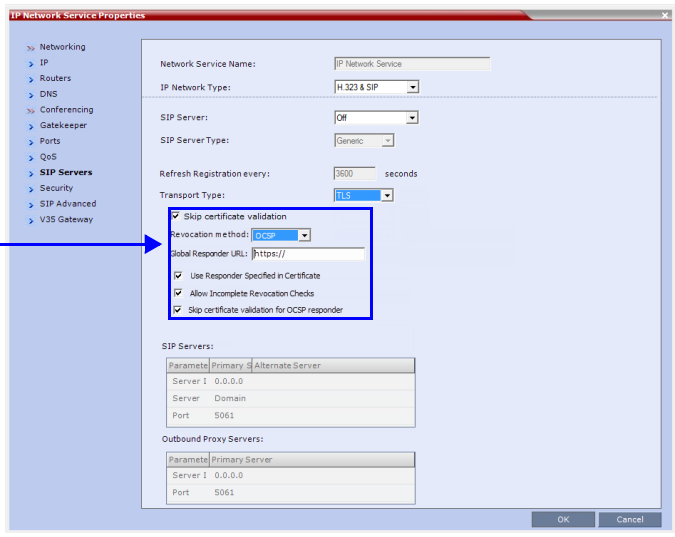


Added: *Hash Method and SAN fields to Create Certificate Request dialog box.*

Removed: *From IP and Management Network Services - SIP Servers tab: TLS Certificate Method; Create Certificate; Send Certificate*



Added: *To IP and Management Network Services: TLS Certificate Validation and Revocation options*



Adding Certificates to the Certificate Repository

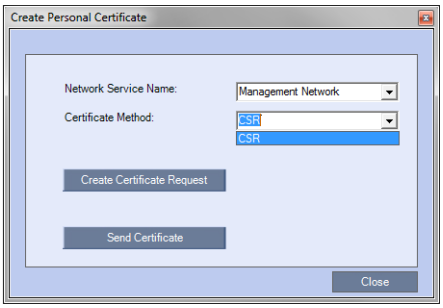
Personal Certificates

To add a Personal Certificate to the Certificate Repository:

1 In the *Certification Repository - Personal Certificates* tab select the *Network Service*.

2 Click the **Add** button.

The *Add* dialog box is displayed with the configured parameters of the selected *Network Service* filled in.



3 Select the *Certificate Method*. (Default is *CSR*)

— Only *CSR* can be selected for the *Default Management Network Service*.

— *CSR* or *PFX/PEM* can be selected for *IP Network Services*.

4 Optional. If *CSR* was selected as the *Certificate Method:*

a Click **Create Certificate Request**.

The *Create Certificate Request* dialog box is displayed with the *Common Name* field filled in.

b Complete the *Certificate Request* fields.

The two additional fields are defined as:

- *Subject Alternative Name* (*SAN*) - This field is required when using *EAP-TLS* in conjunction with a *Network Policy Server* (*MS-NPS*). It allows the optional inclusion of:

  - Principle Name

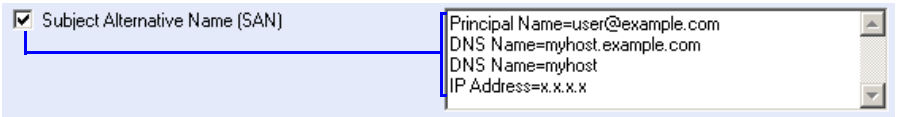
  - DNS Name:

  Long – FQDN

  Short - Host only

  - IP Address (IPv4 and IPv6)

When the *Subject Alternative Name* (*SAN*) check box is selected the input box becomes active, allowing the user to modify the example values provided, to match local certificate requirements and delete those that are not applicable.



The user can add up to 20 different *SAN*s. If an incorrect *SAN* type is entered, an error message, *Unsupported SAN type,* is displayed when the **Send Details** button is clicked.

- The *SAN* field, *DNS Name* (*FQDN*) is not used for *Machine Account* validation. For example, when using a DMA, the DMA will not validate the *RMX* unless the *FQDN* field in the *User Properties* (*New User*) dialog box is correctly filled in.
- The *SAN* field should not be used when configuring the *RMX* for use in *MS Lync Environments*.

- *Hash Method* - Select the output value for the *Secure Hash Algorithm:*
  - *SHA-256* the output value is 256 bits.
  - *SHA-1* the output value is 160 bits.

  For backward compatibility, with previous versions, either SHA-1 or SHA-256 can be selected as the hash algorithm used in the creation of CSRs (Certificate Signing Requests).

5 Click **Send Certificate**.

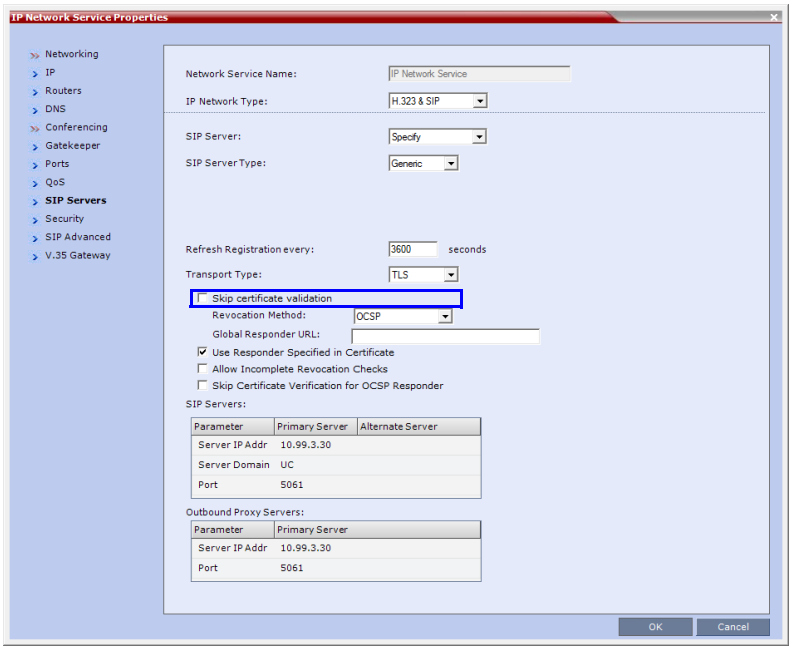
For all certificates, both *Management* and *SIP TLS*:

- Once the certificate is sent a message is displayed indicating successful installation of the certificate and the new certificate replaces the old certificate.
- If the certificate installation fails the old certificate continues to function and a message is displayed indicating one of the following the reasons for the failure:
  - Invalid password.
  - Certificate expired.
  - Certificate *DNS* name does not match *RMX* (service) *DNS* name.
  - Chain is not trusted
  - General - <Error message from the *SSL* library>.

Certificate Validation Option

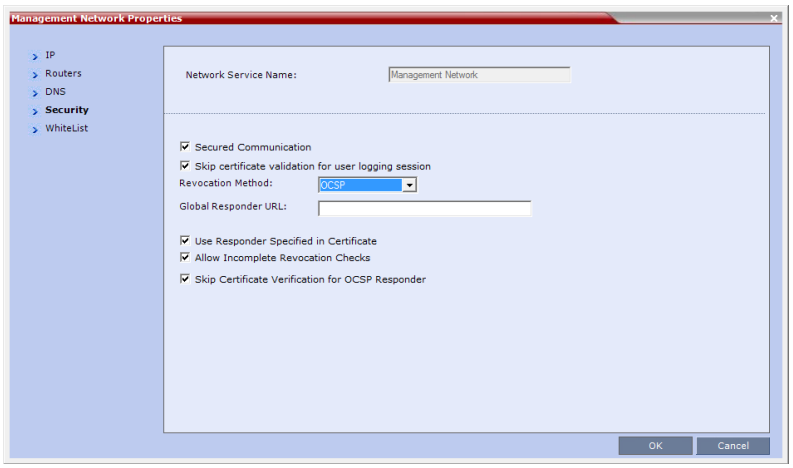
Validation of peer *SIP TLS* certificates against one or several installed *CA* certificates can be enabled or disabled for the *Default Management* and each defined *IP Service* by selecting or clearing the *Skip certificate validation* check box.

The check box is checked by default to *Skip certificate validation for user logging session* and no validation of expiration, *CA* signature or *CRL/OCSP* checking is performed.



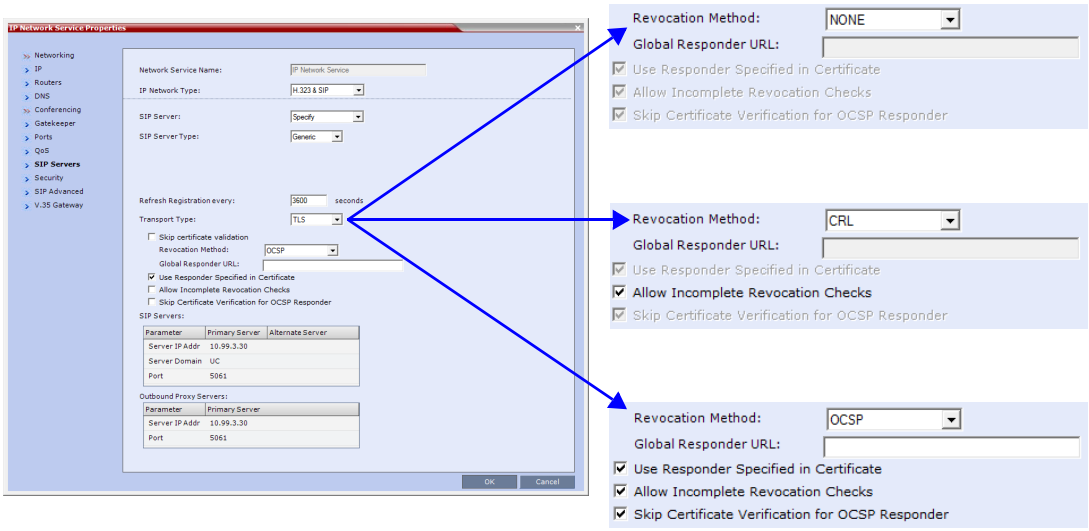
Clearing the check box enables full validation requires that there be at least one *CA* certificate in the *certificate repository*, failing which a message *At least one CA certificate should be installed* is displayed.

If the *Secured Communication* option is unchecked in the *Management Network - Security* tab all *Certificate Validation* and *Revocation* fields are disabled.



Certificate Revocation

Certificate Revocation of *IP Network* and peer *SIP TLS* certificates for each defined *IP Service* can be enabled, disabled and configured:



Revocation Method

One of three *Certificate Revocation Methods* can be selected:

- ***NONE*** (Default) - *Certificate Revocation* is not implemented.
- **CRL** - Requires at least one *CRL* file be installed, failing which an error message, *At least one CRL should be installed*, is displayed.
- **OCSP** - When selected, additional configuration options are displayed.
  - *Global Responder URL*
    - The format of the URL is validated and must be of the format: `http(s)://responder.example.com/ocsp`
    - The *URL* can be either *http* or *https*.
    - If the *Global Responder URL* does not respond an *Active Alarm* is raised.
  - *Use Responder Specified in Certificate*
    - The default for this check box is unchecked.
    - **If the check box is checked** *Responder URL* is taken from the certificate. If the certificate does not contain a *Responder URL*, the *Global Responder URL* is used.
    - **If the check box is unchecked** the *Global Responder URL* is used. If the *Global Responder URL* is incorrectly configured a message, *Global responder URL must be configured*, is displayed.
  - *Allow Incomplete Revocation Checks*

    If *OCSP* is selected:
    - If the check box is checked and the *Global Responder* or the *Responder Specified in the Certificate* does not respond for any reason the certificate is not considered revoked.
    - If the check box is unchecked and the *Global Responder* or the *Responder Specified in the Certificate* does not respond for any reason the certificate is considered revoked.

If *CRL* is selected:

- If the check box is checked and the *CRL* of the specific *CA* is not loaded, all *Certificates* are the *CA* are not considered revoked.
- If the check box is unchecked and the *CRL* of the specific *CA* is not loaded, all *Certificates* are the *CA* are considered revoked.

— *Skip Certificate Validation for OSCP Responder*

- No *Certificate Validation* is performed.

- **System Flag:**

  Should intermittent login problems occur when logging in to the *RMX's Management Network*, the **OCSP_RESPONDER_TIMEOUT** *System Flag* can be manually added to *system.cfg* and its value set to the number of seconds the *RMX* is to wait for an *OCSP* response from the *OCSP Responder* before failing the connection.

  Default: 3 (seconds)

  Range: 1-20 (seconds)

PKI Self-signed Certificate

In compliance with *UC APL* requirements, *PKI Self-signed Certificates* are supported for the both the *Default Management* and *IP Network Services*.

A mixture of *Self-signed* and *CA-signed Certificates* is supported, however a *CA-signed* certificate will always override a *Self-signed Certificate*.

Self-signed Certificate Creation

Self-signed Certificates are created during:

- Initial system start-up before any *CA-signed Certificates* have been installed.
- *IP Network Services* creation.
- *Network Services* updates that result in *Host Name* changes.
- Daily validity checks of *Self-signed Certificates*.
- *Backup* and *Restore* of the system configuration

Self-signed Certificate field values are automatically inserted when the certificate is created:

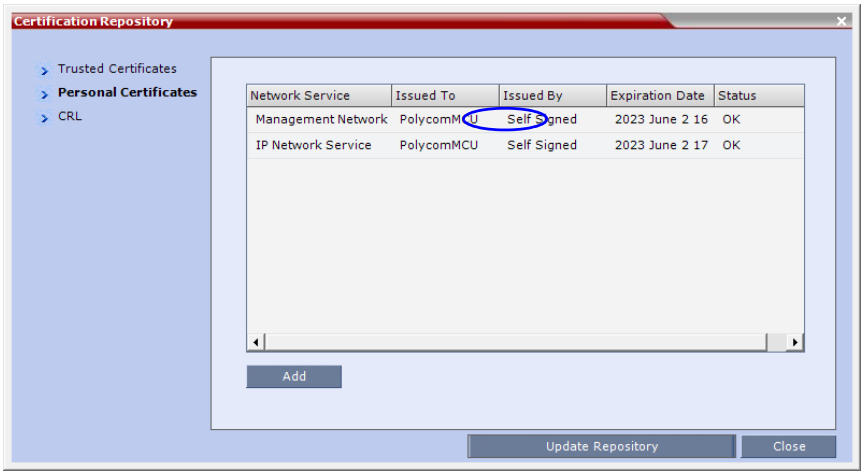
***Table 2-12** Self-signed Certificate - Creation*

Field	Value
Signature Algorithm	SHA1
Issuer / Issued To	Service Host Name Both the *Issuer* and *Issued To* fields have the same values. CN = host name of the service name DC = Polycom OU = Self Signed Certificate O = Polycom RMX **Note:** The value of *CN* is derived from the *IP Network Service Name*, while the values of *DC*, *OU* and *O* are hard coded. For a full description of these fields see *RFC 5280*.

Table 2-12 Self-signed Certificate - Creation (Continued)

Field	Value
Valid from	Date of creation
Valid to	Date of creation + 10 years
Subject (Common Name)	Service Host Name
Public Key	2048 bits

Self-signed Certificates are indicated in the *Certification Repository - Issued By* field.



Media Encryption and Authentication

In compliance with UC_APL_SEC_0013, the RMX supports an additional *Privacy Protocol* AES_CM_128_HMAC_SHA1_32, in addition to AES_CM_128_HMAC_SHA1_80.

System Flag

The *Privacy Protocol* selection is controlled by the **SRTP_SRTCP_HMAC_SHA_LENGH** *System Flag*. To modify its setting, manually add it to *system.cfg* and set its value as summarized in Table 2-13.

Range: 80, 32, 80_32

Default: 80

Table 2-13 Privacy Protocols - Flag Settings

SRTP_SRTCP_HMAC_SHA_LENGH Flag Value	Negotiation Protocol SDP	Authentication Tag Length	
		RTP	RTCP
80	AES_CM_128_HMAC_SHA1_80	80	80
32	AES_CM_128_HMAC_SHA1_32	32	80

Table 2-13 *Privacy Protocols - Flag Settings*

SRTP_SRTCP_HMAC_SHA_LENGH Flag Value	Negotiation Protocol SDP	Authentication Tag Length	
		RTP	RTCP
80_32	*First:* AES_CM_128_HMAC_SHA1_32 Second*:* *AES_CM_128_HMAC_SHA1_80*	32 or 80 (Depending on negotiation result)	80

SIP TCP Keep-Alive

In compliance with *UC APL* requirements, the *NAT Keep Alive* method has been enhanced according to *IETF RFC 5626* and *RFC 6223*.

For a full description of *Keep Alive* see *IETF RFC 5626* and *IETF RFC 6223*.

Keep Alive behavior is defined for each *IP Network Service* and can be modified by adding the following *System Flags* and modifying their values according to Table 2-14.

For more information seethe *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "IP Network Service Definition"* on page **1-66**.

Table 2-14 *System Flags - SIP_TCP_KEEPALIVE_TYPE / BEHAVIOR*

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

	RFC5626
	• In the SIP Header, the Flow-Timer Header Field is mandatory.
	• *Keep Alive* messages are sent only after successful registration. A *Pong* response is expected and if none is received, the value of the **SIP_TCP_KEEP_ALIVE _BEHAVIOR** *System Flag* is checked.
	If its value is: DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE:
	  • For a *Register Dialog,*a *Reregister Message* is sent. There is no disconnection.
	  • For a *Call Dialog*, no further messages are sent. There is no disconnection.
	If its value is: RE_REGISTRATION_WHEN_NO_PONG_RESPONSE:
	  • Both *Register* and *Call Dialogs* are disconnected.

	RFC6223
	• Behavior is the same as for *RFC5626* with the following differences:
	  • In the *SIP Header*, the *Via Header "keep"* is mandatory.
	  • In the *SIP Header*, the *Flow-Timer Header Field* is optional.

	PLCM (Default when *Generic SIP Server Type* is selected for the *Network Service*).
	• For *Call* and successful *Register Dialogues*:
	  • Two *CR LF* character sequences are sent
	  • No *PONG* response is expected

Table 2-14 System Flags - SIP_TCP_KEEPALIVE_TYPE / BEHAVIOR (Continued)

Flag	Possible Flag Values
SIP_TCP_KEEP_ALIVE_BEHAVIOR	If the value of the *System Flag*, **SIP_TCP_KEEPALIVE_TYPE = RFC5626** or **RFC6223** and no *Pong* is received, the value of this *System Flag* is checked. Possible Values: • RE_REGISTRATION_WHEN_NO_PONG_RESPONSE • DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE (Default) For a full description see the description for the ***SIP_TCP_KEEPALIVE_TYPE*** *flag (above).*

Keep Alive Frequency

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

If the RMX is functioning as the server, the *Keep Alive* frequency is set according to the hard coded values listed in Table 2-15.

Table 2-15 Keep Alive - Frequency

Field	Seconds
SIP_TCP_KEEPALIVE_DISABLE	None
SIP_TCP_KEEPALIVE_MS	300
SIP_TCP_KEEPALIVE_5626	60
SIP_TCP_KEEPALIVE_6223	
SIP_TCP_KEEPALIVE_PLCM	

SNMP

SNMP enables managing and monitoring of the MCU status by **external** managing systems, such as HP OpenView or through web applications.

Guidelines

- *IPv4* and *IPv6* are supported.
- The implementation of *SNMPv3* is *FIPS 140* compliant.
- In *Ultra Secure Mode*:
  - *Version 3* is the default for both *SNMP Agent Version* and *SNMP Trap Version*.
  - The default *Authentication Protocol* is *SHA*
  - The default *Privacy Protocol* is *AES*.

MIBs (Management Information Base)

MIBs are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB.

The SNMP systems poll the MCU according to the MIB definitions.

MIB Files

The H.341 standard defines the MIBs that H.320 and H.323 MCUs must comply with. In addition, other MIBs should also be supported, such as MIB-II and the ENTITY MIB, which are common to all network entities.

The MIBs are contained in files in the *SNMP MIBS* sub-directory of the RMX root directory. The files should be loaded to the SNMP external system and compiled within that application. Only then can the SNMP external application perform the required monitoring tasks.

The MULTI-MEDIA_MIB_TC must be compiled before compiling the other MIBs.

Private MIBs

- *RMX-MIB (RMX-MIB.MIB)*
  - — Contains the statuses of the RMX: Startup, Normal and Major.
  - — Contains all the Alarms of the RMX that are sent to the SNMP Manager.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported:

Section	Object Identifier
system	mib-2 1
interfaces	mib-2 2
ip	mib-2 4

The Alarm-MIB

This MIB is used to send alarms. When a trap is sent, the Alarm-MIB is used to send it.

The following alarms are supported:

Alarm	Description
Power Cycle - Cold Restart	The sending *Agent* is re initializing itself, usually because of a reboot.
Software - Warm Restart	The sending *Agent* is re initializing itself, usually because of a normal restart.
Link Disconnect -Link Down	One of the communication links on the *Agent Node* has failed. The first element in the variable bindings contains the name and value of the *ifIndex* instance for the interface that is down

Alarm	Description
Link Reconnect - Link Up	One of the communication links on the *Agent Node* has become active. The first element in the variable bindings is the name and value of the *ifIndex* instance for the affected interface

H.341-MIB (H.341 – H.323)

- Gives the address of the gatekeeper.
- Supports H.341-MIB of SNMP events of H.323.

Standard MIBs

This section describes the MIBs that are included with the RMX. These MIBs define the various parameters that can be monitored, and their acceptable values.

MIB Name	Description
MULTI-MEDIA-MIB-TC (MULTIMTC.MIB)	Defines a set of textual conventions used within the set of Multi Media MIB modules.
H.320ENTITY-MIB (H320-ENT.MIB)	This is a collection of common objects, which can be used in an H.320 terminal, an H.320 MCU and an H.320/H.323 gateway. These objects are arranged in three groups: Capability, Call Status, and H.221 Statistics.
H.320MCU-MIB (H320-MCU.MIB)	Used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The *Conference* group consists of the active conferences. The *Terminal* group is used to describe terminals in active MCU conferences. The *Controls* group enables remote management of the MCU.
H323MC-MIB (H323-MC.MIB)	Used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The *Conference* group is used to identify the active conferences in the MCU. The *Notifications* group allows an MCU, if enabled, to inform a remote management client of its operational status. **Note:** The RMX supports only one field in H.341-H323MC MIB. The RMX reports the Gatekeeper address using H.341-H323MC MIB – 323McConfigGatekeeperAddress (0.0.8.341.1.1.4.2.1.1.4) in response to a query from a manager.
MP-MIB (H323-MP.MIB)	Used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The *Configuration* group is used to identify audio/video mix configuration counts. The *Conference* group describes the audio and video multi-processing operation.
MIB-II/RFC1213-MIB (RFC1213.MIB)	Holds basic network information and statistics about the following protocols: TCP, UDP, IP, ICMP and SNMP. In addition, it holds a table of interfaces that the Agent has. MIB-II also contains basic identification information for the system, such as, Product Name, Description, Location and Contact Person.

MIB Name	Description
ENTITY-MIB (ENTITY.MIB)	Describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.
IP MIB (RFC 4293)	IP MIB supports both IPv4 & IPv6 entities. For a full description of the IP MIB see IETF RFC 4293.

Unified MIB

Note: This information is subject to change. The information below is not final.

The RMX uses the Polycom Unified MIB, in addition to the RMX specific MIB. The Polycom Unified MIB is an MIB that is used by many Polycom products. The following table describes the information provided by the RMX in the Unified MIB.

Name	Type	Description
Debug	Boolean	Indicates whether the unit is in a debugging state.
IncomingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to receive incoming H.323 calls.
OutgoingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to make outgoing H.323 calls.
HDBitrateThrshld	Integer	The minimum bit rate required by endpoints in order to connect to an HD conference.
MaxCPRstln	Integer	Maximum resolution of a CP conference.
MaxCPRstlnCfg	Integer	Configured resolution for a CP conference.
EndpointDispayName	String	The name of the MCU that is displayed on the screen of endpoints that are connecting to the conference.
PALNTSC	NTSC/PAL/ AUTO	The video encoding of the RMX.
SeparateMgmtNet	Boolean	Indicates whether management network separation is enabled.
NumPorts	Integer	Total number of ports.
NumVideoPorts	Integer	Number of ports configured for video.
ServiceH323	Integer	Indicates the status of H.323 capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceSIP	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.

Name	Type	Description
ServiceISDN	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
RsrcAllocMode	Fixed/ Flexible	The resource allocation method which determines how the system resources are allocated to the connecting endpoints.
McuSystemStatus	Integer	System State.
FanStatus	Boolean	Status of the hardware fan.
PowerSupplyStatus	Boolean	Status of the power supply.
IntegratedBoardsStatus	Boolean	Status of the integrated boards.
UltraSecureMode	Boolean	Indicates whether the RMX is operating in Ultra Secure Mode.
ChassisTemp	Integer	The temperature of the chasis.
NumPortsUsed	Integer	Number of ports currently in use.
NewCallsPerMinute	Integer	New calls in the last minute.
ScsfNewCallsPerMinute	Integer	Successful new calls in the last minute.
FldNewCallsPerMinute	Integer	Failed new calls in the last minute.
PctScsflNewCalls	Integer	Percentage of new calls in the last minute which were successful.
CallsEndedScsflPerMin	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailedPerMin	Integer	Number of calls in the last minute which ended with a failure code.
CallsEndedScsfl	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailed	Integer	Number of calls in the last minute which ended with a failure code.
NumActvCnfrncs	Integer	Number of active conferences.

Traps

The MCU is able to send Traps to different managers. Traps are messages that are sent by the MCU to the SNMP Manager when an event such as MCU Reset occurs.

Guidelines

- *Version 1, Version 2* and *Version 3* traps are supported.
- When *SNMPv3* is selected only *SNMPv3 Queries* and *Traps* receive responses.

- A mixture of *Version 1, Version 2* and *Version 3* traps is not permitted.

Three types of traps are sent as follows:

1 ColdStart trap. This is a standard trap which is sent when the MCU is reset.

```
coldStart notification received from: 172.22.189.154 at 5/20/
  2007 7:03:12 PM
  Time stamp: 0 days 00h:00m:00s.00th
  Agent address: 172.22.189.154 Port: 32774 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Enterprise: enterprises.8072.3.2.10
  Bindings (3)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:00m:00s.00th
    Binding #2: snmpTrapOID.0 *** (oid) coldStart
```

Figure 1 *An Example of a ColdStart Trap*

2 Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

```
authentication Failure notification received from:
  172.22.189.154 at 5/20/2007 7:33:38 PM
  Time stamp: 0 days 00h:30m:27s.64th
  Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Enterprise: enterprises.8072.3.2.10
  Bindings (3)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:30m:27s.64th
    Binding #2: snmpTrapOID.0 *** (oid) authenticationFailure
```

Figure 2 *An Example of an Authentication Failure Trap*

3 Alarm Fault trap. The third trap type is a family of traps defined in the POLYCOM-RMX-MIB file, these traps are associated with the RMX active alarm and clearance (proprietary SNMP trap).

```
rmxFailedConfigUserListInLinuxAlarmFault notification received
  from: 172.22.189.154 at 5/20/2007 7:04:22 PM
  Time stamp: 0 days 00h:01m:11s.71th
  Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Bindings (6)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:01m:11s.71th
    Binding #2: snmpTrapOID.0 *** (oid)
    rmxFailedConfigUserListInLinuxAlarmFault
    Binding #3: rmxAlarmDescription *** (octets) Insufficient
    resources
    Binding #4: rmxActiveAlarmDateAndTime *** (octets)
    2007-6-19,16:7:15.0,0:0
    Binding #5: rmxActiveAlarmIndex *** (gauge32) 2
    Binding #6: rmxActiveAlarmListName *** (octets) Active
    Alarm Table
*   Binding #7: rmxActiveAlarmRmxStatus *** (rmxStatus) major
```

Figure 3 An Example of an Alarm Fault Trap

Each trap is sent with a time stamp, the agent address, and the manager address.

Status Trap

The MCU sends status traps for the status **MAJOR** - a trap is sent when the card/MCU status is MAJOR.

All traps are considered "MAJOR".

Defining the SNMP Parameters in the RMX

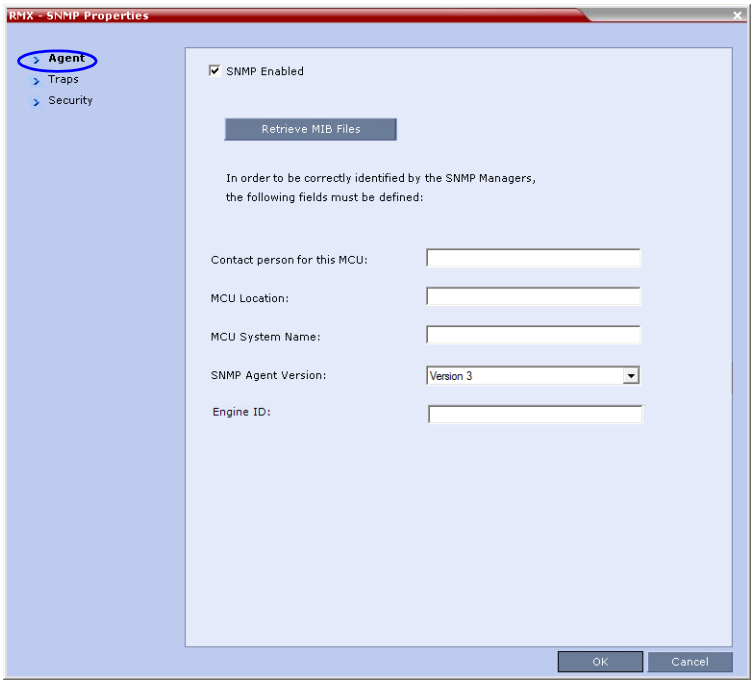
The SNMP option is enabled and configured using the *RMX Web Client* application.

The addresses of the Managers monitoring the MCU and other security information are defined in the *RMX Web Client* application and are saved on the MCU's hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the *RMX Web Client* application.

To enable SNMP option:

1 In the *RMX Web Client* menu bar, click **Setup > SNMP**.

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



This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

2 In the *Agent* dialog box, click the **SNMP Enabled** check box.

3 Click the **Retrieve MIB Files** button to obtain a file that lists the MIBs that define the properties of the object being managed.

The *Retrieve MIB Files* dialog box is displayed.

4 Click the **Browse** button 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 box.

6 Click the **Save** button.
The MIB files are saved to the selected directory.

7 Click **Close** to exit the *Retrieve MIB Files* dialog box.

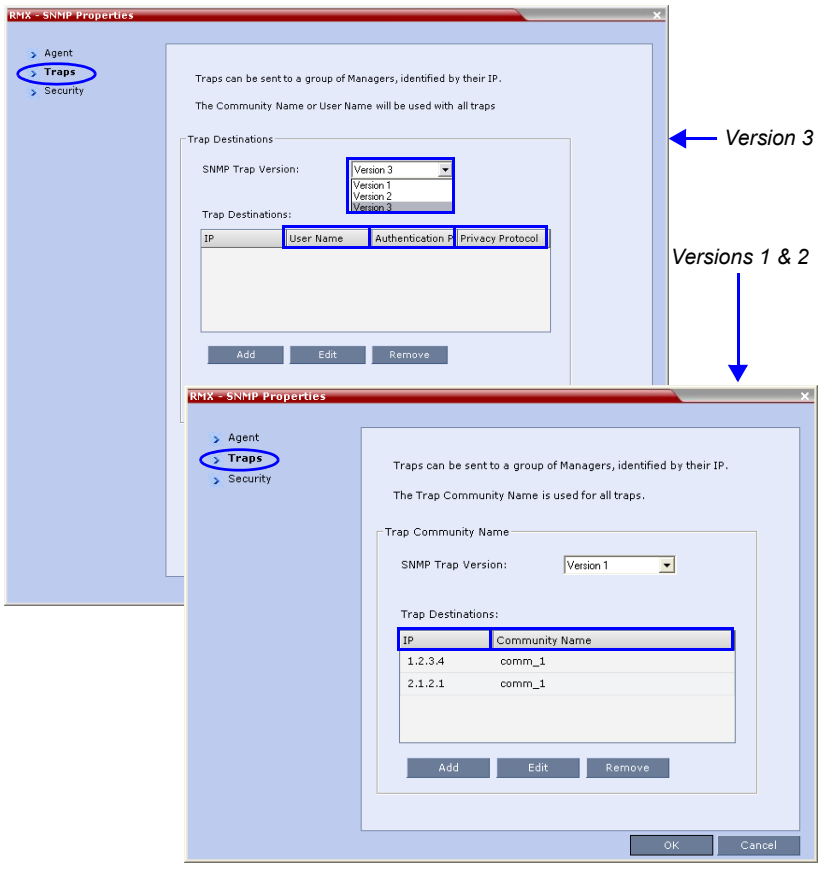
8 In the *Agent* dialog box, define the parameters that allow the SNMP Management System and its user to easily identify the MCU.

Table 2-16 *RMX-SNMP Properties - Agent Options*

Field	Description	Version
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.	1, 2, 3
MCU Location	Type the location of the MCU (address or any description).	
MCU System Name	Type the MCU's system name.	
SNMP Agent Version	Select Version 1 / 2 / 3 from the drop-down menu.	
Engine ID	This field can be left empty, allowing the RMX to automatically generate an *Engine ID* both *Queries* and *Traps*. Optionally, the administrator can enter an *Engine ID* comprised of up to 27 ASCII characters.	3

9 Click the **Traps** tab.

The *SNMP Properties – Traps* dialog box opens.



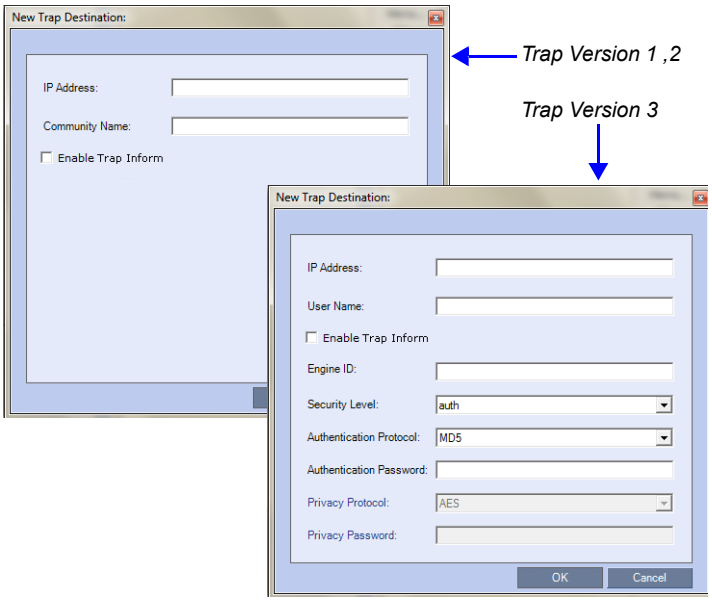
Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the *Trap Destinations* box.

10 Select the *SNMP Trap Version*.

The version of the traps being sent to the IP Host. The standard *SNMP Version 1, 2* and *3* traps, are taken from *IETF RFC 1215*. The *SNMP Trap Version* parameters must be defined identically in the external *SNMP* application.

11 Click the **Add** button to add a new *Manager* terminal.

Depending on the *SNMP Trap Version* selected, one of the two following *New Trap Destination* dialog boxes opens.



12 Define the following parameters:

Table 2-17 *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

***Table 2-17** SNMPv3 - Traps (Continued)*

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.

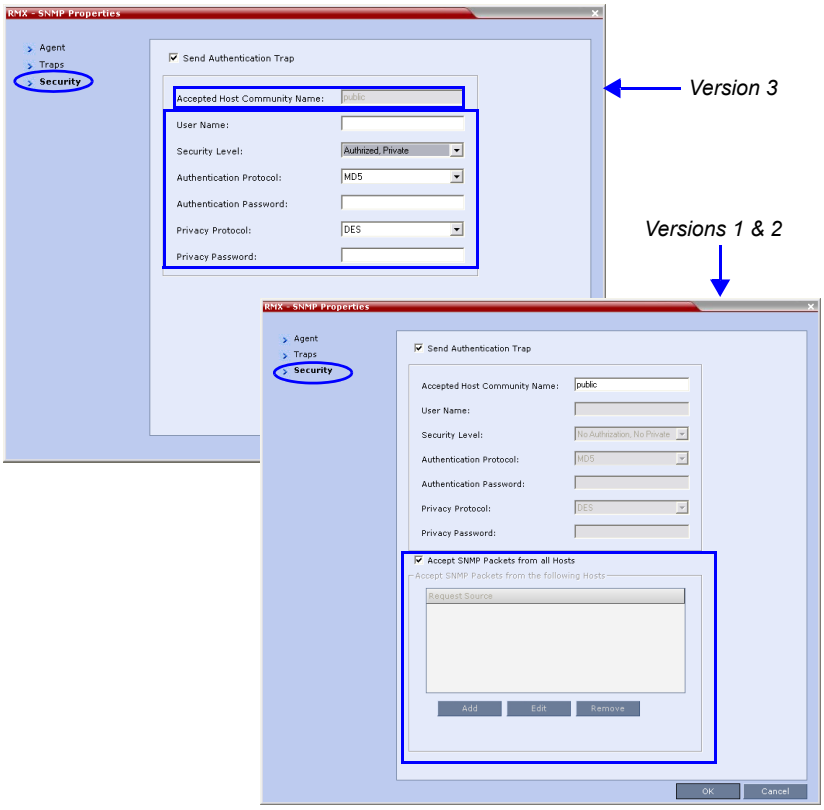
The new *IP Address* and *Community name* is added to the *Trap Destinations* box.

a To delete the IP Address of a Manager terminal, select the address that you wish to delete, and then click the **Remove** button.

The IP address in the *Trap Destinations* box is removed.

14 Click the **Security** tab.

The *RMX-SNMP Properties – Security* dialog box opens.



This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. When the *"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 box.

15 Define the following parameters:

Table 2-18 *SNMP - Security*

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, 3

Table 2-18 *SNMP - Security (Continued)*

Field	Description		
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 will be regarded as a violation of security, and, if the Send Authentication Trap check box is selected, an appropriate message will be sent to the SNMP Manager.		Versions 1, 2
Accept SNMP Packets from all Host	Select this option if a query sent from any Manager terminal is valid. When selected, the Accept SNMP Packets from These Hosts option is disabled.		
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		Version 3
Security Level	Select a *Security Level* from the drop-down menu. **Range:** *No Auth, No Priv; Auth, No Priv; Auth, Priv* **Default:** Auth, Priv		
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		

16 To specifically define one or more valid terminals, ensure that the *Accept SNMP Packets from any Host* option is cleared and then click the **Add** button.

The *Accepted Host IP Address* dialog box opens.

17 Enter the *IP Address* of the Manager terminal from which valid queries may be sent to the MCU, and then click **OK**.
Click the **Add** button to define additional *IP Addresses*.
The *IP Address* or *Addresses* are displayed in the *Accept SNMP Packets from These Hosts* box.

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 the *Send Authentication Trap* check box is selected, an appropriate message will be sent to all the terminals listed in the *SNMP Properties – Traps* dialog box.

18 In the *RMX - SNMP Properties - Security* dialog box, click **OK**.

Version 8.1.4.J Detailed Description - New Features

New Video Resolution 1080p60

This version adds the option of *HD1080p* resolution at 60 fps for improved resolution of motion video. In previous versions the highest resolution at 60 fps was *HD720p*.

Guidelines

HD1080p60 is supported:

- With *MPMx* cards only.
- In *Continuous Presence* (*CP*) mode:
  - At bit rates of up to 4Mbps.
  - *HD1080p60* is supported asymmetrically: The RMX receives *HD720p60* and sends *HD1080p60*.
  - *HD1080p60* is only selectable when *Video Quality* is set to **Motion.**
    System behavior when *Video Quality* is set to **Sharpness** is unchanged.
- In *Video Switching* (*VSW*) mode:
  - At bit rates of up to 6Mbps.
  - *HD1080p60* is supported symmetrically: The RMX receives and sends *HD1080p60*.
- In *Telepresence* environments the RMX sends *HD1080p60* to all endpoints except for those with *1x1 Video Layouts*, which receive the same resolution and frame rate from the RMX as they send. TIP endpoints are not supported
- PAL endpoints are supported at a frame rate of 50 fps.
- Each *HD1080p60* participant consumes 9 system resources.
  (For comparison: Each *HD720p60* participant consumes 6 system resources.)

HD1080p60 is not supported:

- For *ISDN* participants.
- For *Content* sharing.
- With *RTV*

CP Resolution Decision Matrix

All the CP resolution options and settings are based on a decision matrix which matches video resolutions to connection line rates, with the aim of providing the best balance between resource usage and video quality at any given line rate.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "The CP Resolution Decision Matrix"* on page **2-4**.

H.264 Base Profile and High Profile Comparison

The following illustrations show a comparison between the resolutions used at various line rates for *H.264 Baseline* and the *H.264 High Profile,* for the *Motion Video Quality* setting according to the following *Resolution Configuration Modes:*

- *Resource-Quality Balanced*
- *Resource Optimized*
- *Video Quality Optimized*

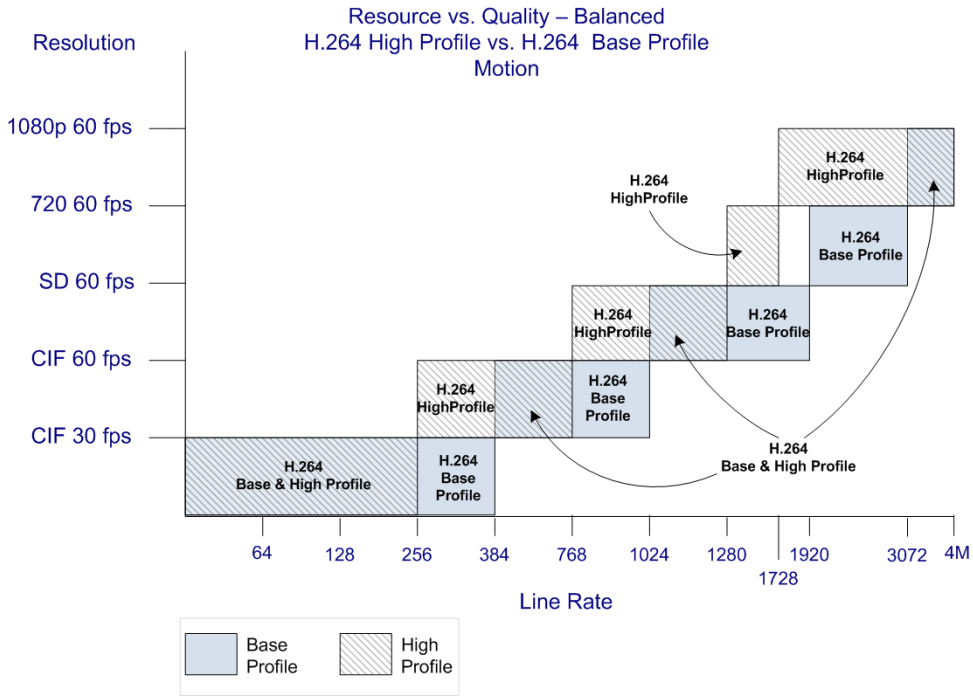


Figure 2-1 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource-Quality Balanced*

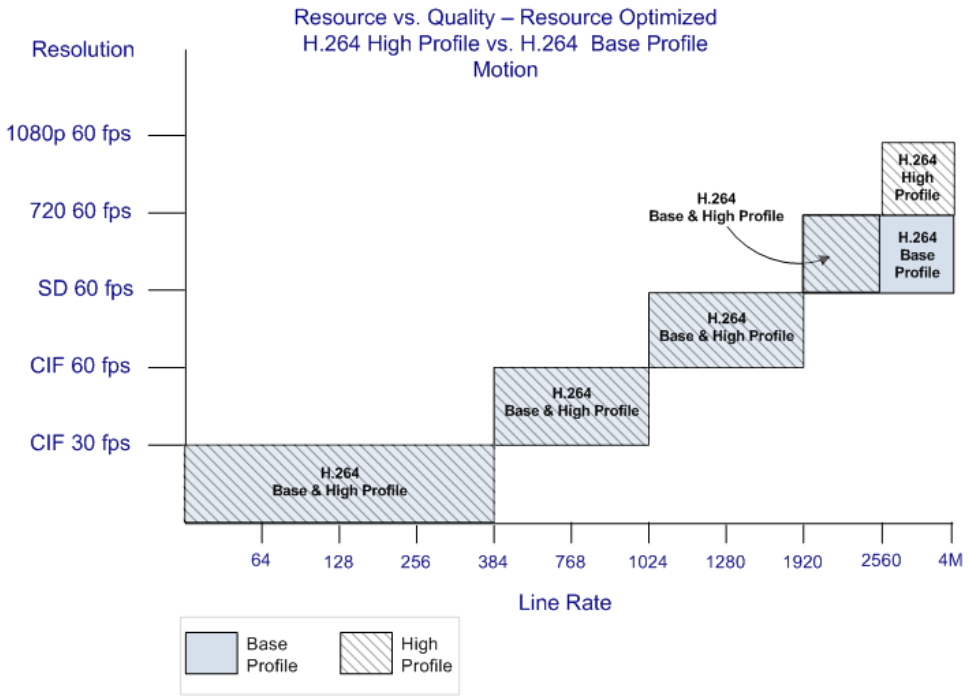


Figure 2-2 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource Optimized*

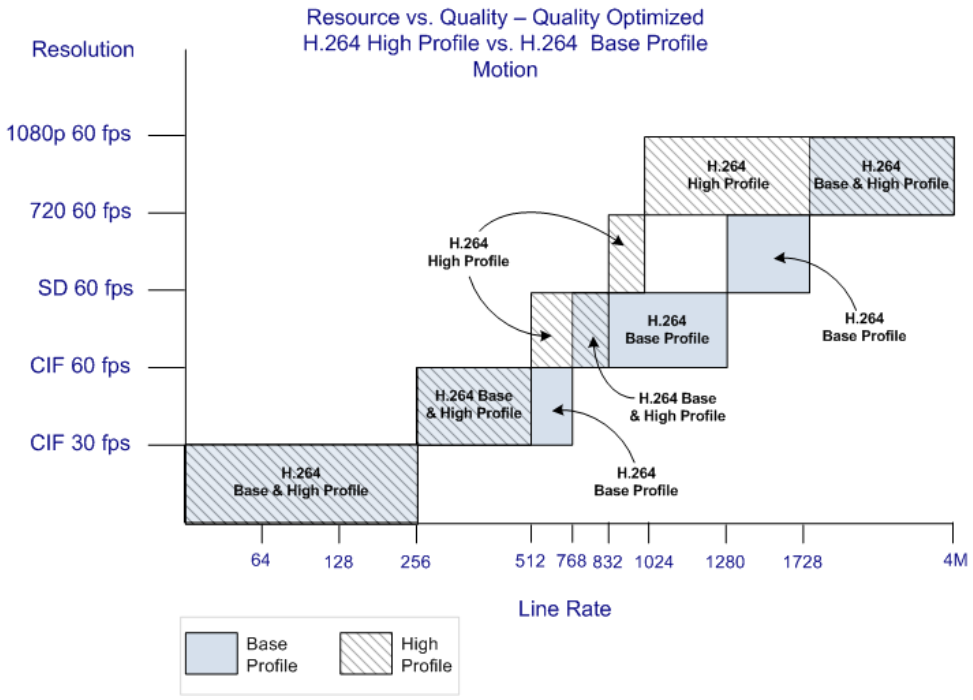


Figure 2-3 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Video Quality Optimized*

Default Minimum Threshold Line Rates and Resource Usage Summary

HD1080p60 Resolution is included in the following table summarizing the *Default Minimum Threshold Line Rates* and *Video Resource* usage for each of the pre-defined optimization settings for each *Resolution*, *H.264 Profile*, *Video Quality* setting (*Sharpness* and *Motion)* for *MPMx Card Configuration Mode*.

MPMx			Resource-Quality Balanced (Default)				Resource Optimized				Video Quality Optimized			
			Sharpness		Motion		Sharpness		Motion		Sharpness		Motion	
		Profile →	High	Base	High	Base	High	Base	High	Base	High	Base	High	Base
Default Minimum Threshold (kbps) by Resolution, Profile, Resources	HD1080p60	Line Rate			1728	3072			2560	4096			1024	1728
		Resources	9				9				9			
	HD1080p30	Line Rate	1536	4096			4096	4096			1024	1728		
		Resources	6				6				6			
	HD720p60	Line Rate			1280	1920			1920	1920			832	1280
		Resources	6											
	HD720p30	Line Rate	768	1024			1920	1920			512	832		
		Resources	3				3				3			
	SD60	Line Rate			768	1024			1024	1024			832	1280
		Resources	3				3				3			
	SD30	Line Rate	256	256			384	384			256	256		
		Resources	1.5				1.5				1.5			
	CIF60	Line Rate			256	384			384	384			256	256
		Resources	1.5				1.5				1.5			
	CIF30	Line Rate	64	64	64	64	64	64	64	64	64	64	64	64
		Resources	1				1				1			

Enabling HD1080p60

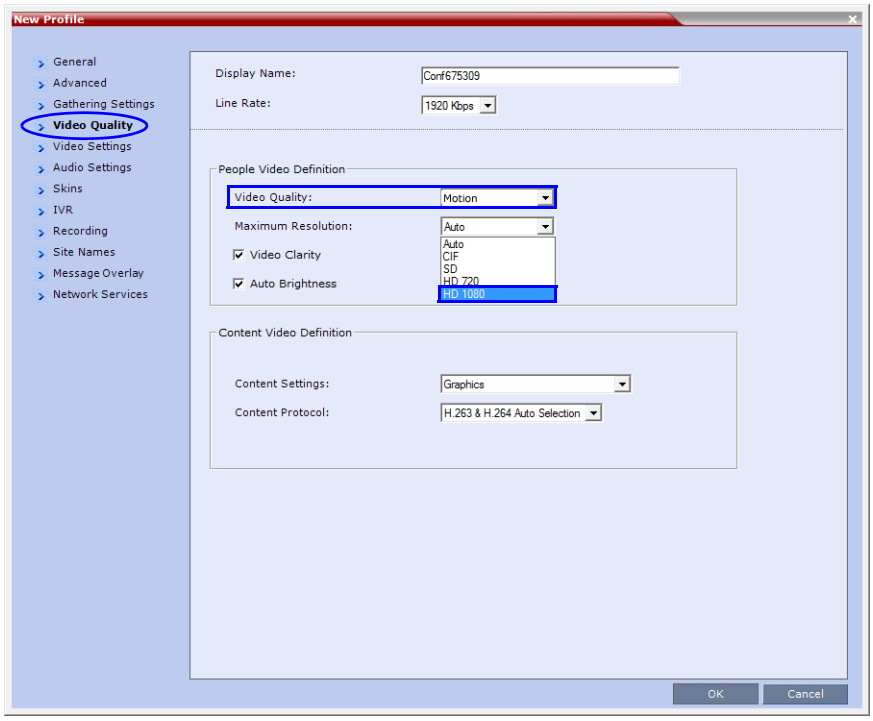
HD1080p60 is enabled and configured using the *New Profile - Video Quality* dialog box and the *Basic* and *Detailed Resolution Configuration* dialog boxes:

- An additional option, HD1080, has been added to the Maximum Resolution drop-down menu of the New Profile - Video Quality dialog box.
- An additional radio button HD1080p60 has been added to the Basic and Detailed Resolution Configuration dialog boxes.

To enable HD1080p60:

1. In the *New Profile - Video Quality* tab:
   a. Select **Motion** in the *Video Quality* drop-down menu.
   b. Select **HD1080** in the *Maximum Resolution* drop-down menu.

HD1080 must be selected as the *Maximum Resolution* before *HD1080p60* can be selected using the *Resolution Configuration* dialog boxes.

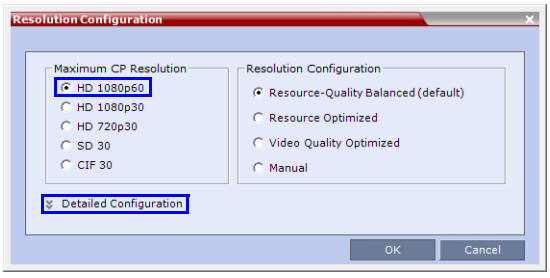


All other *Conference Profile* fields and their settings are described in detail in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide* "*Defining New Profiles*" on page **2-20**.

2 When the *Conference Profile* is complete, click **OK**.

3 In the *Resolution Configuration* dialog box:

a Click the **HD1080p60** radio button.



b **Optional**. If detailed configuration is required, click **Detailed Configuration** and complete the configuration using the sliders in the *Motion* tabs of the *Detailed Resolution Configuration* dialog boxes.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "This chapter describes Resolution Configuration in MPMx Card Configuration Mode as MPM and MPM+ cards are not supported in this version."* on page **1-138**.

4 When the *Resolution Configuration* is complete, click **OK**.

Endpoint Connection

Endpoints will connect at resolutions as set out in the following table, depending on whether they support *H.264 High Profile* or not:

Video Quality Setting	Endpoint Connection Bit Rate (kbps)		Resolution
	High Profile Supported	**High Profile Not Supported**	
Sharpness	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	SD30
	512<= bit rate <**1024**	**1024**<= bit rate <**1536**	HD720p30
	1024<= bit rate	**1536**<= bit rate	HD1080p30

Video Quality Setting	Endpoint Connection Bit Rate (kbps)		Resolution
	High Profile Supported	High Profile Not Supported	
Motion	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	CIF60
	512<= bit rate <**832**	**1024**<= bit rate <**1536**	SD60
	832<= bit rate	**1536**<= bit rate	HD720p60
			HD1080p60

System Flags

These *System Flags* must be added to the *System Configuration* file before they can be modified. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "Modifying System Flags"* on page **1-1**.

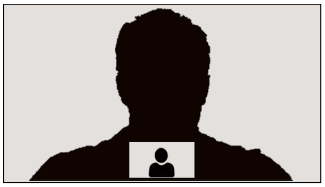
Flag	Default (kbps)	Description
H264_BASE_PROFILE_MIN_RATE_HD1080P60_MOTION	2048	Endpoints that do not support *H.264 High Profile* will connect according to the minimum bitrate thresholds defined by this *System Flag*.
VSW_HD1080p60_HP_THRESHOLD_BITRATE	1728 Minimum 1024	Controls the Minimum Threshold Line Rate (kbps) for HD1080p60 resolution for H.264 *High Profile*-enabled *VSW* conferences.
VSW_HD_1080p60_BL_THRESHOLD_BITRATE	3072 Minimum 1728	Controls the Minimum Threshold Line Rate for HD1080p60 resolution for H.264 *Base Profile*-enabled *VSW* conferences.
MAX_CP_RESOLUTION	HD1080p60fps	The flag value is applied to the system during *First Time Power-on* and after a system upgrade.

Layout Overlays

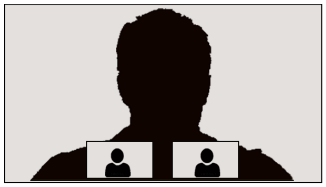
Overlay Layouts allow additional participant endpoints to be displayed in 1x1 conference *Video Layouts*.

The following *Overlay Layouts* are included in this version for use in *CP Conferences*:

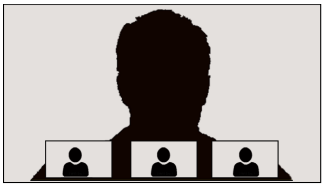
1Standalone Endpoint



2 Standalone Endpoints

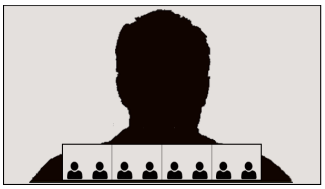


3 Standalone Endpoints



Although the following *Overlay Layout* is included in the *Profiles - Video Settings* dialog box, it is not available for use in any conferencing mode and is only available when included in the *Polycom® Multipoint Layout* (*MLA*) application:

Single Overlay Cell: 2-4 Screens



These *Overlay Layouts* will only be available in *ITP* (*Telepresence*) conferences when support for *Overlay Layouts* is included in the *Polycom® Multipoint Layout* (*MLA*) application.

Guidelines

- The *Overlay Layouts* are supported:
  - With *MPMx* cards only.
  - In RMX *CP Conferencing Mode* only.
  - With *ITP*, non-*ITP* and *CTS* endpoints used only as standard endpoints.
  - With both new and classic *Skins* in RMX *CP* mode. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide*, *"Skins"*.
- *Overlay Layouts* are not supported in *ITP* conferences as they are not supported by the *MLA* application.
- The *Overlay Layouts* are 20% of the height of the endpoint display and are supported on endpoints of both 16:9 and 4:3 aspect ratios.
- *Overlay Layouts* are recommended for use with high resolution endpoints.
- *Overlay Layouts* are not selected as defaults by the system. Default layouts are selected as in previous versions and are described in detail in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide*, *"Auto Layout – Default Layouts in CP Conferences"*.
- *Message Overlay* is not affected by the use of *Overlay Layouts* and is displayed as the top level overlay.

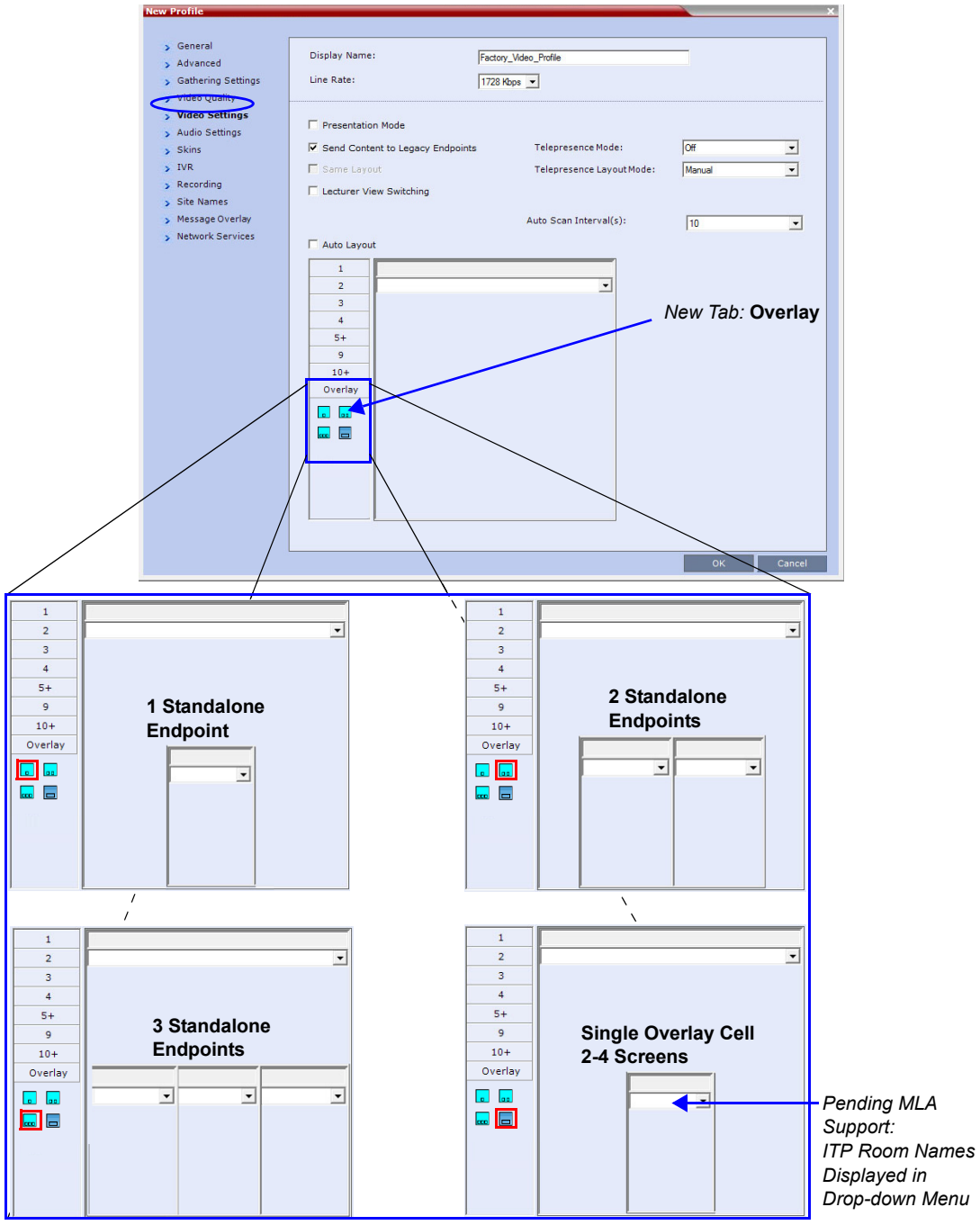
- *Vertical Position* for *Site Name* display: *Site Names* are displayed for all cells. Because the smaller cells are located at the bottom of the large cell, when enabling *Site Names* it is advisable not to locate the *Site Name* at the bottom of the cells.
- *Standalone Endpoint Cells* are displayed each with a border. For all *Overlay Layouts,* border color is dependent on the selected *Skin*.
  For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide*, "*Skins*".
- System behavior for *Video Forcing* and *Personal Layout Control* using the *Overlay Layouts* during an ongoing conference is the same as for other video layouts. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide, "Video Forcing"*.
- *Overlay Layouts* are only available for selection for the *Conference Layout* and are not available for selection for *Personal Layout*.
- *Overlay Layouts* are not available for selection when using *PCM* or *Click&View*.

PCM is not supported when the RMX is in *Ultra Secure Mode*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators's Guide*, "*Ultra Secure Mode"* and *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "PCM"*

- *PCM* menus are available when the *Overlay Layouts* are active, and they are displayed as the top level overlay

Selecting the Overlay Layouts

The *Overlay Layouts* are selected in the *New Profile - Video Settings* dialog box, in the *Overlay* tab of the *Video Layout* tree.



Non-encrypted Conference Message

When mixing encrypted and non-encrypted endpoints in a conference using the "*Encrypt When Possible*" encryption option in the *Conference Profile* the encryption status of the conference can change as encrypted and non encrypted participants connect and disconnect.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "Mixing Encrypted and Non-encrypted Endpoints in one Conference"* on page 3-27.

It is important that participants already connected, and those connecting to the conference are aware of whether the conference is encrypted or not.

An *Encryption Status Message* can be enabled by adding the *System Flags* summarized in Table 2-19 to *system.cfg* and modifying their values. Using the flags, the user can enable, disable and control the display of the conference's encryption status to both connected and connecting participants.

Table 2-19 *Encryption Status Message Flag Values*

Flag	Range / Description
DISPLAY_UNENCRYPTED_MESSAGE_TIMER_FOR_ENCRYPT_WHEN_POSSIBLE	**1 - 300**: The duration (seconds) for display of the message: **The conference is not secured** **-1**: • Display the message while there is at least one unencrypted participant in the conference. • Display the message when an unencrypted participant connects to the conference and for the duration of the connection. **0**: The message is disabled (Default).
DISPLAY_ENCRYPTED_MESSAGE_TIMER_FOR_ENCRYPT_WHEN_POSSIBLE	**1 - 300**: The duration (seconds) for display of the message: **The conference is secured** **-1**: • Display the message while there are no unencrypted participant in the conference. • Display the message when the last unencrypted participant leaves to the conference and for the duration of the connection. **0**: The message is disabled (Default).

Guidelines

- *Encryption Status Message* is supported in *CP* environments only.
- The *Encryption Status Message* is always displayed in English.
- *Encryption Status Message* is not relevant when *Encrypt All* or *No Encryption* is selected in the *Conference Profile*.
- The *Encryption Status Message* is display according to the conference's *Message Overlay* settings for *Display/Vertical Position*, *Color* and *Font Size*. It is displayed as a *Static* message.

— Table 2-20 summarizes the system behavior when and *Encryption Status* change triggers an *Encryption Status Message* while a *Conference Message Overlay* or *Message to a Selected Participant* is being displayed.

— Table 2-21 summarizes the system behavior when a *Conference Message Overlay* or *Message to a Selected Participant* is initiated while an *Encryption Status Message* is being displayed.

Table 2-20 *Conference Message Overlay / Encryption Status Message Interactio*

Change of Encryption Status				**Display**
Current Message		**New Message**		
Type	**Message Setting / Flag Value**	**Type**	**Message Setting / Flag Value**	
Conference Message Overlay or Message to Selected Participant	Static	Encryption Status Message	1 - 300	The *Conference Message Overlay* is displayed again at the end of the duration of the *Encryption Status Message*.
			-1	*Encryption Status Message* replaces the *Conference Message Overlay* and is displayed until the *Encryption Status* changes.
	Defined number of Repetitions	Encryption Status Message	1 - 300	*Encryption Status Message* replaces the *Conference Message Overlay or Participant Message* for the duration of the *Encryption Status Message.* No message is displayed unless the Encryption Status changes.
			-1	*Encryption Status Message* replaces the *Conference Message Overlay or Participant Message* for the duration of the *Encryption Status Message.* *Encryption Status Message* is displayed until the *Encryption Status* changes.

Table 2-21 *Encryption Status Message / Conference Message Overlay Interaction*

Change of Encryption Status				Display
Current Message		New Message		
Type	Message Setting / Flag Value	Type	Message Setting / Flag Value	
Encryption Status Message	-1	Conference Message Overlay or Message to Selected Participant	Defined number of Repetitions	*Message Overlay* replaces the *Encryption Status Message Overlay* and is displayed for the defined number of repetitions. The *Encryption Status Message is then displayed* until the *Encryption Status* changes.
			Static	*Message Overlay* replaces the *Encryption Status Message Overlay* and is displayed until encryption status changes.
	1 - 300	Conference Message Overlay or Message to Selected Participant	Static	*Conference Message Overlay* replaces the *Encryption Status Message* and is displayed until the *Encryption Status* changes.
			Defined number of Repetitions	*Conference Message Overlay* replaces the *Encryption Status Message f*or the defined number of repetitions. No message is displayed until the *Encryption Status* changes.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide* "*Message Overlay Tab*" on page **2-41**.

Multiple Cascading Links

This version adds support for *Multiple Cascade Links* between RMXs hosting conferences that include *Immersive Telepresence Rooms* (*ITP*) such as Polycom's OTX and RPX Room Systems.

In previous versions the video stream of only one of the *ITP* endpoints could be sent to the remote RMX.

Guidelines

- *Basic Cascading* topology is used. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Basic Cascading using IP Cascaded Link"* on page **1-242**.
- *Multiple Cascade Links* are implemented by creating a *Link Participant* which consists of a main link and sub-links which are automatically generated and sequentially numbered. For more information see"*Creating a Link Participant" on page* **102**.

- All cascaded links must use H.323 protocol.
- *Multiple Cascade Links* are supported with *MPMx* cards.
- *Multiple Cascade Links* are supported in *CP* conferencing mode.
- The number of cascading links is defined manually according to the maximum number of Room System cameras in the cascaded conference.
- When the active speaker is in an Immersive Telepresence Room, *Multiple Cascade Links* are used, one link for each of the Room System's cameras.
  - An RPX 4xx Room System requires 4 *Cascaded Links* to carry the video of its 4 cameras.
  - An RPX 2xx Room System requires 2 *Cascaded Links* to carry the video of its 2 cameras.
  - An OTX 3xx Room System requires 3 *Cascaded Links* to carry the video of its 3 cameras. The OTX Room System must be configured as *Room Switch* in order to send multiple streams. When configured in *CP Mode*, its cameras zoom out and all 3 screens are sent as one stream.
- The number of links is defined when creating the *Link Participant*. Each conference in the cascade must have a *Link Participant* with the same number of *Multiple Cascade Links* defined. Calls from *Link Participants* not defined with the same number of links are rejected. *Number of cascading links is not identical for all conferences* is listed as the *Call Disconnection Cause*. For more information see "*Creating a Link Participant*" on page **102** and "*Monitoring Multiple Cascade Links*" on page **104**.
- Although it is possible to disconnect and reconnect specific *Multiple Cascade Links* using the *RMX Web Client / RMX Manager* it not advisable to do so.
  - If the main link is disconnected all sub-links are disconnected and deleted. Reconnecting the main link reconnects all sub-links.
  - If a sub-link is disconnected it remains disconnected until it is manually reconnected.
  - The number of *Multiple Cascade Links* cannot be modified while any of the links are in a disconnected state. All previous links must be deleted before modification is possible.

    For more information see "*Monitoring Multiple Cascade Links*" on page **104**.
- A *Link Participant* can be dragged from the address book into a conference.
  - If it is the first *Link Participant* in the conference, the number of *Multiple Cascade Links* defined for the participant are created and connected.
  - If it is not the first *Link Participant* in the conference, the number of *Multiple Cascade Links* defined for the participant is ignored.
- If there are insufficient resources to connect all *Multiple Cascade Links* in either of the RMXs, none of the links are connected and *resources deficiency -0* is listed as the *Call Disconnection Cause*. For more information see "*Monitoring Multiple Cascade Links*" on page **104**.
- *Multiple Cascade Links* that are not used by MLA are inactive but continue to consume resources.
- All RMXs participating in the cascade must have the same *Telepresence Mode* definitions, either all defined as *CP* or all defined as *Room Switch*.
- When *Multiple Cascade Links* are defined in the *Conference Profile*, the *Layout Type* field of the *Link Participant*'s *Participant Properties - Media Sources* dialog box is set to **Conference** and cannot be modified.

- TIP Telepresence Rooms (CTS) are supported without *Content*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000, "Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)"* on page **1-1**.

Enabling and Using Multiple Cascade Links

The settings required to enable *Multiple Cascade Links* on the RMX are minimal and are described in "*Creating a Link Participant*" on page **102**.

Most of the layout configuration is performed using *Polycom's Multipoint Layout Application (MLA)*.

Figure 2-4 and Figure 2-5 show example layouts and media flows when MLA is configured for a cascading conference between two RMXs.

In Figure 2-4:

- The OTX Room System connects to RMX A.
- The RPX Room System connects to RMX B.
- This layout requires that the *Telepresence Layout Mode* to be set to **Room Switch** in the *Conference Profiles* of the *Cascading Conferences* in each RMX.
- The current speaker is a participant in the RPX ITP Room.
- Directional media flows, A ⇆ B, are shown separately for readability purposes.

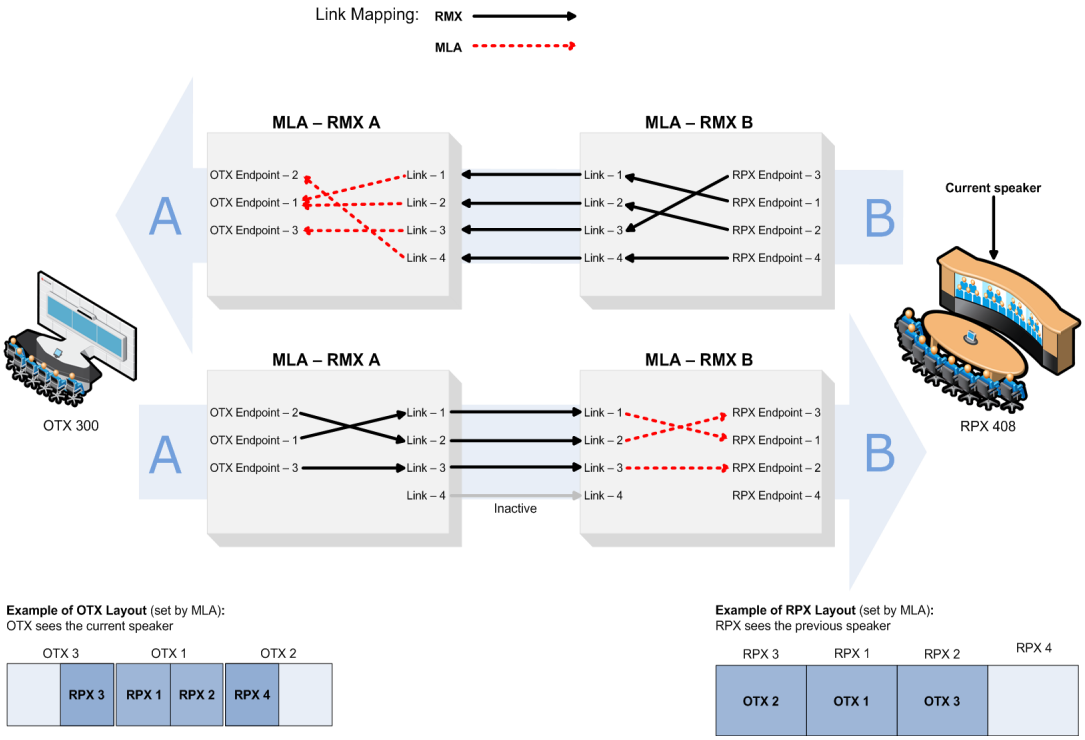


Figure 2-4 *RMX Telepresence Layout Mode - Room Switch*

In Figure 2-5:

- An HDX endpoint and an OTX Room System connects to RMX A.
- An HDX endpoint and an RPX Room System connects to RMX B.

- This layout requires that the *Telepresence Layout Mode* to be set to **Continuous Presence** in the *Conference Profiles* of the *Cascading Conferences* in each RMX.
- The current speaker is the HDX endpoint connected to RMX A.

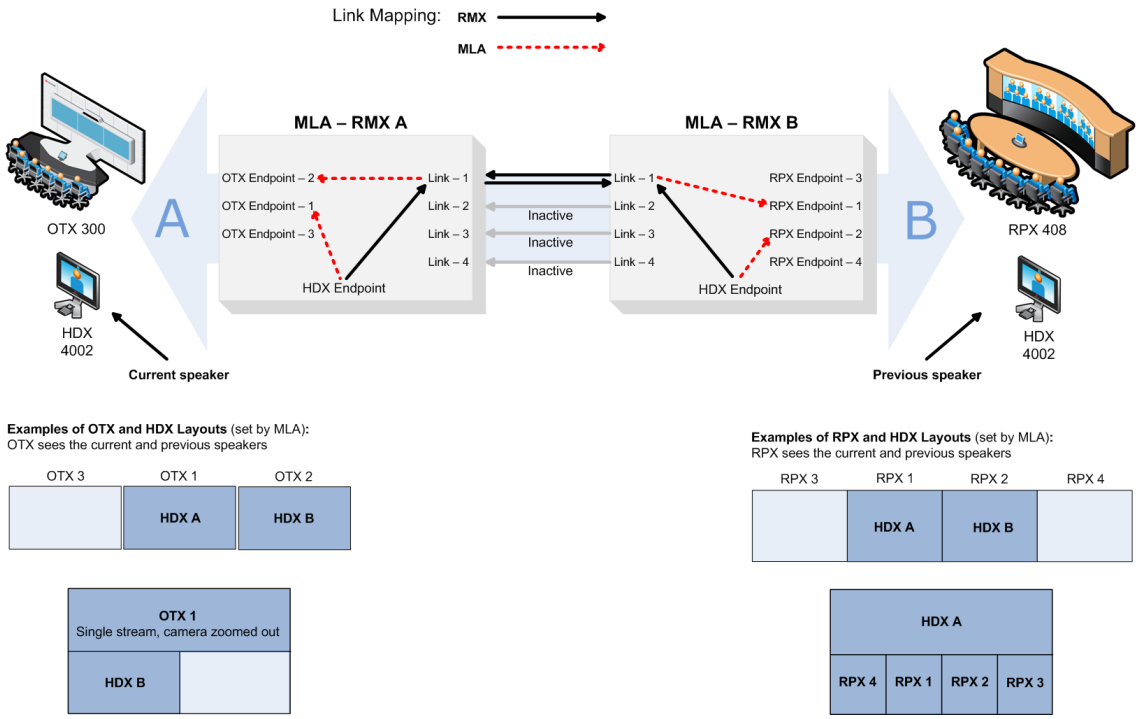


Figure 2-5 *RMX Telepresence Layout Mode - Continuous Presence*

For more information see:

- *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide, "Telepresence Layout Mode".*
- *Polycom® Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*
- *Polycom® Immersive Telepresence (ITP) Deployment Guide*

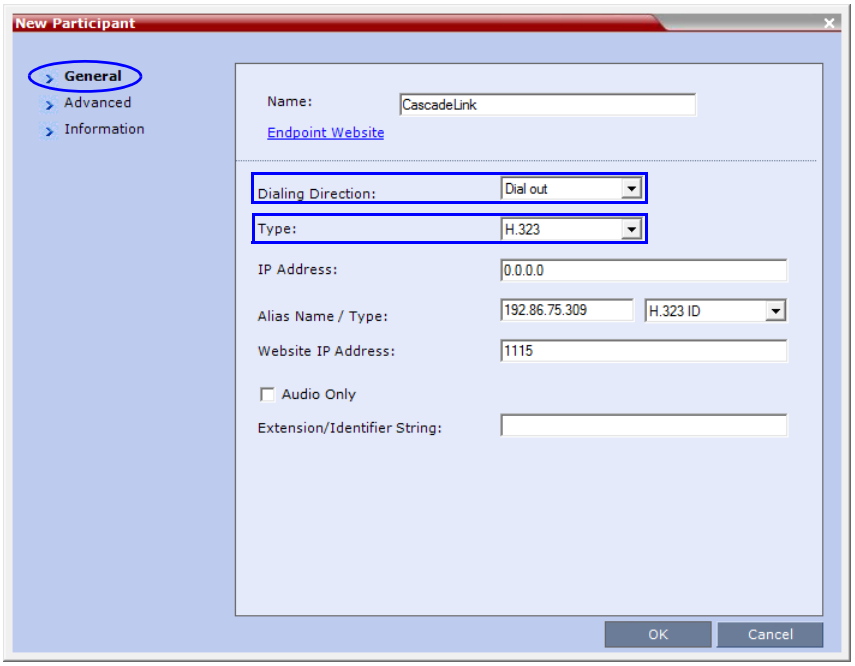
Creating a Link Participant

Link Participant in the Dial Out RMX

The *Link Participant* is defined in the *New Participant* dialog box.

In the *General* tab:

- *Dialing Direction* must be selected as **Dial out.**
- *Type* must be selected as **H.323**.



For more information see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide,* "*Creating a Cascade Enabled Dial-out/Dial-in Participant Link*" on page **5-15**.

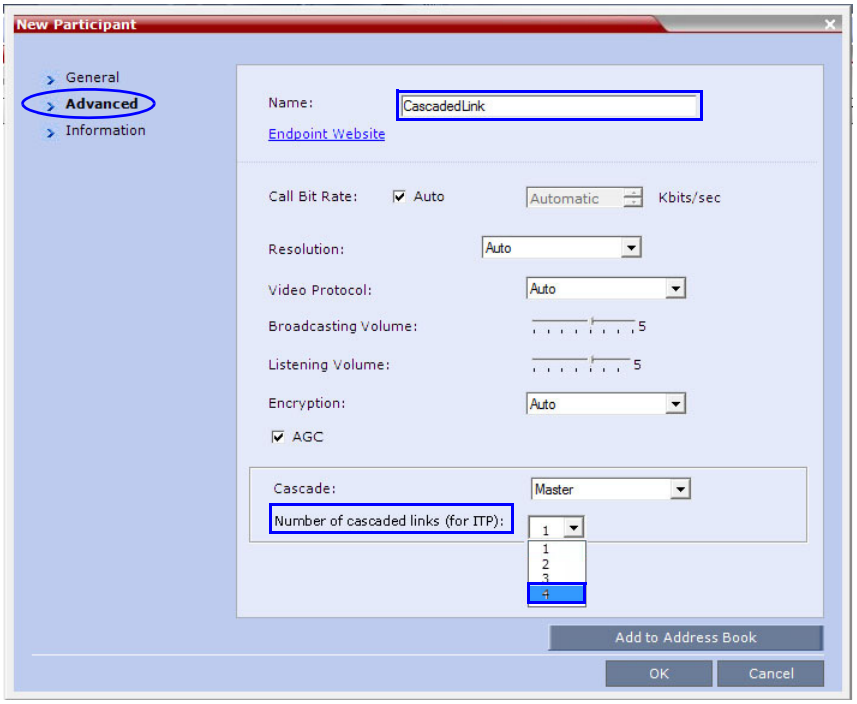
In the *Advanced* tab:

(This field is only enabled if the RMX system is licensed for *Telepresence Mode*.)

- In the *Cascade* drop-down menu, select either **Master** or **Slave**.
- In the *Number of cascaded links (for ITP)* drop-down menu, select the maximum number of *Multiple Cascade Links* required according to the number of Room System endpoints in the cascaded conference.

  This field enables the administrator to select the maximum number of *Multiple Cascade Links* required according to the number of Room System endpoints in the cascaded conference.

  For example if an *RPX 4xx* is included, the number of links required is 4.



The RMX automatically adds a number suffix to the name of the *Link Participant*, for example if the *Participant Link Name* is *CascadeLink* and the *Number of cascaded links (for ITP)* field is set to 4, the following *Multiple Cascade Links* are created:

- *CascadeLink-1*
- *CascadeLink-2*
- *CascadeLink-3*
- *CascadeLink-4*

Participant Link in the Dial In RMX

The call from *Participant Link* defined in the *Dial-out* RMX is identified by the *Dial-in* RMX as having been initiated by a *Participant Link*.

Suffixes are appended the *Multiple Cascade Links* according to the *Number of cascaded links (for ITP)* field depending on whether the *Dial -In Participant Link* is defined or un-defined:

Participant Link is un-defined:

The *Multiple Cascade Link* names are automatically assigned by the RMX.
For example on a RMX 1500 the names of the links are:

- *POLYCOM RMX 1500-1*
- *POLYCOM RMX 1500-2*
- *POLYCOM RMX 1500-3, etc.*

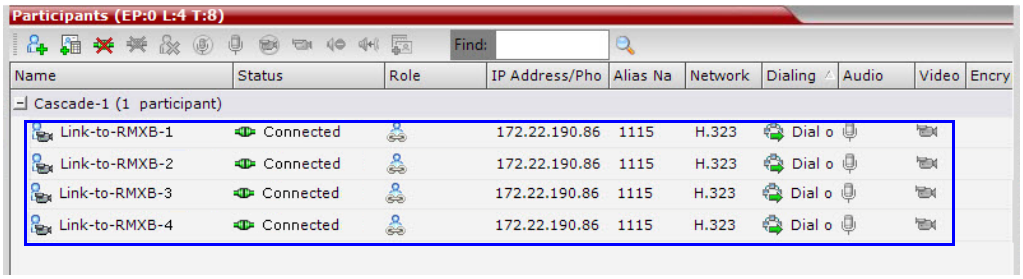
Participant Link is a defined:

The *Multiple Cascade Link* names are assigned according to the name of the defined participant that is to function as the cascade link and the *Number of cascaded links (for ITP)* information sent by the calling *Dial-Out Participant Link*.
For example if the defined participant that is to function as the cascade link is named *Cascade_Link_From_B* the names of the links are:

- *Cascade_Link_From_B-1*
- *Cascade_Link_From_B-2*
- *Cascade_Link_From_B-3, etc.*

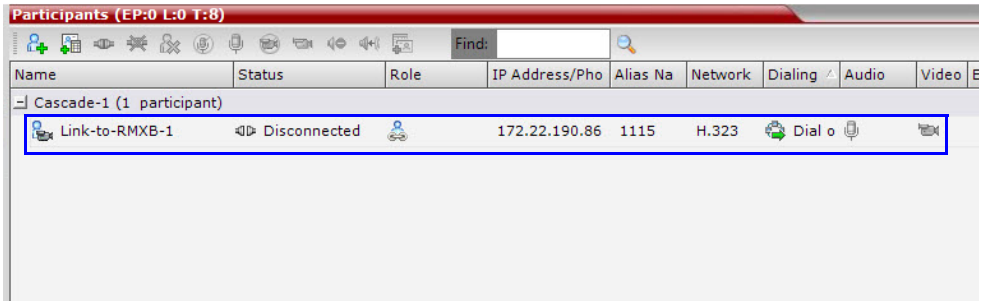
Monitoring Multiple Cascade Links

Multiple Cascade Links connections can be monitored in the *Participants* list of the *RMX Web Client / RMX Manager* main screen:

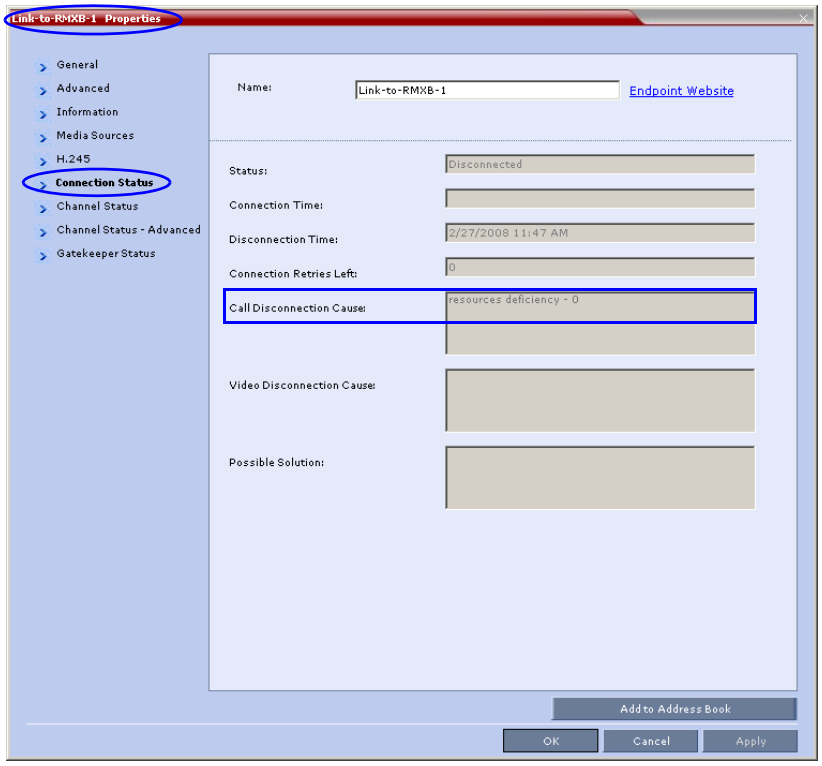


Disconnection Causes

- If there are insufficient resources to connect all the required links:
  - None of the links are connected.
  - The first link is listed as **Disconnected** in the *Participants* list of the *RMX Web Client / RMX Manager* main screen.



— Resource deficiency is listed as the *Call Disconnection Cause* in the *Participant Properties - Connection Status* dialog box.

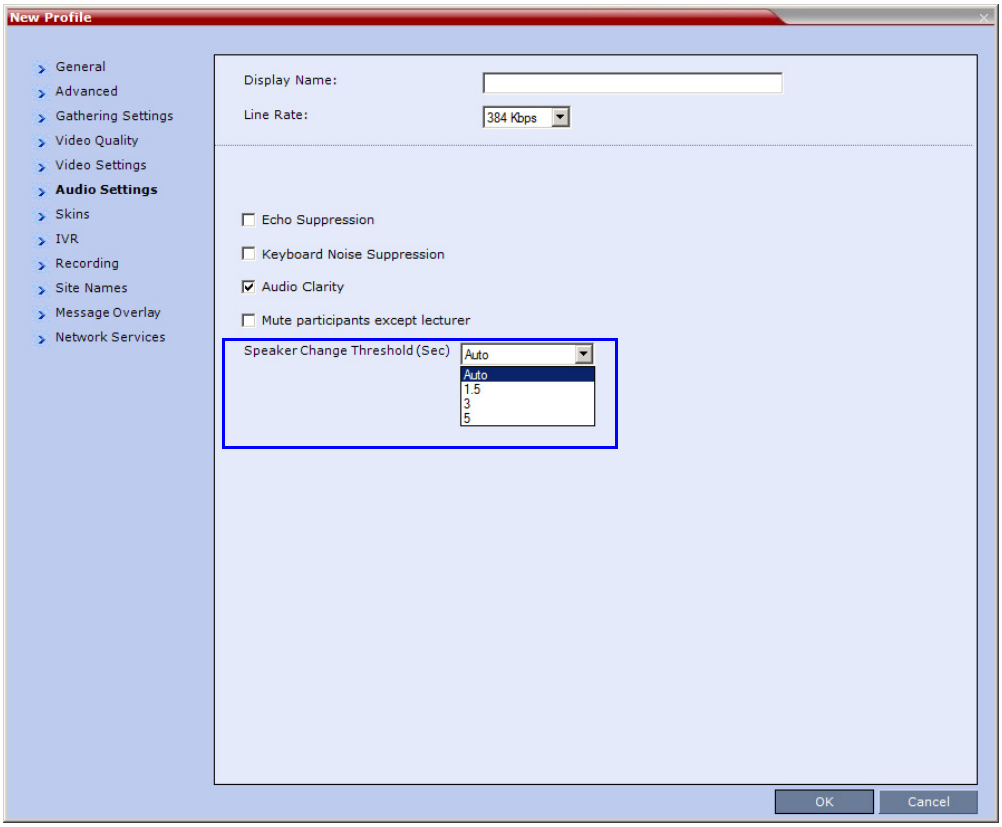


- If a calling *Link Participant* is not defined with same number of links as all the other *Link Participants* in the cascaded conferences:
  — The call is rejected.
  — The *Call Disconnection Cause* is: *Number of cascading links is not identical for all conferences.*

Speaker Change Threshold

The *Speaker Change Threshold* is the amount of time a participant must speak continuously before becoming the speaker. When defining or editing a conference profile, you can define the *Speaker Change Threshold*.

Speaker Change Threshold is defined in the *New Profile - Audio Settings* dialog box.



To adjust the *Speaker Change Threshold:*

>> Select the desired threshold:

- Auto (Default, 3 seconds)
- 1.5 seconds
- 3 seconds
- 5 seconds

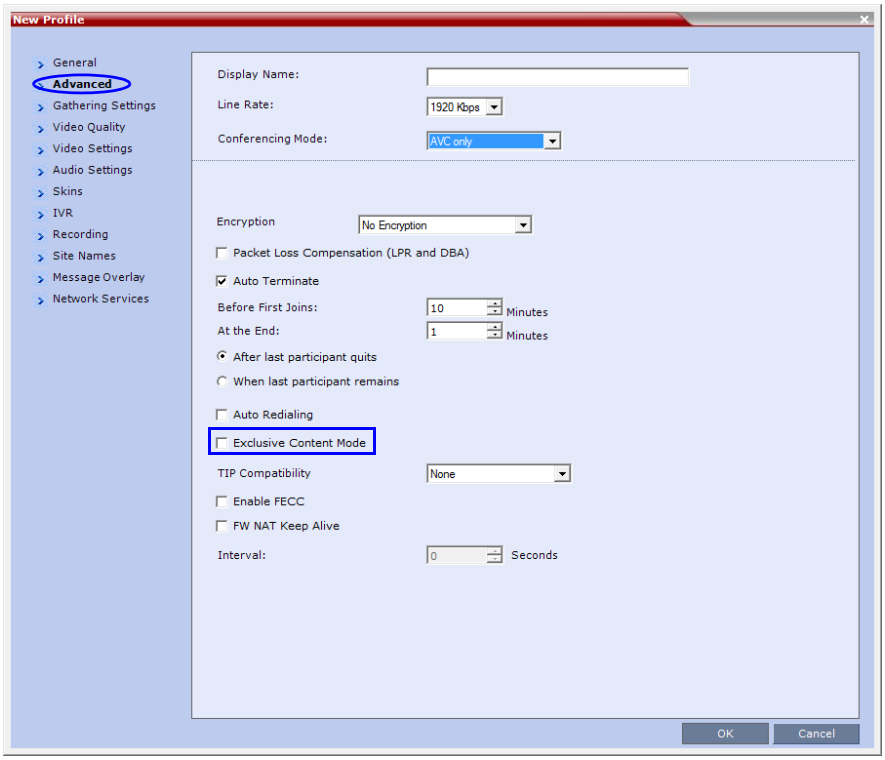
Exclusive Content Mode

Exclusive Content Mode allows you to limit *Content* broadcasting to one participant, preventing other participants from interrupting the *Content* broadcasting while it is active.

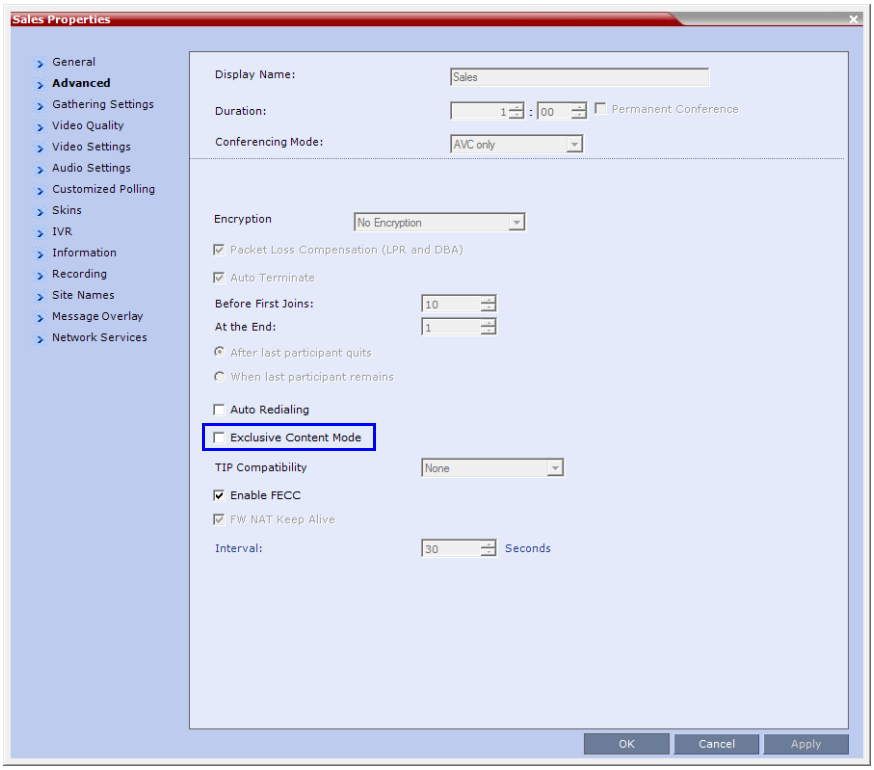
Guidelines

- *Exclusive Content Mode* is available in all Conferencing Modes.

- The *Exclusive Content Mode* is enabled or disabled by a check box in the in the *Advanced* tabs of the *Conference Profile*. The check box is cleared (feature is disabled) by default.



- *Exclusive Content Mode* can be enabled or disabled during an ongoing conference using the *Conference Properties - Advanced* dialog box.



- In *Exclusive Content Mode,* if the RESTRICT_CONTENT_BROADCAST _ TO_LECTURER *System Flag* is set to:
  - **NO** - the first participant to send content becomes the *Content Token* holder and has to release the *Content Token* before any other participant can acquire the token and begin transmitting *Content*.
  - **YES** - only the designated *Lecturer* can be the *Content Token* holder.
- The *Exclusive Content Mode* check box replaces the EXCLUSIVE_CONTENT_ MODE *System Flag* which was used to control *Exclusive Content Mode* for the system in previous versions.
- In *Exclusive Content Mode*, if an endpoint attempts to send *Content* a few seconds after another endpoint sent *Content*, the *Content* stream it is receiving is momentarily interrupted by a slide which is displayed for a few seconds before the normal *Content* stream is resumed.

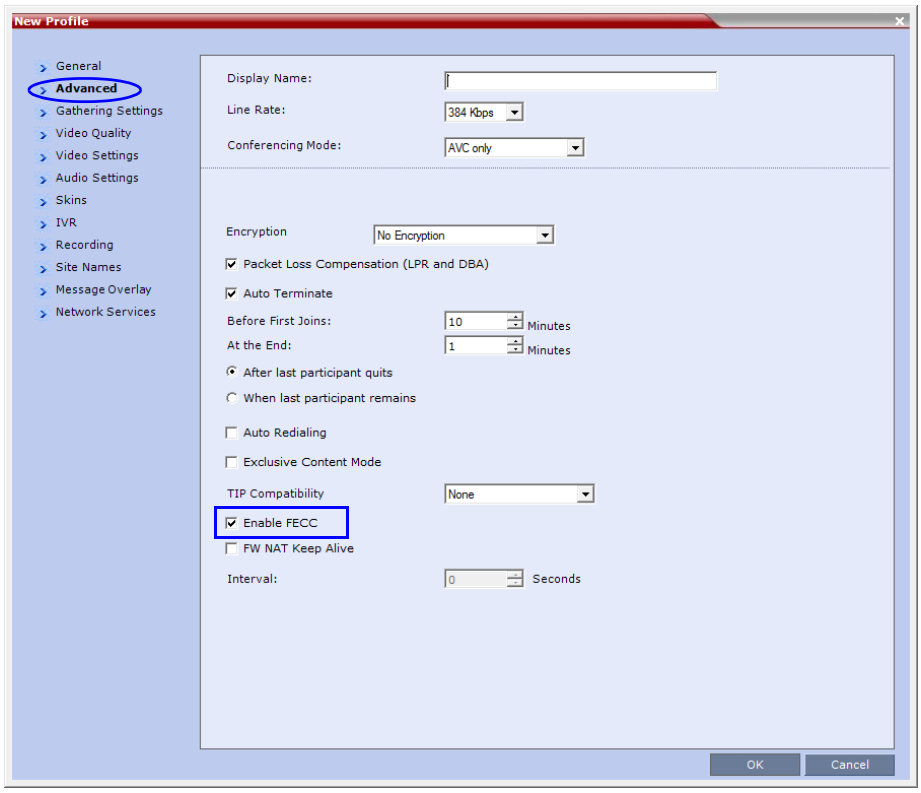
FECC Control

FECC can be enabled and disabled for individual conferences in the *Conference Profile*.

Guidelines

- The **Enable FECC** check box in the *Profile – Advanced* tab replaces the *FECC* activation functionality of the FECC and SIP_ENABLE_FECC *System Flags*. The check box is selected by default.

- When the *Enable FECC* check box is selected, *Far End Camera Control* can be activated either directly using the *Remote Control* device or by using *PCM*.
- When the *Enable FECC* check box is cleared, both *FECC* activation methods, using PCM or using remote control, are disabled and users (*SIP*, *H.323* and *ISDN*) will not be able to control far end cameras.
- FECC is not supported by the ISDN protocol, therefore it is not supported in ISDN calls.
- After upgrading from previous versions, the *Enable FECC* check box is selected by default.
- If in the previous version either of the FECC or SIP_ENABLE_FECC *System Flags* were set to NO, the administrator must manually clear the check box, if required.
- When the PCM_FECC *System Flag is* set to YES, the system enables navigation of *PCM* using the *Remote Control* device's arrow keys. Disabling *FECC* at conference level by clearing the *Enable FECC* check box does not affect *PCM* navigation.



Mute Participants Except Lecturer

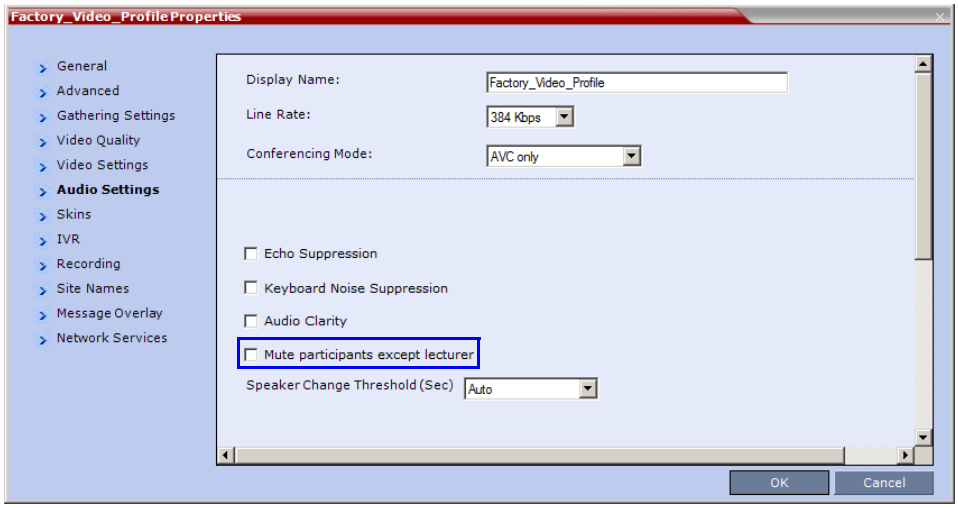
When the *Mute Participants Except Lecturer* option in the *Conference Profile* is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the RMX Web Client/RMX Manager.

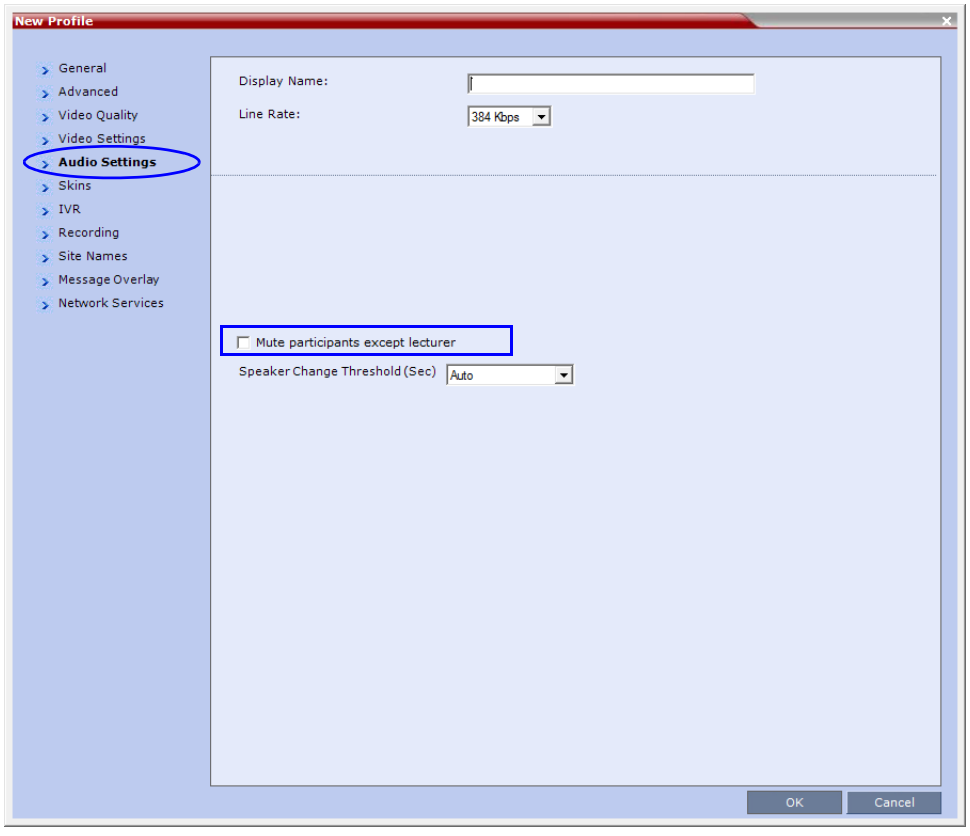
Guidelines

- Both administrators and operators (users) are allowed to set the *Mute Participants Except Lecturer* option.
- When the *Mute Participants Except Lecturer* option is enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the *Closed Caption* or *Message Overlay* functions.
- When the *Mute Participants Except Lecturer* option is enabled in the *Conference Profile* settings, all conferences to which this profile is assigned will start with this option enabled. All participants, except for the designated lecturer, are muted.
- The *Mute Participants Except Lecturer* option can be enabled or disabled at any time after the start of the conference. When enabled, it allows all the conference participants to converse before the lecturer joins the conference or before they are muted. When disabled, it unmutes all the participants in the conference.
- If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted.
- When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer.
- When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the *Mute Participants Except Lecturer* option.
- A participant can override the *Mute Participants Except Lecturer* option by activating the *Mute All Except Me* option using the appropriate DTMF code, provided the participant has authorization for this operation in the IVR Services properties. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the *Mute Participants Except Lecturer* option after a participant has previously activated the *Mute All Except Me* option. The participant is muted and the lecturer, if designated, is unmuted.
- In cascaded conferences, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.

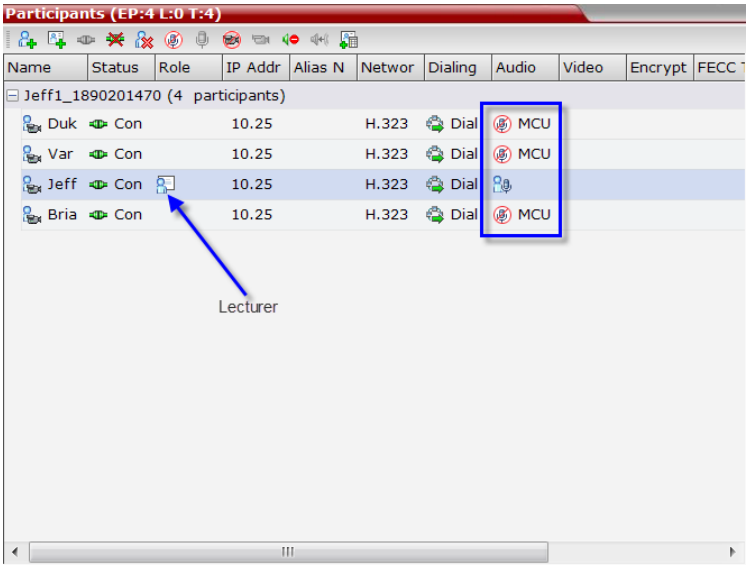
Enabling the Mute Participants Except Lecturer Option

The *Mute Participants Except Lecturer* option is enabled or disabled (default) in the *Conference Profile* or in an ongoing conference in the *Profile Properties - Audio Settings* tab.



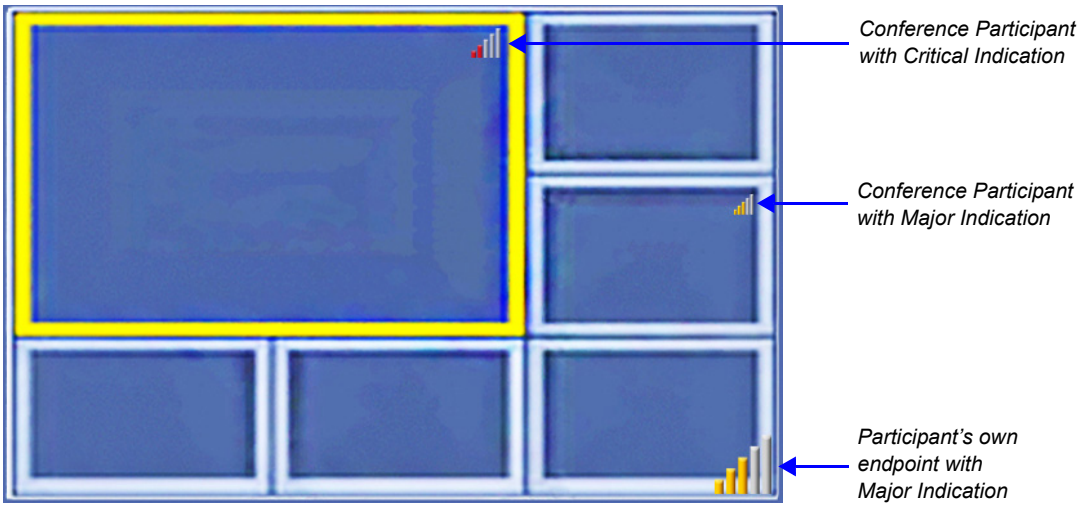


When the *Mute Participants Except Lecturer* option is enabled and a conference has started, the **Mute by MCU** icon is displayed in the *Audio* column in the *Participants* pane of each participant that is muted.



Network Quality Indication

If network quality issues occur, *Network Quality Indicators* provide information to participants about their own network quality and that of other participants displayed in the cells of the conference *Video Layout*.



Guidelines

Network Quality Indicators are displayed for:

- The *Video Channel* only in *AVC Conferencing Mode*.
  Content, *Audio* and *FECC Channel* quality issues are not indicated.
- The participant's own endpoint:
  - *Network Quality Indicators* are displayed by default and can be disabled
  - For media transmitted to and received from the *RMX (Video in / Video out)*.
- Participants displayed in the cells of the conference *Video Layout*:
  - *Network Quality Indicators* are not displayed by default and can be enabled
  - The media transmitted from the endpoint to the *RMX* (*Video in*).

Network Quality Indicators:

- Are supported with *MPMx* cards only
- Are not supported in *AVC - Video switched* conferences

Network Quality

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*.

Major and *Critical* states are indicated with yellow and red indicator bars respectively.


Major


Critical

When network quality improves from *Critical* to *Major* remaining stable for 5 seconds, the *Network Quality Indicator* is changed accordingly and when network quality improves from *Major* to *Normal*, remaining stable for 5 seconds, the *Network Quality Indicator* is no longer displayed.

Indication Threshold Values

The default *Major* and *Critical* indication threshold values can be modified by manually adding the following *System Flags* and modifying their values as required.

Table 2-22 *Network Quality Indicator - Indication Threshold Flags*

Flag	Description
NETWORK_IND_MAJOR_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Normal* to *Major*. Default: 1

Table 2-22 Network Quality Indicator - Indication Threshold Flags

Flag	Description
NETWORK_IND_CRITICAL_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Major* to *Critical*. Default: 5

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide, "Manually Adding and Deleting System Flags"* on page **1-18**.

Customizing Network Quality Indicator Display

Display of the *Network Quality Indicators* can be customized for the following:

- The participant's own endpoint
- Participants displayed in the cells of the conference *Video Layout*

The *Network Quality Indicator* display can be customized by manually adding the following *System Flags* and modifying their values as required.

Table 2-23 Network Quality Indicator - Display Customization Flags (Continued)

Flag	Description
DISABLE_SELF_NETWORK_IND	Disable the display of the *Network Quality Indicator* of the participant's own endpoint. Default: NO Range: YES / NO
DISABLE_CELLS_NETWORK_IND	Disable the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: YES Range: YES / NO
SELF_IND_LOCATION	Change the location of the display of the *Network Quality Indicator* of the participant's own endpoint. Default: BOTTOM_RIGHT Range: • TOP_ LEFT • TOP • TOP_RIGHT • BOTTOM_ LEFT • BOTTOM • BOTTOM_RIGHT

Table 2-23 *Network Quality Indicator - Display Customization Flags (Continued)*

Flag	Description
CELL_IND_LOCATION	Change the location of the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: TOP_RIGHT Range: • BOTTOM_LEFT • BOTTOM_RIGHT • TOP_LEFT • TOP_RIGHT

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Manually Adding and Deleting System Flags"* on page **1-18**.

Content at HD1080p Resolution

Endpoints that support H.264 can now receive H.239 Content at the following resolutions:

- *HD720p* at 30fps
- *HD1080p* at 15fps

These resolutions are in addition to the existing *HD720p* at 5fps *Content* resolution.

Guidelines

- *Content* at *HD1080p* resolution is supported at conference and call rates of 768 kbps or higher.
- The initial *Content* rate is determined by the conference *Profile - Line Rate* and *Content*
- *Settings*.
- The *Content* rate is lowered if endpoints connect at lower call rates.
- All connected endpoints must support the minimum required conference *Line Rate* and be capable of receiving *HD1080p* content.
- The *Content Protocol* setting in the conference *Profile* must be set to *Up to H.264*.
- All endpoints will receive *Content* at the highest resolution common to all connected endpoints.
- During a *H.264 Content* session, changes to resolution or frame rate do not interrupt *Content* transmission.

- Table 2-24 summarizes the *Maximum Resolution* of *Content* and *Frames per Second* (*fps*) for *Bit Rate Allocations* to the *Content Channel*.

Table 2-24 *Content - Maximum Resolution, Frames/Second per Bit Rate Allocation*

Bit Rate Allocated to Content Channel (Kbps)	Content	
	Maximum Resolution	Frames/Second
*From **64** and less than **512***	H.264 HD720p	5
*From **512** and up to **768***	H.264 HD720p	30
*From **768** and up to **1536***	H.264 HD1080p	15

- The *Profile - Content Settings*: *Graphics, Hi Resolution Graphics* and *Live Video* increasing affect the amount of bandwidth allocated to *Content* and the probability of *HD1080p* being supported.

Table 2-25 summarizes the bit rate allocation to the *Content* channel for each of the three *Content Settings*.

Table 2-25 *Decision Matrix - Bit Rate Allocation to Content Channel per Conference Line Rate*

Content Settings	Content Bit Rate Allocation per Conference Line Rate (kbps)										
	64 96	128	256	384	512	768 832	1024 1152	1472 17281 1920	2048	4096	6144
Graphics		64	64	128	128	256	256	256	512	256	1536
Hi Resolution Graphics		64	128	192	256	384	384	512	768	1536	1536
Live Video		64	128	256	384	512	768	768	1152	1536	1536

- If a *Legacy Endpoint* connects, the highest *Content* resolution for the conference is *HD720p* at 30 fps.
- *Content* is shared across Cascaded Links using H.263 irrespective of whether either or both the cascade-enabled Entry Queue and the Cascaded Link have Up to H.264 Content sharing defined in their profiles.

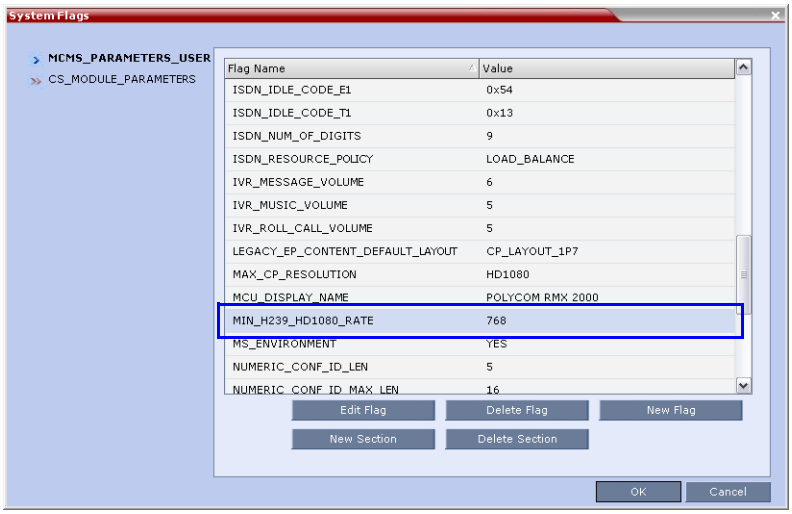
Modifying the Threshold Line Rate for HD Resolution Content

The threshold line rate for *HD Resolution Content* is the line rate at which the RMX will send *Content* at *HD1080 Resolution*. The default is 768 kbps.

To modify the HD Resolution Content threshold line rate:

1 On the RMX menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.



2 In the *MCMS_PARAMETERS* tab, double-click the **MIN_H239_HD1080_RATE** entry.

The *Update Flag* dialog box is displayed

3 In the *Value* field, enter the minimum threshold line rate at which *HD1080 Resolution Content* will be enabled.

4 Click **OK** to exit the *Update Flag* and then again to exit the *System Flags* dialog box.

Disabling HD Resolution Content

To disable HD720p/ HD1080p resolution content:

1 On the RMX menu, click **Setup > System Configuration**.

2 In the *System Flags - MCMS_PARAMETERS* tab, double-click the **MIN_H239_HD1080_RATE** entry.

3 In the *Update Flag - Value* field, enter **0**.

4 Click **OK** to exit the *Update Flag* and then again to exit the *System Flags* dialog box.

System Flags

IBM SUT RTCP Flow Control

RTCP-FB

For *IBM Sametime Unified Telephony Lite* (*SUT*) *Clients*, *RTCP-FB* replaces the use of *SIP INFO* messages when the *RMX* issues an *INTRA* request or other flow control commands to change the video rate.

System Flag

You can modify the *TMMBR* parameter (*Temporary Maximum Media Stream Bit Rate*) by adding the following flags:

RTCP_FLOW_CONTROL_TMMBR_ENABLE

Enables/disables the SIP RTCP flow control parameter.

Default: YES

RTCP_FLOW_CONTROL_TMMBR_INTERVAL *System Flag* and setting its value as required.

Range: 5 - 999 (seconds)

Default: 180

For more information see the *RMX 1500/2000/4000 Administrator's Guide*, *"Manually Adding and Deleting System Flags"* on page **1-18**.

SIP RTCP_FIR_ENABLE

RTCP_FIR_ENABLE When set to **YES**, the *Full Intra Request (FIR)* is sent as *INFO* (and not *RTCP*).

Default = YES

Exporting and Importing Conference Templates

Conference Templates can be exported from one MCU and imported to multiple MCUs in your environment. Additionally, you can export *Conference Templates* and their associated *Conference Profiles* simultaneously. Using this option can save configuration time and ensures 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.

- Administrators can export and import *Conference Templates*. Operators are only allowed to export *Conference Templates*.
- You can select a single, multiple or all *Conference Templates* to be exported.
- Both *Conference Templates* and their associated *Conference Profiles* can be exported and imported simultaneously when enabling the **Export includes conference profiles** or **Import includes conference profiles** options.
- Exporting and importing *Conference Templates* only can be used when you want to export and import individual *Conference Templates* without their associated Conference Profiles. This option enables you to import *Conference Templates* when *Conference Profiles* already exist on an MCU.

Exporting Conference Templates

Conference Templates are exported to a single XML file that can be used to import the *Conference Templates* on multiple MCUs.

Using the *Export Conference Templates* option, you can:

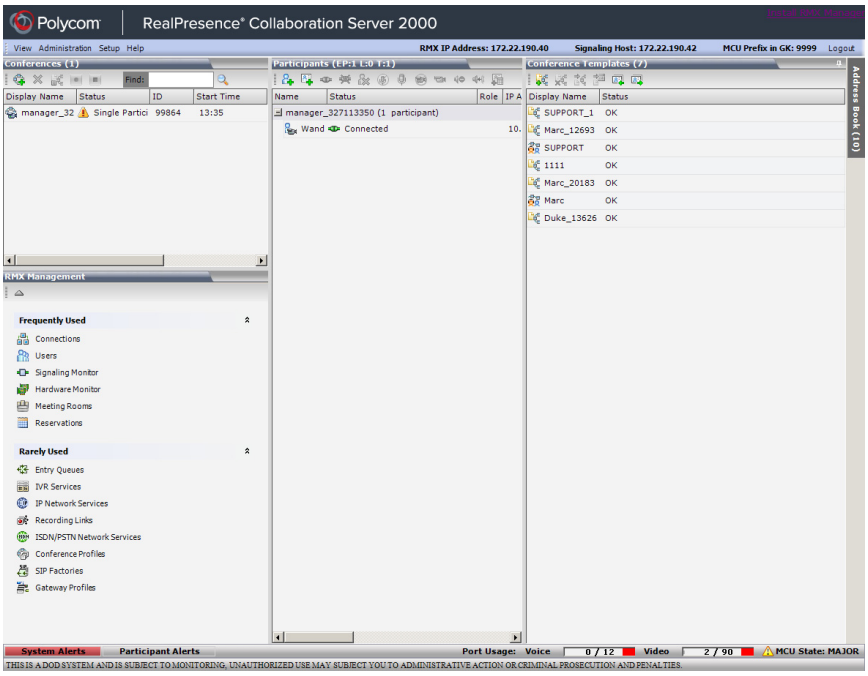
- Export all *Conference Templates* from an MCU

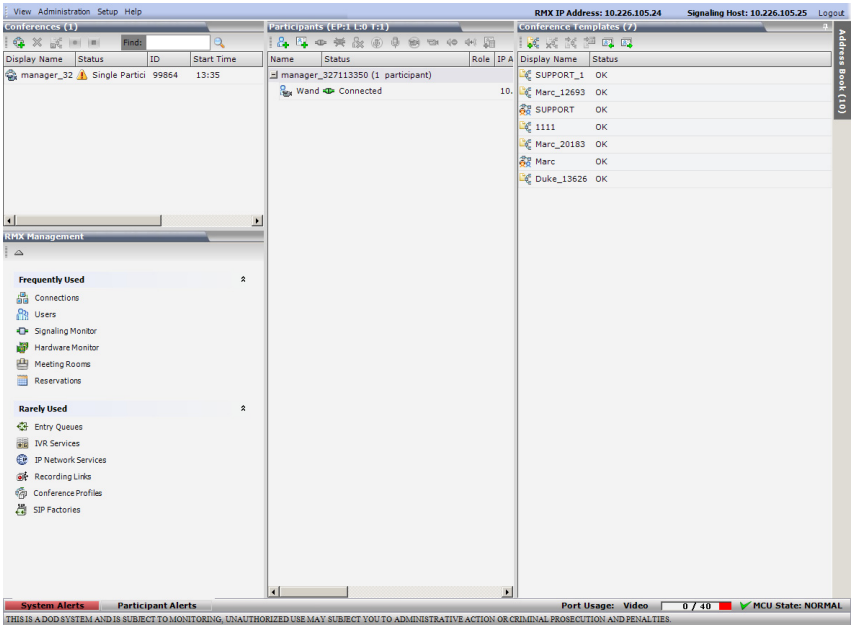
- Export selected *Conference Templates*

Exporting All Conference Templates from an MCU

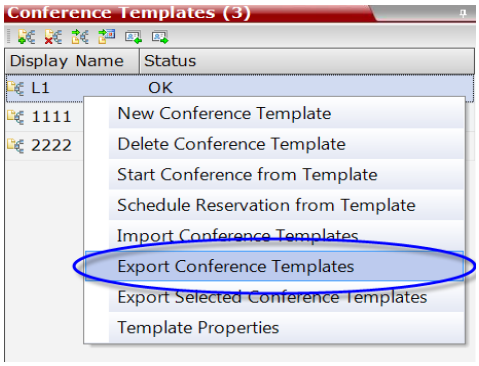
To export all Conference Templates from an MCU:

1 In the *RMX Web Client* main window, click the *Conference Templates* tab.
The *Conference Templates* list pane is displayed.

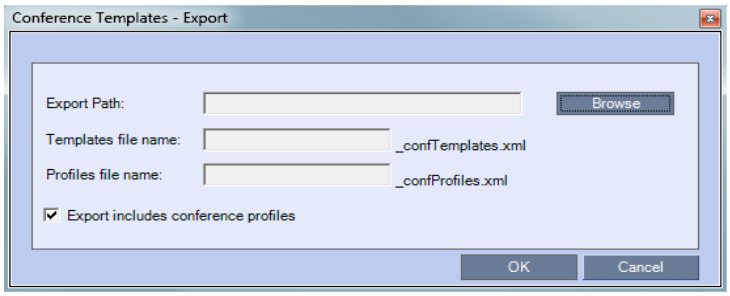




2 Click the **Export Conference Templates** button or right-click the *Conference Templates* list, and then click **Export Conference Templates**.



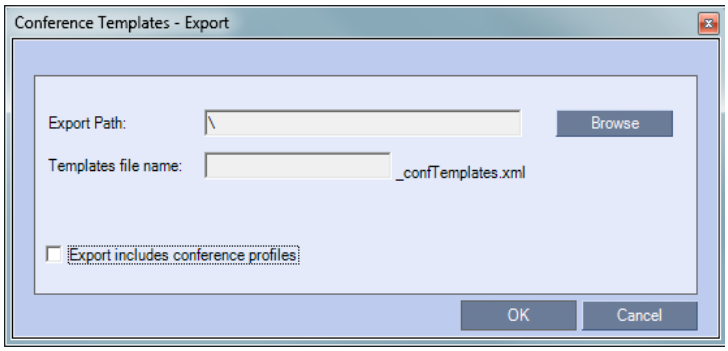
The *Conference Templates - Export* dialog box is displayed.



3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export *Conference Templates*.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.



5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

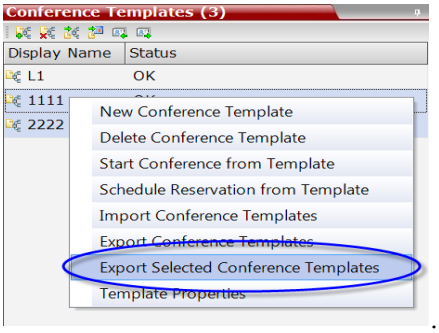
Exporting Selected Conference Templates

You can export a single *Conference Template* or multiple *Conference Templates* to other MCUs in your environment.

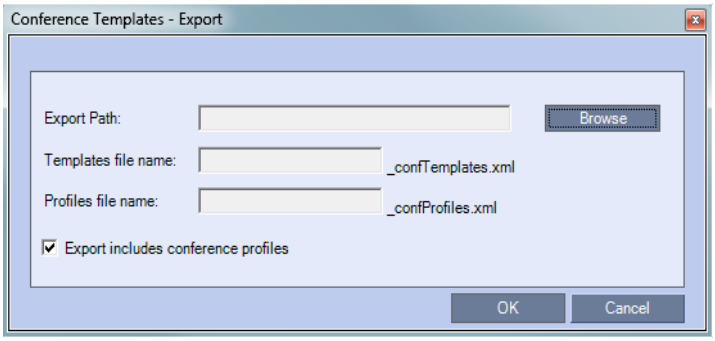
To export selected Conference Templates:

1 In the *Conference Templates* list, select the templates you want to export.

2 Right-click the *Conference Templates* to be exported, and then click **Export Selected Conference Templates**.



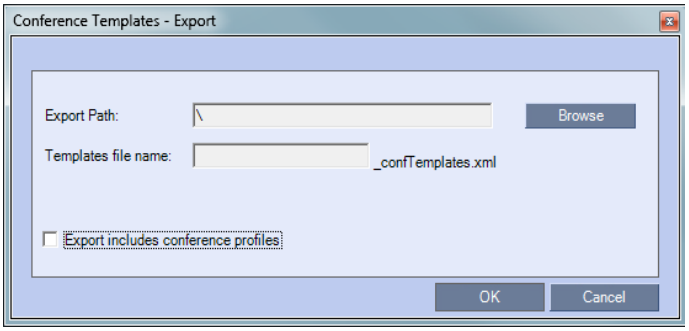
The *Conference Templates - Export* dialog box is displayed.



3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export Conference Templates.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.



5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type, *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

Importing Conference Templates

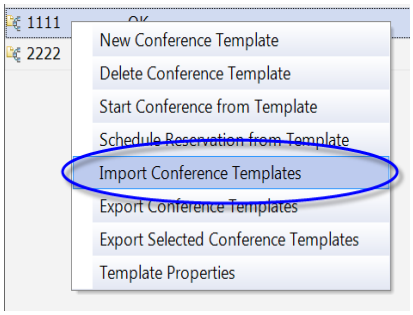
You can import *Conference Templates* and *Conference Profiles* from one MCU to multiple MCUs in your environment.

To import Conference Templates:

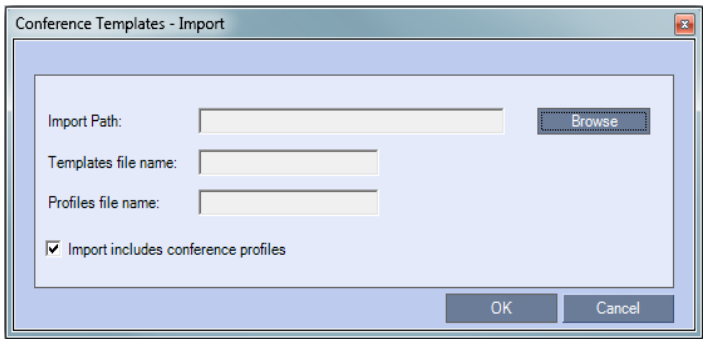
1 In the *RMX Web Client* main window, click the *Conference Templates* tab.

The *Conference Templates* are displayed.

2 Click the **Import Conference Templates** button or right-click the Conference Templates pane, and then click **Import Conference Templates.**

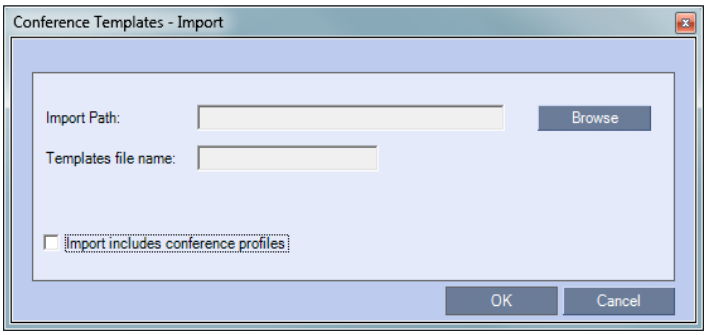


The *Conference Templates - Import* dialog box is displayed.



3 Optional. Clear the **Import includes conference profiles** check box when you only want to import *Conference Templates*.

When this check box is cleared, the *Conference Templates - Import* dialog box is displayed without the *Profiles file name* field.



4 In the *Import Path* field, click **Browse** to navigate to the path and file name of the *Conference Templates* you want to import.

When clicking the exported templates file you want to import, the system automatically displays the appropriate files in the *Templates file name* field and the *Profiles file name* field (when the **Import includes conference profiles** check box is selected).

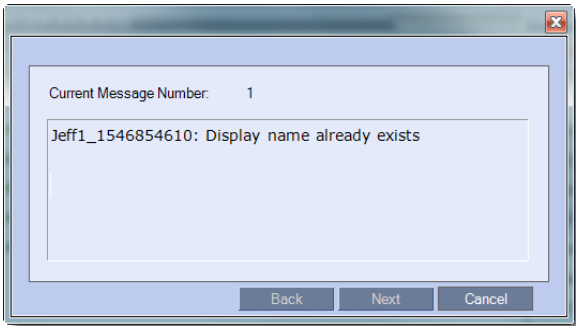
5 Click **OK** to import the *Conference Templates* and their associated *Conference Profiles,* if selected.

Conference Templates are not imported when:

— A *Conference Template* already exists

— An associated *Conference Profile* is not defined in the *Conference Profiles* list

When one or more *Conference Templates* are not imported, a Message Alert window is displayed with the templates that were not imported.



6 Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Templates* are added to the *Conference Templates* list. When the **Import includes conference profiles** check box is selected, the imported *Conference Profiles* are added to the *Conference Profiles* list.

Exporting and Importing Conference Files

Conference Profiles can be exported from one MCU and imported to multiple MCUs in your environment, enabling you to copy the *Conference Profiles* definitions to other systems. This can save configuration time and ensures 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.

Guidelines

- Administrators can export and import *Conference Profiles*. Operators are only allowed to export *Conference Profiles*.
- You can select a single, multiple, or all *Conference Profiles* to be exported.
- *Conference Templates* and their related *Conference Profiles* can be exported and imported simultaneously using the *Conference Templates* export and import function. For more information, see the **Exporting and Importing Conference Templates** section.

Exporting Conference Profiles

Conference Profiles are exported to a single XML file that can be used to import the *Conference Profiles* on multiple MCUs.

Using the Export Conference Profile feature, you can:

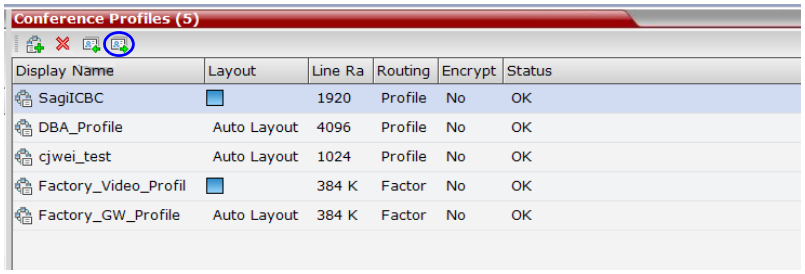
- Export all *Conference Profiles* from an MCU
- Export selected *Conference Profiles*

Exporting All Conference Profiles from an MCU

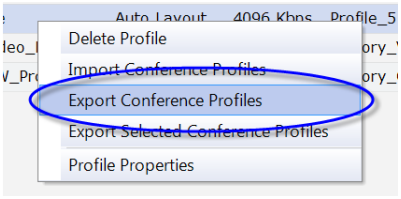
To export all Conference Profiles from an MCU:

1. In the *Management* pane, expand the *Rarely Used* list.
2. Click the **Conference Profiles** button.

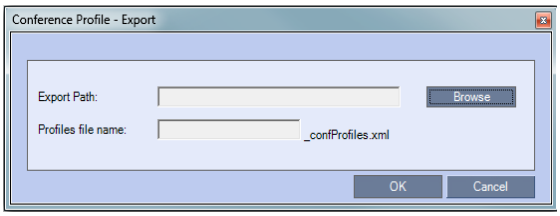
   The *Conference Profiles* are displayed in the *List* pane.



3 Click the **Export Conference Profiles** button or right-click the *Conference Profiles* pane, and then click **Export Conference Profiles**.



The *Conference Profile - Export* dialog box is displayed.

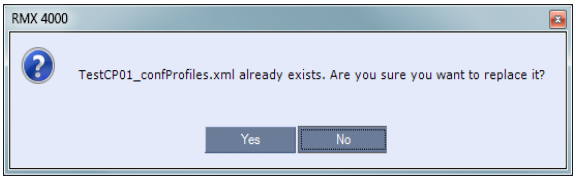


4 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

5 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

6 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.



7 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

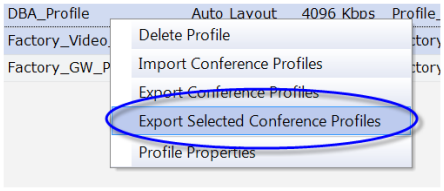
Exporting Selected Conference Profiles

You can select a single Conference Profile or multiple Conference Profiles and export them to a file to be imported to other MCUs in your environment.

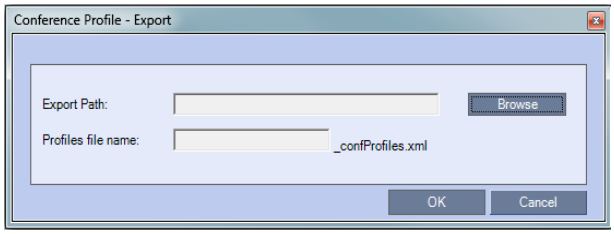
To export selected Conference Profiles:

1 In the *Conference Profiles* pane, select the profiles you want to export.

2 Right-click the selected *Conference Profiles*, and then click **Export Selected Conference Profiles**.



The *Conference Profile - Export* dialog box is displayed.

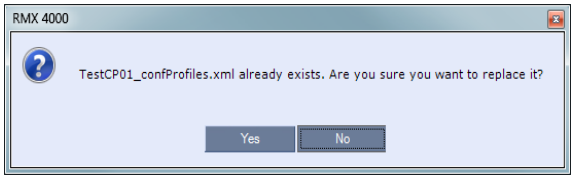


3 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

4 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

5 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.



6 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

Importing Conference Profiles

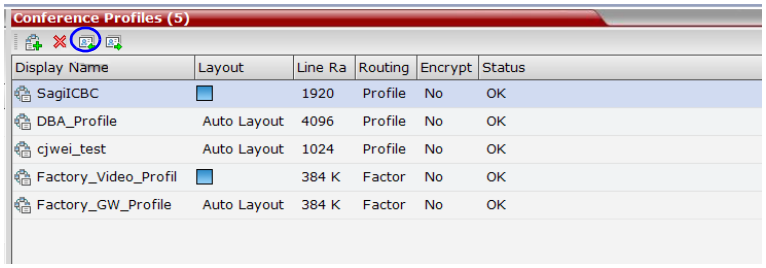
You can import Conference Profiles from another MCU in your environment.

To import Conference Profiles:

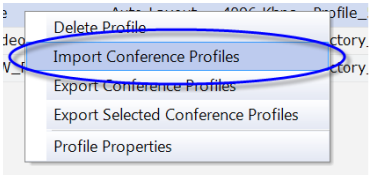
1 In the *Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

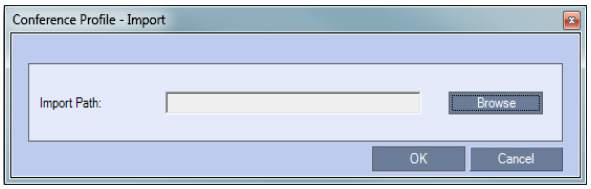
The *Conference Profiles* are displayed in the *List* pane.



3 Click the **Import Conference Profiles** button or right-click the Conference Profiles pane, and then click **Import Conference Profiles**.



The *Conference Profile - Import* dialog box is displayed.



4 In the *Import Path* field, click **Browse** to navigate to the path and file name of the exported *Conference Profiles* you want to import.

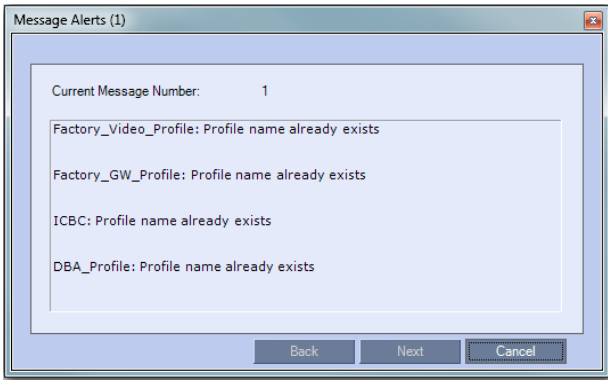
5 Click **OK** to import the *Conference Profiles*.

Conference Profiles are not imported when:

— A *Conference Profile* already exists

— An IVR Service does not exist for the related *Conference Profile*

When *Conference Profiles* are not imported into the *Conference Profiles* list, a Message Alert window is displayed with the profiles that were not imported.



Conference Profiles that are not problematic are imported.

6 Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Profiles* appear in the *Conference Profiles* list.

Managing Noisy Content

The system can identify participants who send frequent requests to refresh their Content display usually as a result of a problematic network connection. The frequent refresh requests cause frequent refresh of the Content display and degrade the viewing quality.

When the system identifies the noisy participants, the system will automatically suspend the requests to refresh the sent Content to avoid affecting the quality of the Content viewed by other conference participants. This process is controlled by System flags.

Content Display Flags

- **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 Collaboration Server system. 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 setting: 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 setting: 10
- **CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS**

  This flag controls the requests to refresh (intra) the Content sent from the Collaboration Server system 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 the 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 setting: 5

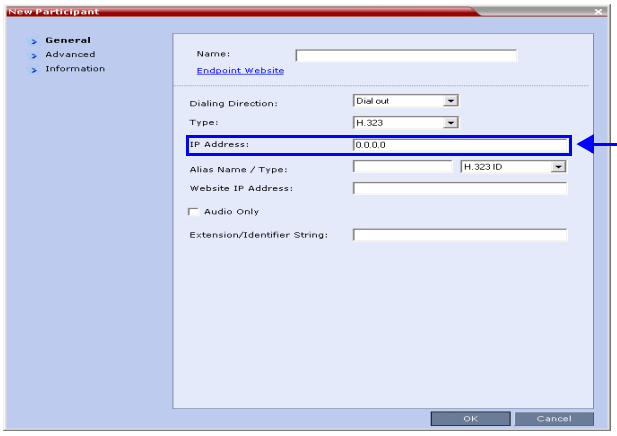
Direct IP Dialing

For RMXs registered to a gatekeeper, the *RMX* 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.

Dial-out Calls

For *Dial-out* calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_OUT** *System Flag*.

When the flag is set to NO (default), if the *Gatekeeper* is not functioning, the RMX dials to the endpoint using the endpoint's IP address configured in the *IP Address* field of the *New Participant/Participant Properties - General* dialog box.



If no IP address is defined in the *Participant Properties*, the call will fail.

The method by which calls are dialed out to the endpoint is dependant on the flag value and the availability of the *Gatekeeper* as summarized in the following table:

Table 2-26 *GK_MANDATORY_FOR_CALLS_OUT - System Flag*

Flag Value	Gatekeeper Available	Results
NO	NO	Dial out to endpoint *IP Address* **bypassing the Gatekeeper.**
NO	YES	Dial out to endpoint *Alias Name* using the *Gatekeeper.*
YES	NO	No dial out to endpoint.
YES	YES	Dial out to endpoint *Alias Name* using the *Gatekeeper.*

Dial-in Calls

For *Dial-in* calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_IN** and *System Flag*.

When the flag is set to NO (default), if the *Gatekeeper* is not functioning, calls from endpoints will be connected directly to the *Entry Queue*, *Conference* or *Meeting Room* that was dialed.

The method by which dial-in calls are accepted or rejected is dependant on the flag value and the availability of the *Gatekeeper* as summarized in Table 2-27:

Table 2-27 *GK_MANDATORY_FOR_CALLS_IN - System Flag*

Flag Value	Gatekeeper Available	Results
NO	NO	Dial-in call is connected **bypassing the Gatekeeper.**
NO	YES	Dial-in call is connected using the *Gatekeeper.*
YES	NO	Dial-in call is rejected.

Table 2-27 GK_MANDATORY_FOR_CALLS_IN - System Flag (Continued)

Flag Value	Gatekeeper Available	Results
YES	YES	Dial-in call is connected using the *Gatekeeper.*

Enabling or Disabling Direct IP Dialing

The direct IP dialing is enabled by default. To disable it, manually add the flags **GK_MANDATORY_FOR_CALLS_OUT** and **GK_MANDATORY_FOR_CALLS_IN** to the *System Configuration - MCMS_PARAMETERS* dialog box and for each flag enter the required value (YES or NO).

For more information on flag definition, see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*, "*Modifying System Flags*" on page **1-1**.

For flag changes (including deletion) to take effect, reset the RMX. For more information see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*, "*Resetting the Collaboration Server 800s*" on page **1-78**.

Microsoft Certification - Microsoft Lync Integration

FEC Support

Microsoft RTV FEC (Forward Error Correction) is supported in the RMX to control and correct packet loss when receiving and sending video streams using the Microsoft Lync Server 2010 communications software. All RTV resolutions and options, including B Frame, are supported.

Redundant video packets are sent over the network during video stream transmission. When packet loss occurs, FEC is automatically activated and the redundant packet is used to recover the lost packet.

When receiving video transmissions, packet loss automatically triggers FEC in the RMX. When sending video transmissions, RMX sends FEC packets when the RTCP RX report contains packet loss that is greater than or equal to 1 percent.

ICE Over TCP

RMX initially launches the ICE (Microsoft Interactive Connectivity Establishment) Extensions (MS-ICE 2) connection over UDP when ICE is enabled for Microsoft Lync clients. When ICE over UDP is blocked in the firewall UDP port, the ICE connection through the TCP protocol is automatically used instead of UDP for fallback. There is no configuration required for this process.

Media Over TCP

In previous RMX versions, media such as video, audio, content and FECC is transmitted using the UDP transport protocol. In version 7.7, media is automatically transmitted through TCP when UDP, the default transport protocol, is not available. Media over TCP is supported using the Microsoft ICE environment.

The media transport protocol type (UDP/TCP) is displayed in the *Participant Properties - Channel Status - Advanced* dialog box.

The media transport protocol type is displayed for the following IP addresses:

- RMX IP Address
- Participant IP Address
- ICE RMX IP Address - only when ICE is functional
- ICE Participant IP Address - only when ICE is functional

Meeting Room Presence Modes

In previous RMX versions, Meeting Room presence modes consisted of *Available* and *Offline*. RMX Meeting Rooms for Microsoft Lync clients now supports the following presence modes:

- Offline - (Gray) Meeting Room is not active
- Available - (Green) Meeting Room is active but no connected participants
- Busy - (Red) Meeting Room is active with at least one connected participant

The following figure illustrates the different presence modes for Meeting Rooms in Microsoft Lync:

RMX supports conferencing entities presences of up to 100 Microsoft Lync clients. When this number is exceeded, the additional conferencing entity may appear to be successfully registered but the presence status will be shown as 'Offline' in Lync for any entities beyond the limit.

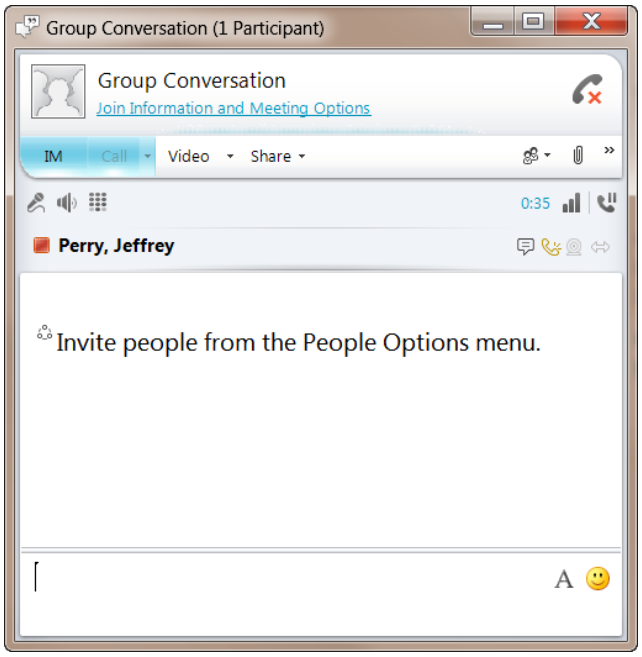
Connecting an RMX Meeting Room to a Microsoft AV-MCU Conference

Microsoft Lync users can connect an RMX Meeting Room to a conference running on the Microsoft A/V MCU. This allows RMX Lync users to connect with a conference in progress on the A/V MCU and be an active participant in the conference. The connection to the A/V MCU is the same configuration as a cascading conference between multiple RMX MCUs.

To connect to an A/V MCU conference:

1 From the Menu bar, click **Meet Now** to create an ad-hoc conference.

The Group Conversation dialog box is displayed.



2 From the Contacts List on Lync, drag a Virtual Meeting Room (VMR) into the Group Conversation list.

After the Virtual Meeting Room is connected on Lync, an invitation is sent from the A/V MCU to the RMX using the Centralized Conference Control Protocol (CCCP). The RMX responds and triggers a standard SIP invite sent from the A/V MCU to the RMX.

Multiple participants can now connect to both the RMX Meeting Room and the A/V MCU, and participate in a cascaded conference.

When a conference begins with Audio Only, a Lync user cannot add video to the conference after the VMR is connected to the conference. The conference will remain as Audio Only.

Network Error Recovery

When a short network error occurs, for example 5 seconds, RMX can automatically recover network errors, enabling calls in Microsoft Lync to continue the video or audio conference without disconnecting. However, when a longer network error occurs, the call is disconnected. The presence status mode is correctly updated from *Busy* to *Available*. There is no configuration required for this procedure.

SIP Dialog Recovery

RMX has the ability to automatically recover from a SIP dialog failure, which can occur in long duration calls in Meeting Rooms using the Microsoft Lync client. There is no configuration required for this procedure.

Polycom Open Collaboration Network (POCN)

Collaboration with Microsoft and Cisco

In previous versions, the RMX was capable of working with various *POCN* partners separately.

This version introduces an enhancement to the *POCN* solution, enabling *Polycom*, *Microsoft* and *Cisco* users, each within their own environment, to participate in the same conference running on an RMX.

Polycom's solution is to allow the RMX to natively inter-operate 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 *Figure 1* 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 RMX 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 *Figure 1*:

- *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

Solution 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*

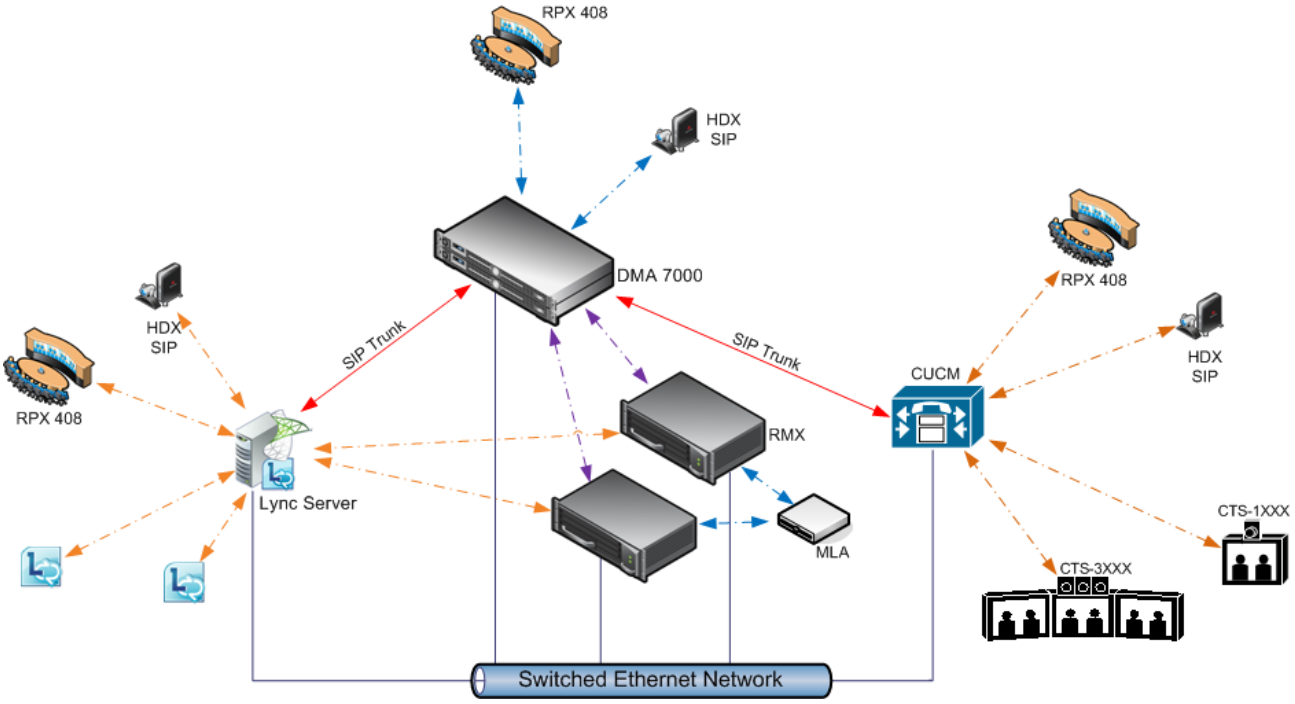


Figure 2-6 *POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components.*

Component	Version
Polycom	
HDX	3.0.5
RSS	8.0
DMA	5.0

Component	Version
CMA	6.0.1
CMAD	5.2.3
ITP (OTX, RPX, ATX, TPX)	3.0.5
Conferencing for Outlook (PCO)	1.0.7
Touch Control	1.3
Microsoft	
OCS 2007 R2	3.5.6907.236
Lync 2010	4.0.7577.183 CU4
OC 2007 R2 client	3.5.6907.236
Lync 2010 client	4.0.7577.4051 CU4
Exchange 2007 R2 SP3	8.3.213.1
Exchange 2010 SP2	14.2.247.5
Outlook 2007	12.0.6557.5001 SP2
Outlook 2010	14.0.6112.5000
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:

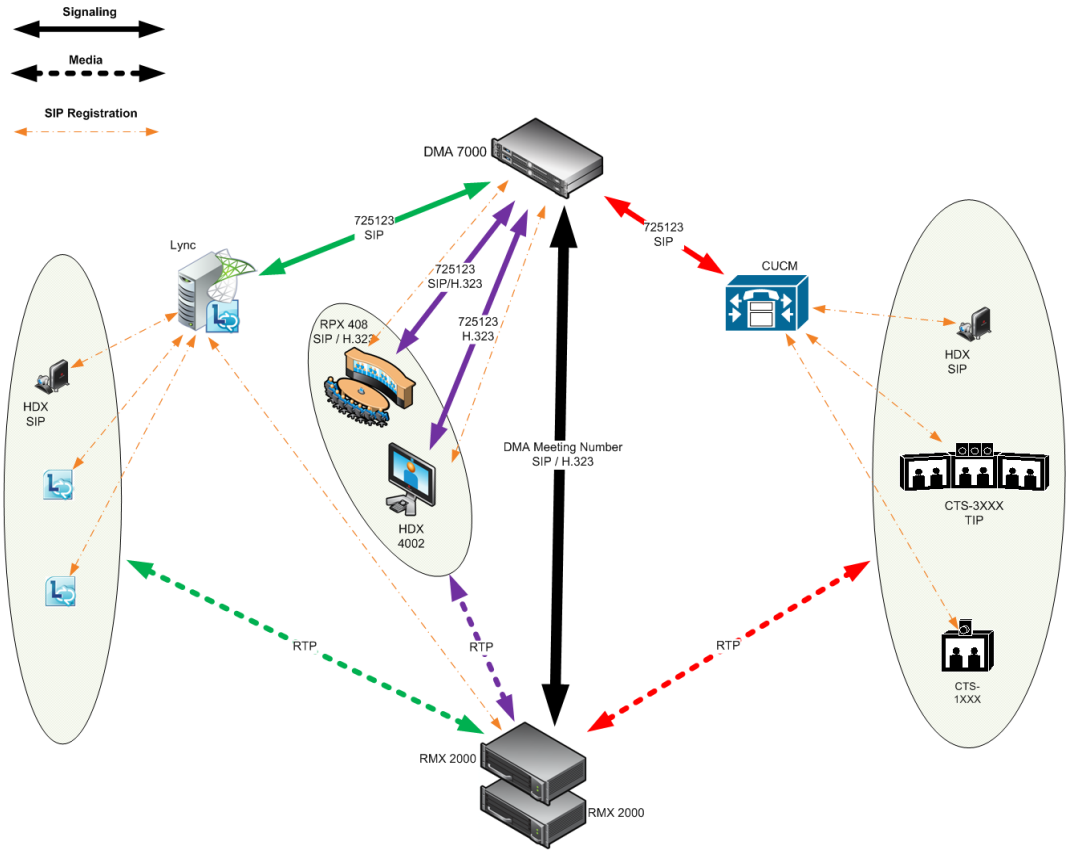
- In the *Lync* environment*:*
  - Sending or receiving *Content*.
  - Dial-out to *Lync* clients.
  - Presence of *VMRs*
- In the *Cisco* environment*:*
  - *TLS* and *SRTP*
  - *OBTP*

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 the *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 the *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 *RMX, Microsoft* and *Cisco Telepresence Systems (CTS) Integration Solution Architecture*.

Table 2-28 *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.

Table 2-28 *Solution Architecture Components*

Component	Version	Description
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 RMX.
RMX	8.1.1	MCU: • Functions as the network bridge for multipoint calls between *H.323*, *SIP* and *TIP* endpoints. • The RMX can be interfaced to *CUCM* using a *SIP* trunk, enabling *CTS* to join multipoint calls on RMX. Signaling goes through the *CUCM* while the media in *TIP* format goes directly between the *CTS* and RMX. • The RMX must be configured to route outbound SIP calls to DMA. • RMX 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		
OCS 2007 R2	3.5.6907.236	
Lync 2010	4.0.7577.183 CU4	
OC 2007 R2 client	3.5.6907.236	
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	

Table 2-28 Solution Architecture Components

Component	Version	Description
Outlook 2010	14.0.6112.5000	

TIP Layout Support & Resource Usage

Cisco Telepresence endpoints using TIP protocol support only one (CTS 1000) or three (CTS 3000) display screens. Therefore, 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.

Supported TIP Resolutions and Resource Allocation

Supported Resolutions

In a Telepresence TIP-enabled environment, only two video resolutions are available: 720p30 & 1080p30.

Table 2-29 Supported resolution per conference line rate

Conference Line Rate	Selected Resolution
3Mb or higher	1080p 30 fps
963kbps to 3Mb	720p 30 fps
Up to 936kbps	Call is disconnected.

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.

System capacity per MPMx card and resolution is summarized in the following table:

Table 2-30 *MPMx Resolution Capacities*

No. of media processors (ART) per card	No. of TIP screens per media processor	720p30 ports	1080p30 ports
10	3	30	15

Configuring 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 RMX to the *Lync* Server

   a. Install a *Security Certificate* on the RMX.

      The *Certificate* is obtained from the *System Administrator* and saved on the *Workstation*.

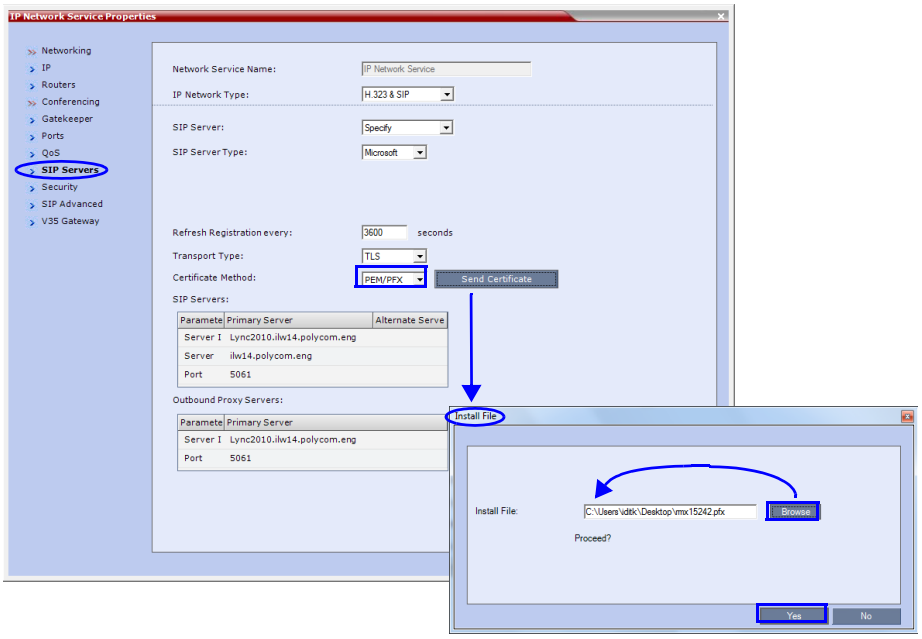
   b. In the *SIP Servers* tab of the *IP Network Services Properties* dialog box:

      iIn the *Certificate Method* drop-down menu, select **PEM/PFX**.

      iiClick the **Send Certificate** button.

      The *Install File* dialog box is displayed.

iiiBrowse to the saved *Certificate* on the *Workstation* and click the **Yes** button to install the certificate.



For more information see:

- *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Integration Into Microsoft Environments*" on page **1-1**.
- *Polycom Unified Communications Deployment Guide for Microsoft Environments, "Configuring Your RMX System for use with the Lync Server"*.

3 Register the RMX with the *Lync Server*.

a In the *IP Network Services Properties* dialog box, click the **SIP Servers** tab.

b In the *SIP Server* field, select **Specify**.

c In the *SIP Server Type* field, select **Microsoft**.

d Set *Refresh Registration every* **3600** *seconds*.

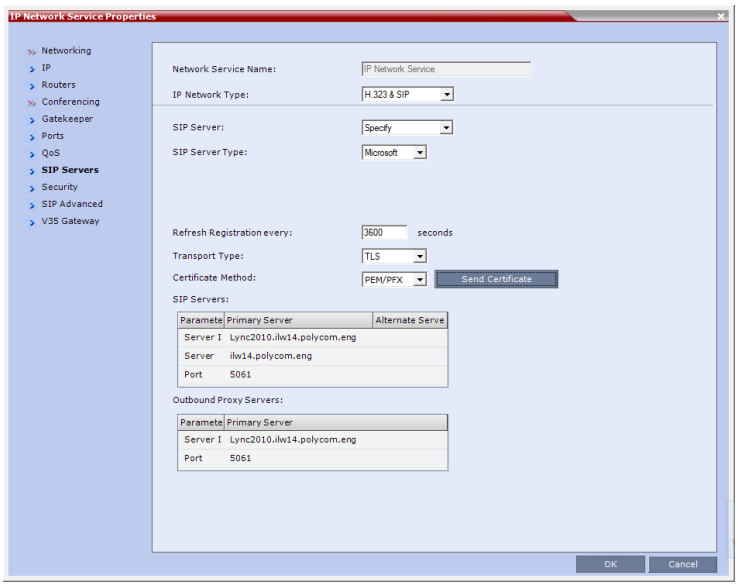
e If not selected by default, change the *Transport Type* to **TLS**.

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, the *Port* field must be set 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, the *Port* field must be set to **5061**. (The same value as entered in Step g.)



For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

1 Set the **ITP_CERTIFICATION** *System Flag* to **YES**.
When set to **NO** (default), this flag disables the *Telepresence* features in the *Conference Profile*.

2 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 the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Modifying System Flags"* on page **1-1**.

3 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.

4 Reset the RMX.

5 For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Resetting the RealPresence Collaboration Server Virtual Edition"* on page **1-79**.

6 Register the *DMA* to the *Lync* server

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, "*Configure a DMA System SIP Peer for the Lync Server*".

7 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*".

8 Register *Lync Clients* to the *Lync* server

For more information see the relevant *Lync* documentation.

9 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*".

10 Register *CTS1000* and *CTS3000* endpoints to the *CUCUM* server

For more information see the relevant *Cisco* documentation.

11 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*".

12 Register *HDX* endpoints to the *DMA* as *Gatekeeper*

For more information see the *Polycom® DMA™ 7000 System Operations Guide*.

13 Open MLA to configure ITP Layouts

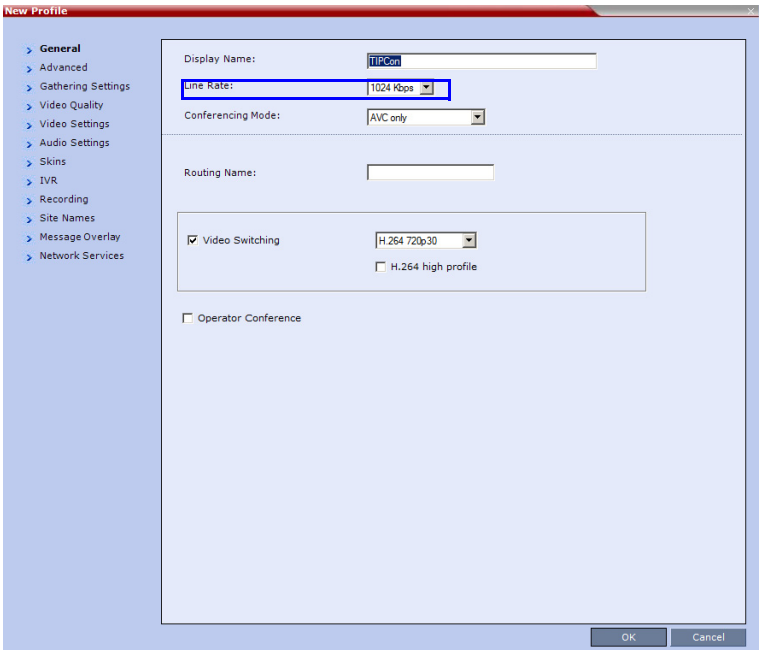
MLA (*Multipoint Layout Application*) is required for managing *CTS 3XXX* layouts whether *Polycom TPX, RPX* or *OTX* systems are deployed or not. *MLA* is a *Windows®* application that allows conference administrators to configure and control video layouts for multipoint calls involving *Polycom Immersive Telepresence* (*ITP*) systems.

For more information see the *Polycom Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*.

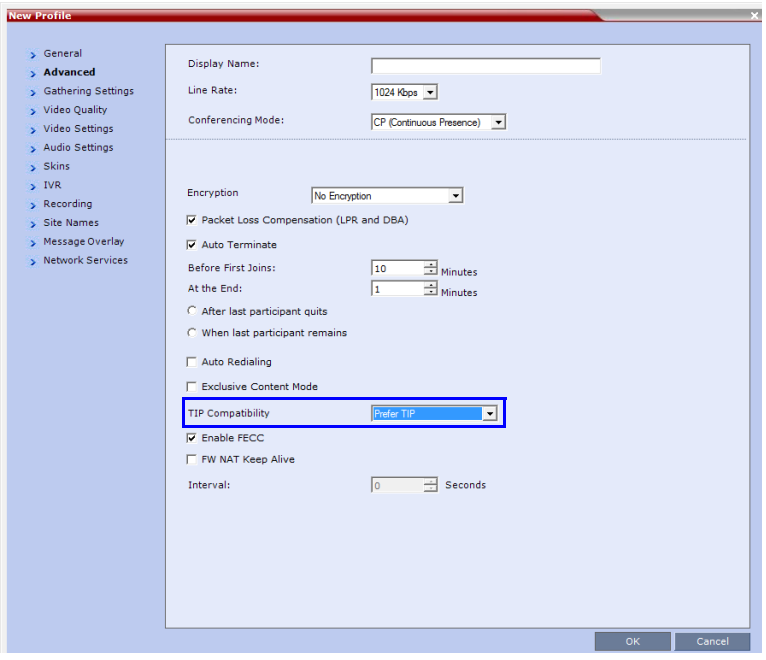
14 Configure a *TIP Enabled Profile* on the RMX.

a Create a *New Profile* for the *Meeting Room*.
For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Defining New Profiles"* on page **2-20**.

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*.



c Click the *Advanced* tab.



d Select the *TIP Compatibility* mode:

Prefer TIP is recommended if *Polycom* endpoints are to connect using *TIP*, otherwise select **Video and Content**.

When *Prefer TIP* is selected *Video Switching, Gathering Settings, Skins, Message Overlay, Site Names* and *Network Indication*(s) are disabled.

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 1300
- CTS 3010

Table 2-31 *TIP Compatibility - None*

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

Table 2-32 *TIP Compatibility - Video Only*

Video Only		Content Receiver	
		HDX / ITP	CTS
Content Sender	HDX / ITP	**Content Media:** H.264 **Flow Control:** H.323 via H.239 SIP via BFCP	None
	CTS	None	None

Table 2-33 *TIP Compatibility - Video & Content*

Video & Content		Content Receiver	
		HDX / ITP	CTS
Content Sender	HDX* / ITP	**Content Media:** TIp Content **Flow Control:** H.323 via H.239 SIP via BFCP TIP via Auto Collaboration	
	CTS		

* If *HDX* supports *TIP Content*.

Selecting *TIP Compatibility* as **Video and Content** disables *Content Settings* in the *Video Quality* tab.

Table 2-34 *TIP Compatibility - Prefer TIP*

<table>
<tr><th colspan="2" rowspan="2">Prefer TIP</th><th colspan="2">Content Receiver</th></tr>
<tr><th>HDX / ITP</th><th>CTS</th></tr>
<tr><td rowspan="2">Content Sender</td><td>HDX / ITP</td><td colspan="2" rowspan="2">Content Media: H.264
Flow Control: H.323 via H.239
SIP via BFCP
TIP via Auto Collaboration</td></tr>
<tr><td>CTS</td></tr>
</table>

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 Polycom RMX 2000 and a CISCO environment is now 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 RMX automatically creates a self-signed certificate to support encrypted communications with CISCO endpoints.

For media encryption. the RMX will first attempt to exchange keys using DTLS. If the RMX fails to exchange keys using DTLS, SIP TLS encrypted with SDES is used to exchange media encryption keys.

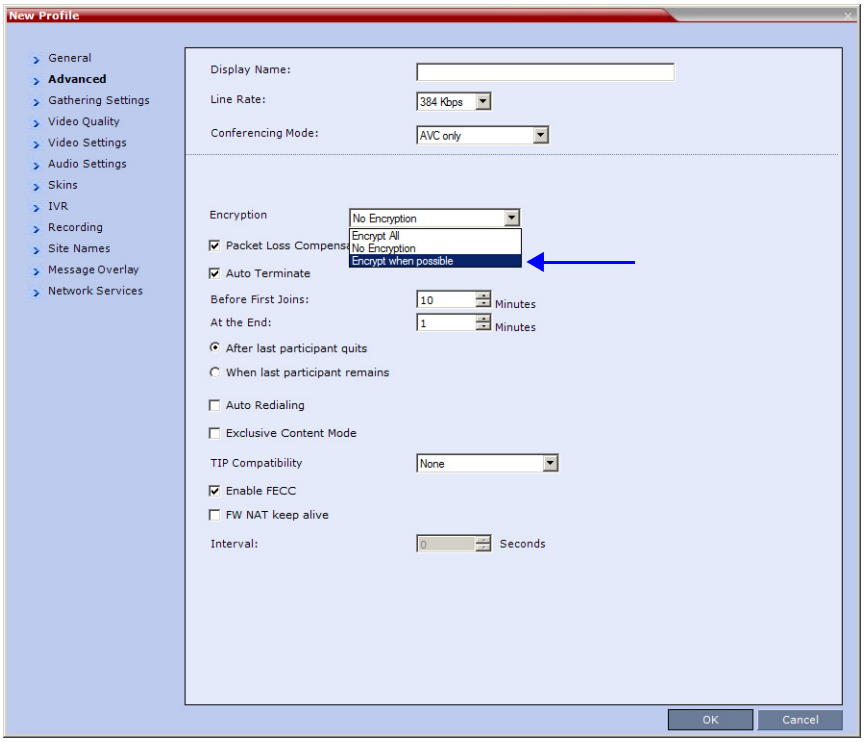
Guidelines

- 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**, click the **Advanced** tab.



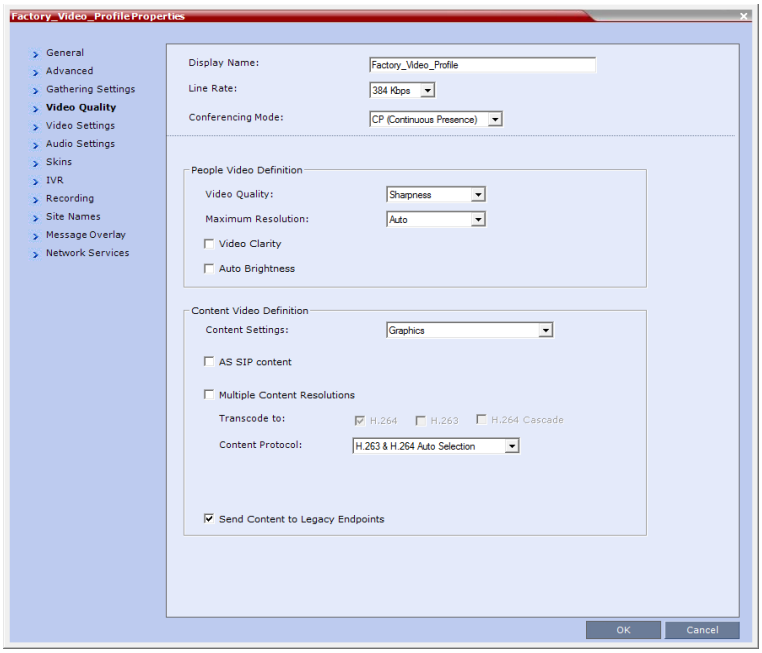
2 Set **Encryption** to either **Encrypt All** or **Encrypt when possible**.

3 Set the 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.

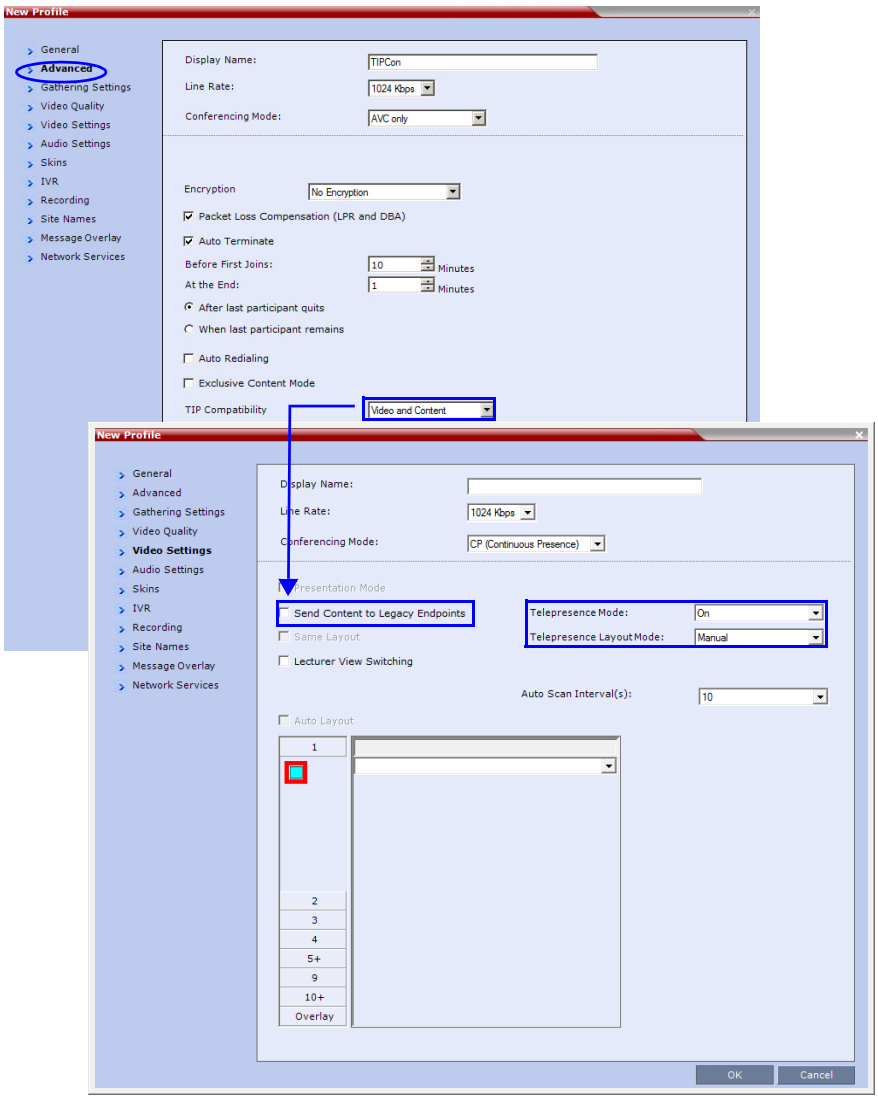
For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Encryption"* on page **2-52**.

a Click the *Video Quality* tab.



Content Settings is disabled if *TIP Compatibility* is set to **Video and Content** in the *Advanced* tab.

b Click 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 the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Creating a New Meeting Room*" on page **6-4**.

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 box 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:

Table 2-35 *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.

Endpoints

6 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*.

7 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.*

8 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.*

9 Configure *TIP* endpoints to register to:

- DMA
- CUCM

The procedures for configuring *TIP- enabled* endpoints are described in detail in the *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 Table 2-36.

Table 2-36 *Video and Content*

Dialing Method	Endpoint Registration		
	Lync	**CUCM**	**DMA**
	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 RMX	• 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 RMX	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints (Not supported in ITP Mode)		
CTS to RMX	• 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 then click **Participant Properties**.

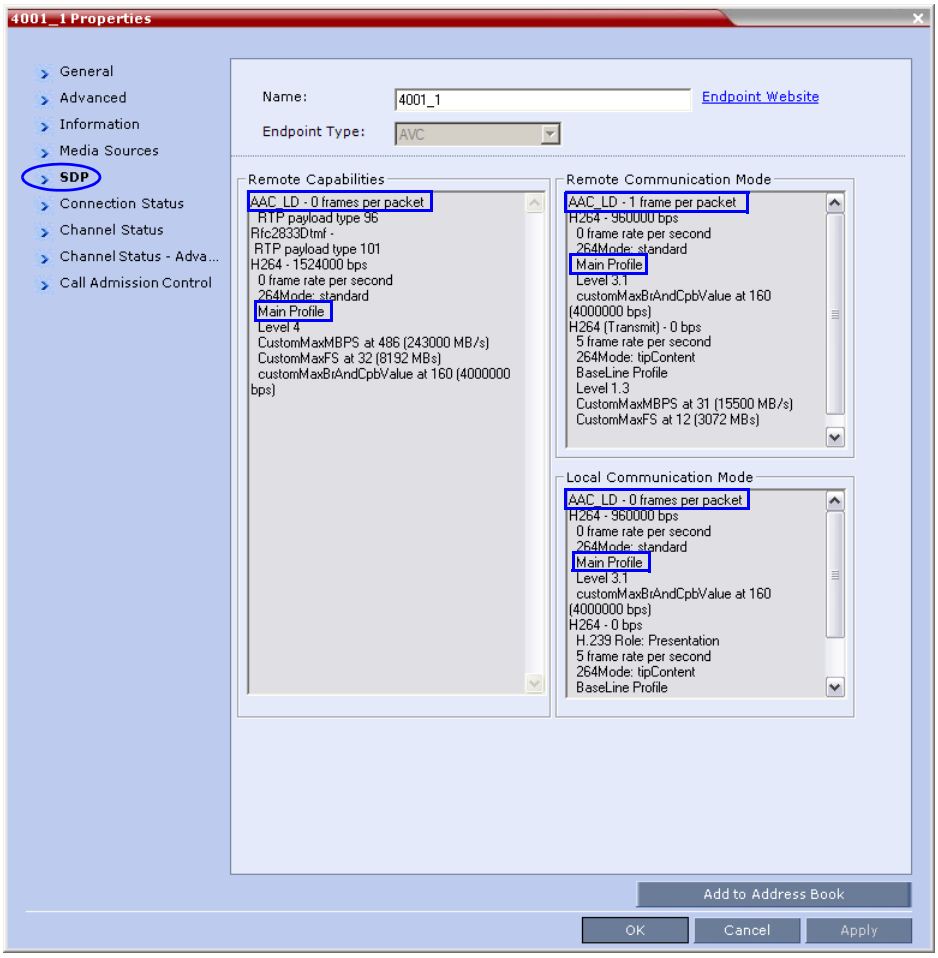
The *Participant Properties - General* dialog box opens.

2 Click the **SDP** tab.

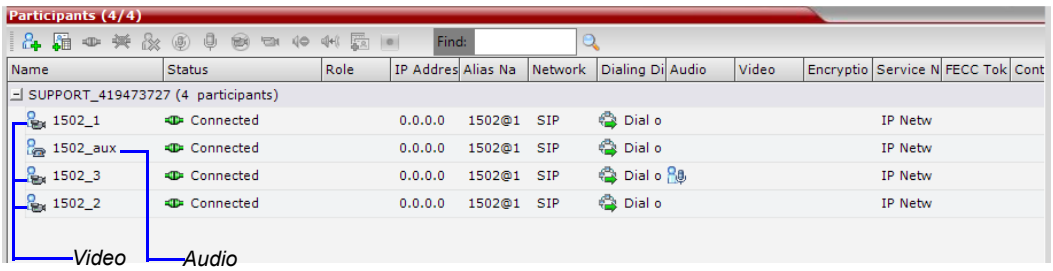
The following are indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:

— 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.



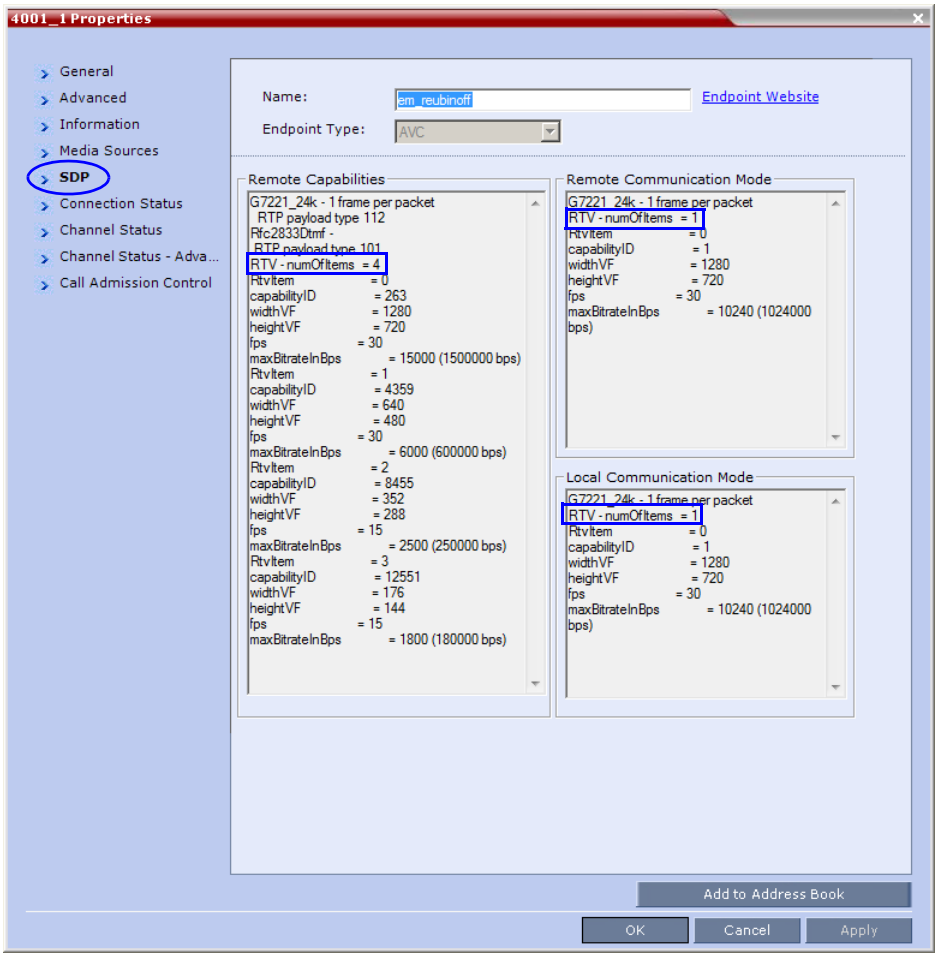
Lync Participants (RTV)

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

The *Participant Properties - General* dialog box opens.

2 Click the **SDP** tab.

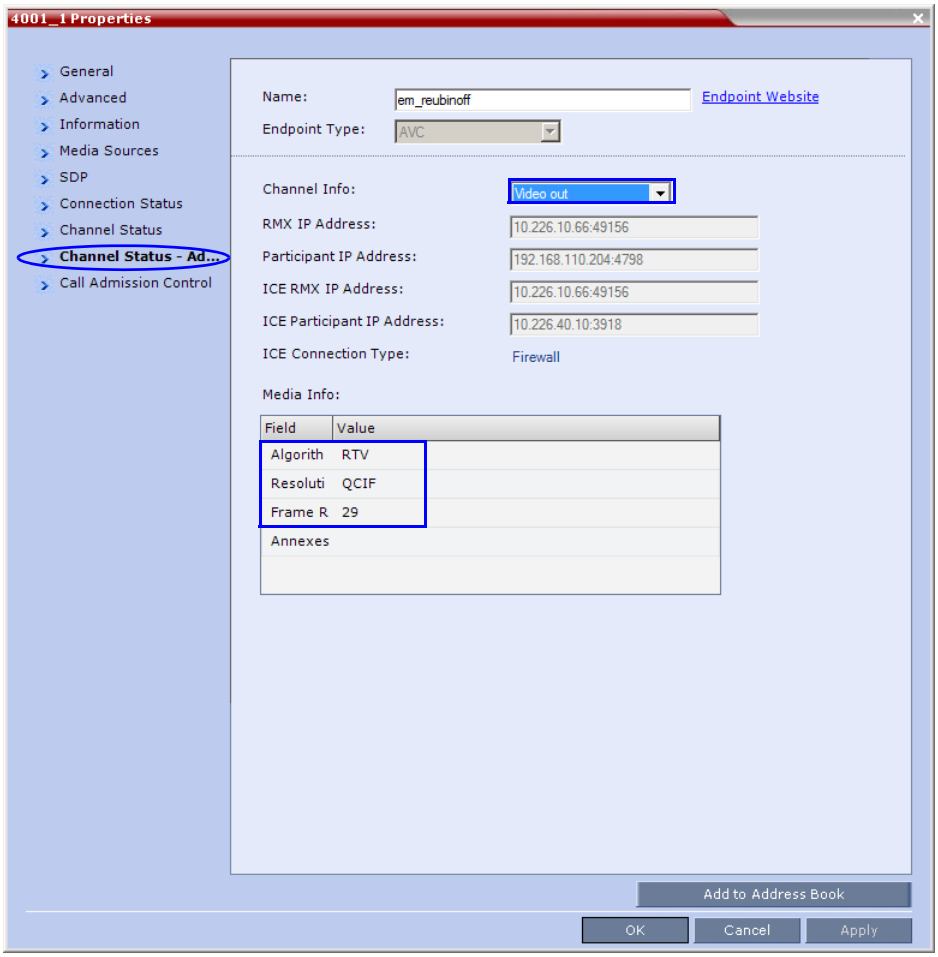
RTV is indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:



3 Click 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 *Video Only*. Frequency: Often.

NAT (Network Address Translation) Traversal

NAT Traversal is a set of techniques enabling participants behind firewalls to connect to conferences, hosted on the RMX, remotely using the internet.

Session Border Controller (SBC)

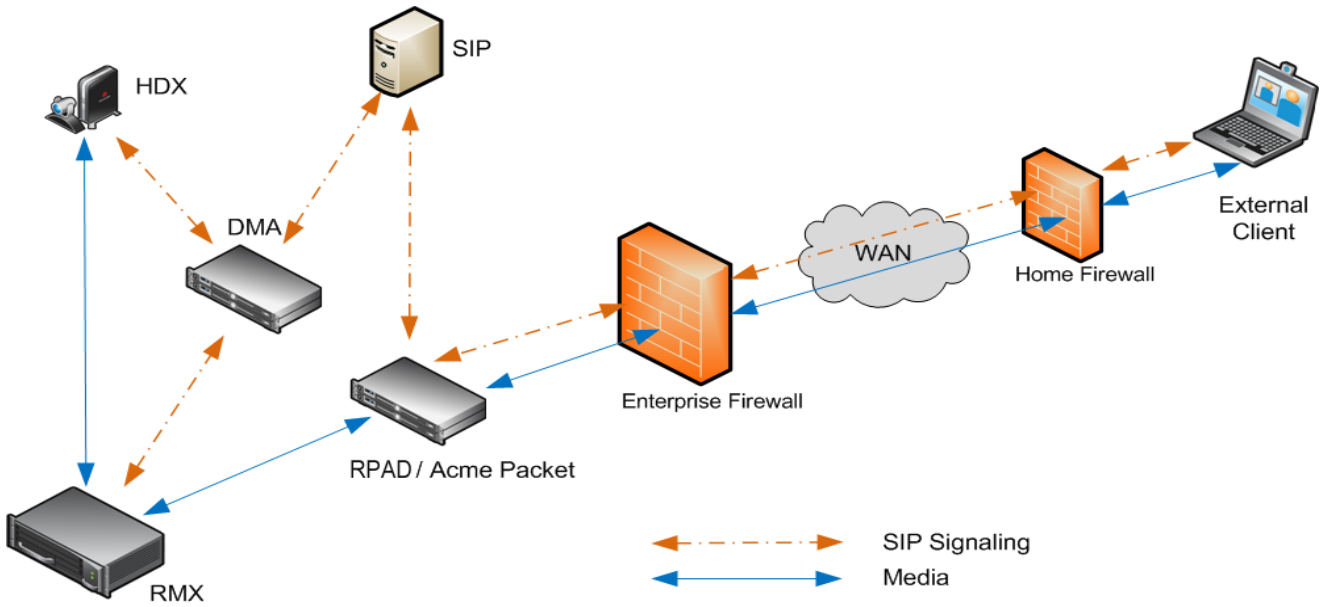
All signaling and media for both SIP and H.323 will be routed through an *SBC*.
The following *SBC* environments are supported:

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

Deployment Architectures

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

Remote Connection Using the Internet

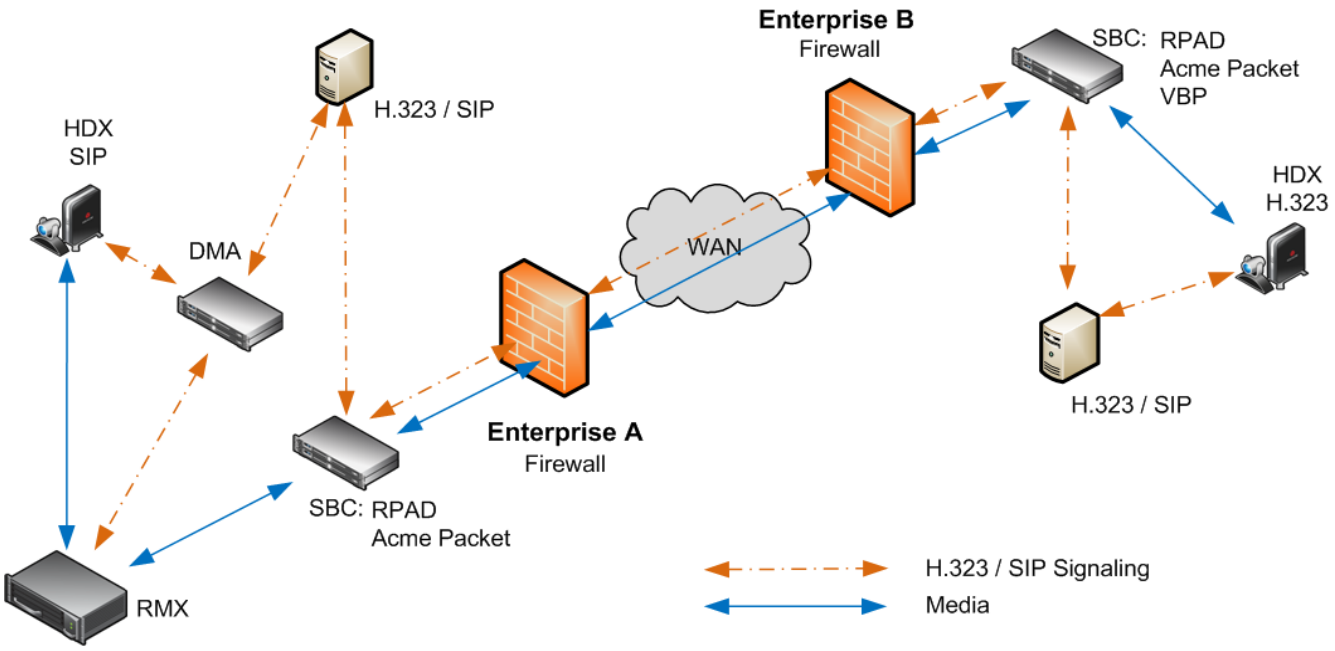


The following *Remote Connection* call flow options are supported:

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

Enterprise Client				CMA Client	
Environment	Registered	SBC		Registered	Environment
SIP / H.323	No	SAM Only	⇆	No	H.323

Business to Business Connections



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

Enterprise A Client				Enterprise B Client		
Environment	Registered	SBC		SBC	Registered	Environment
H.323	Yes	RPAD	⇆	RPAD	Yes	H.323
H.323	Yes	RPAD	⇆	VBP	Yes	H.323
SIP	Yes	RPAD	⇆	RPAD	Yes	H.323
SIP	Yes	Acme Packet	⇆	Acme Packet	Yes	H.323

FW (Firewall) NAT Keep Alive

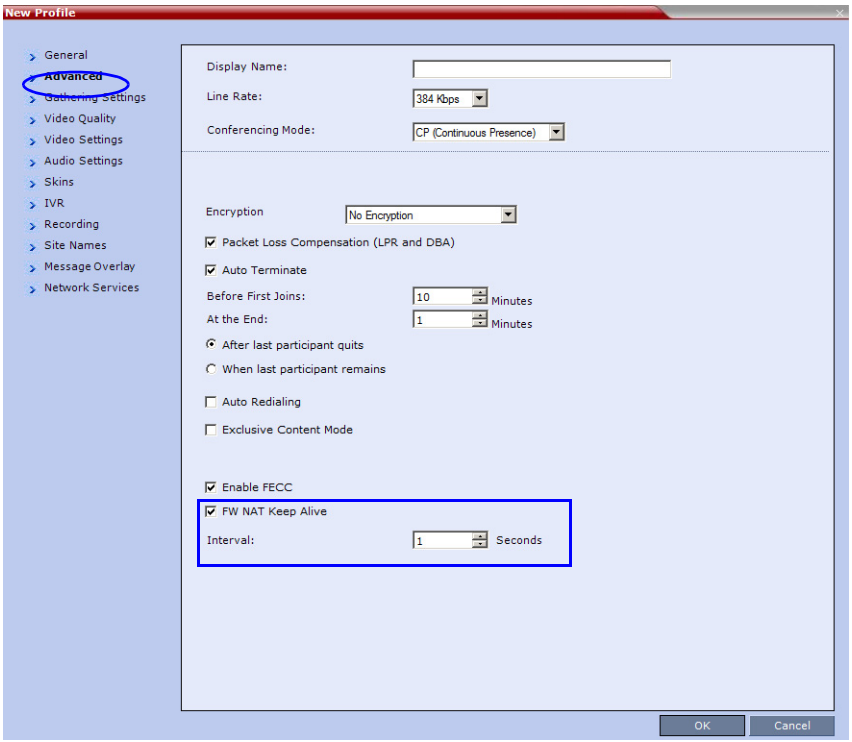
The RMX can be configured to send a *FW NAT keep alive* message at specific *Intervals* for the *RTP, UDP* and *BFCP* channels.

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

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

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

FW NAT Keep Alive is enabled in the *New Profile - Advanced* dialog box.



To enable and modify FW NAT Keep Alive:

1. Select the *FW NAT Keep Alive* check box.
2. If required, modify the *Interval* field within the range of **5 - 86400** seconds.
3. Click OK.

System Configuration in SBC environments

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

For more details on modifying the values of system flags, see "*Manually Adding and Deleting System Flags*" on page **1-18**.

BFCP Over UDP

Support for *BFCP* over *UDP* has been included in this version for improved interoperability with *SIP Clients* that share *Content* using this protocol.

SIP Clients supporting *BFCP* over *UDP*, when connected to conferences on the RMX, can share *Content* with endpoints supporting the following *Content* sharing protocols:

- *BFCP/TCP*
- *BFCP/UDP*
- *H.323/ H.239*
- *H.323 /Polycom People+Content*
- *ISDN Content*

Guidelines

For *SIP Clients* that support both *BFCP/TCP* and *BFCP/UDP*:

- The preferred protocol is *BFCP/UDP*.
- When used in *Cascading* conferences, the *Cascade Link* must be *H.323*.
- *BFCP/UDP* is supported in both *IPv4* and *IPv6* addressing modes.
- *BFCP* utilizes an unsecured channel (port 60002/TCP) even when *SIP TLS* is enabled. If security is of higher priority than *SIP* content sharing, *SIP People+Content* can be disabled. To do this manually add the **ENABLE_SIP_PEOPLE_ PLUS_CONTENT** *System Flag* to the *System Configuration* and set its value to **NO**.
- *SIP People+Content* and *BFCP* capabilities are by default declared to all endpoints. If, however, the endpoint identity is hidden by a proxy server, these capabilities will not be declared by the RMX. Capabilities declaration is controlled by the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag*.

  The default value of the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag* is **YES** resulting in *BFCP* capability being declared with all vendors' endpoints unless it is set to **NO**. When set to **NO**, the RMX will declare *SIP People+Content* and *BFCP* capabilities to *Polycom* and *Avaya* endpoints.
- The **CFG_KEY_ENABLE_FLOW_CONTROL_REINVITE** *System Flag* should be set to **NO** when *SIP BFCP* is enabled.
- If these *System Flags* don't exist in the system, they must be manually added. For more information see "*Modifying System Flags*" on page **1-1**.
- BFCP capabilities are not supported in Microsoft ICE environment.

Dial-out Connections

- For dial-out connections to *SIP Clients*, *BFCP/UDP* protocol can be given priority by adding the adding the **SIP_BFCP_DIAL_OUT_MODE** *System Flag* to *system.cfg* and setting its value to UDP.

The *RMX' s Content* sharing determined by the *System Flag's* settings and *SIP Client* capabilities are summarized in Table 2-37.

Table 2-37 *System Flag - SIP_BFCP_DIAL_OUT_MODE*

<table>
<tr><th rowspan="2">Flag Value</th><th colspan="3">SIP Client: BFCP Support</th></tr>
<tr><th>UDP</th><th>TCP</th><th>UDP and TCP</th></tr>
<tr><td>AUTO (Default)</td><td rowspan="2">BFCP/UDP selected as Content sharing protocol.</td><td>BFCP/TCP selected as Content sharing protocol.</td><td rowspan="2">BFCP/UDP selected as Content sharing protocol.</td></tr>
<tr><td>UDP</td><td>Cannot share Content.</td></tr>
<tr><td>TCP</td><td>Cannot share Content.</td><td colspan="2">BFCP/TCP selected as Content sharing protocol.</td></tr>
</table>

For more information see *the RMX 1500/2000/4000 Administrator's Guide*, "*Manually Adding and Deleting System Flags*" on page **1-18**.

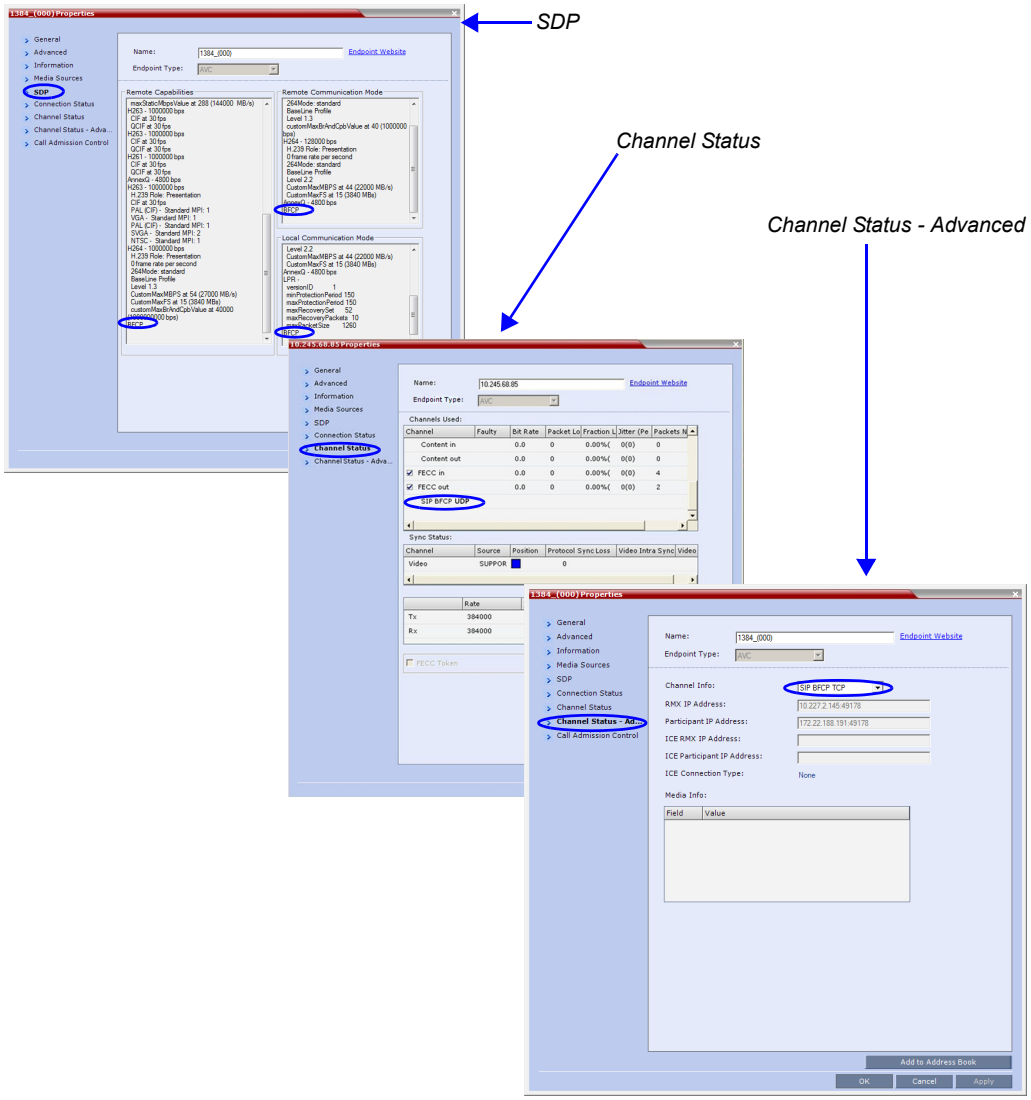
Dial-in Connections

- The RMX will share content with *Dial-in SIP Clients* according to their preferred *BFCP* protocol.
- *SIP Clients* connected as *Audio Only* cannot share *Content*.

Monitoring BFCP

In the *Participant Properties* dialog box, *BFCP* status information appears in:

- All three panes of the *SDP* tab.
- The *Channel Status* tab.
- The *Channel Status -Advanced* tab.



For more information see *the RMX 1500/2000/4000 Administrator's Guide*, "*Participant Level Monitoring*" on page **12-19**.

ICE with Multiple Network Services

In this version, support has been included for *Multiple Network Services* when using *ICE (Interactive Connectivity Establishment*).

One *Network Service* including *ICE* can be configured per media card installed in the RMX as shown in Table 2-38.

Table 2-38 *RMX - Media Cards vs Network Services including ICE*

RMX	Total Media Cards	Network Services (Up to 2 per Media Card)	Network Services that Include ICE (1 per Media Card)
1500	1	2	1
2000	2	4	2
4000	4	8	4

Guidelines

- If *ICE* initialization fails in a *Network Service*:
  - The *Network Service* remains functional but without *ICE* capability.
  - *ICE* capability on media cards that share the same *Network Service* also remain functional but without *ICE* capability.
  - Other *Network Services* with *ICE* capability on other media cards are unaffected.
- A *DNS* server must be specified for each *IP Network Service* that includes *ICE* capability and for the RMX *Management Network Service*.

Version 8.1.4.J Detailed Description - Changes to Existing Features

Multi-Level Address Book

The *Address Book* can be organized into a multi-level hierarchical structure. It can be used to mirror the organizational layout of the enterprises and it is especially suitable for large-scale enterprises with a considerable number of conference participants, organizational departments, and divisions.

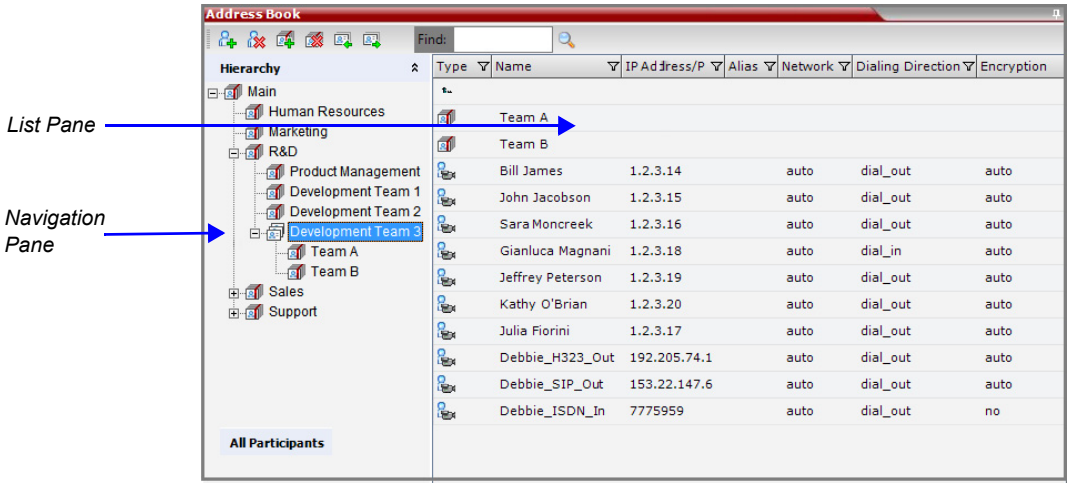
The *Address Book* provides flexibility in arranging conference participants into groups in multiple levels and the capabilities to add groups or participants, move or copy participants to multiple groups within the address book, and use the address book to add groups and participants to a conference or *Conference Template*.

The *Address Book* contains the following types of lists:

- **Hierarchical —** displays a multi-level hierarchical tree of groups and participants.
- **All Participants —** 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 the groups accordingly.

The *Address Book* contains two panes:

- *Navigation pane* - contains the hierarchical tree and *All Participants* list
- *List pane* - displays the list of all the members of the selected group and sub-groups.



Groups in the *Address Book* can contain sub-groups or sub-trees, and individual address book participant entities. Double-clicking a group on the navigation pane displays the group participants and sub-groups in the list pane.

Guidelines

- The multi-level *Address Book* can only be used in a local configuration on the Collaboration Server. The hierarchical structure cannot be implemented with the *Global Address Book* (GAB).
- Adding participants to a conference from the *Global Address Book* is similar to previous versions.
- Up to ten levels can be defined in the hierarchical structure of the address book.
- The default name of the root level is "Main". The "Main" root level cannot be deleted but the root level name can be modified.
- Address book names support multilingual characters.
- Participants in the *Address Book* can be copied to multiple groups. However, only one participant exists in the *Address Book*. Groups that contain the same participants refer to the same definition of the participant entity.

Upgrading and Downgrading Considerations

- When upgrading to a multi-level Address Book version from a single level address book, the following factors have to be taken into consideration:
  - The system automatically creates a new address book with a different name and modifies the new address book to a multi-level hierarchical address book.
  - By default, the address book contains 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.
  - Participants that were not previously associated with any group in the Address Book are placed in the "Main" group.
  - All participants in the address book appear in the "All Participants" group.
  - During the upgrade process, the single-level Address Book file is saved in the system to enable a future the downgrade of the version to a previous, single-level Address Book version (if required).
- When downgrading from a multi-level address book version to a single-level address book version, the multi-level *Address Book* is replaced during the downgrade process by the single-level address book that was saved during the upgrade process.

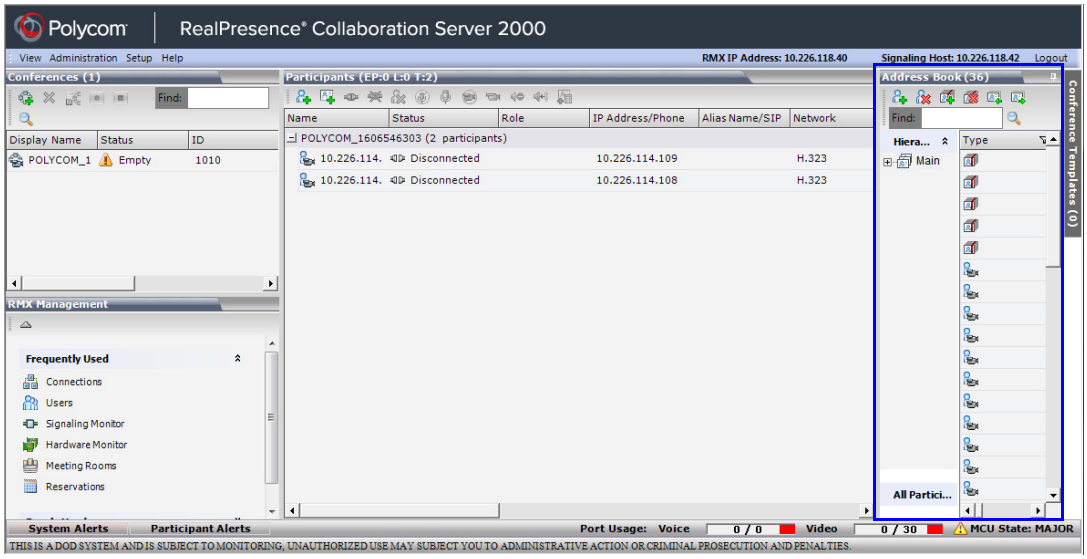
Displaying the Address Book

To display the Address Book:

>> Click the **Address Book** tab on the right of the Collaboration Server window.

The *Address Book* hierarchical tree layout is displayed in the left pane of the *Address Book* pane.

Address book entities and groups associated with the selected group are displayed in the right pane of the *Address Book* pane.



Managing the Address Book

Adding a New Participant

You can add a new participant to the "Main" group or to a group in the *Address Book*. Additionally, you can add a participant from a new conference, ongoing conference, or *Conference Template*.

To add a new participant:

1. In the *Address Book - Navigation* pane, select the group to where you want to add the new participant.
2. Click the **New Participant** button ( ) or right-click the group to where you want to add the participant and select the **New Participant** option.
   - Alternatively, click or anywhere in the *List* pane and select the **New Participant** option.
3. In the *New Participant - General* dialog box, fill in the new participant information. You can select the **Advanced** and **Information** tabs to provide more information about the participant.
4. Click **OK**.

   The participant is added to the selected group.

When adding a participant to the address book from a new conference, *Participants* list of an ongoing conference or *Conference Template*, the participant is added to the "Main" group.

Deleting a Participant

You can delete a participant from the *Address Book*. However, if the participant exists in multiple groups, a message is displayed asking if you want to delete the participant from the selected group or entirely delete the participant from the *Address Book*.

The **Delete Participant** function is not available when selecting multiple participants.

To delete a participant:

1. In the *Address Book* - *Navigation* pane, select the group to where the participant to delete is listed.
2. In the *Address Book* - *List* pane, select the participant you want to delete.
3. Click the **Delete Participant** button or right-click the participant and select the **Delete Participant** option.

   When the participant belongs to only one group, a confirmation message is displayed.

   a. 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.

   b. Select the **Current group** option to delete the participant from the selected group or select the **Address Book** option to permanently delete the participant from the address book (all groups). Click **OK** to perform the delete operation or click **Cancel** to exit the delete operation.

Copying or Moving a Participant

You can copy or move a participant from one group to another group using the **Copy**, **Cut**, and **Paste** options. A participant can belong to multiple groups. However, there is only one entity per participant. Groups that contain the same participants refer to the same definition of the participant entity. Alternatively, you can drag a participant from one location in the *Address Book* to another location, moving the participant to its new location using the drag-and-drop operation.

The cut and copy actions are not available when selecting multiple participants.

To copy or move a participant to another group:

1. Select the participant you want to copy.
2. Right-click the selected participant and select one of the following functions from the drop-down menu:

Table 2-39 Copy/Cut Functions

Function	Description
Copy	Copies the participant to be pasted into an additional group.
Cut	Moves the participant from the current group to a different group. Alternatively, you can move a participant to another location by dragging the participant to the new location.

3 In the *Address Book* navigation pane, navigate and select the group in which you want to paste the participant.

4 Right-click the selected group and click one of the following **Paste** functions from the drop-down menu:

Table 2-40 *Paste functions*

Function	Description
Paste Participant	Creates a link to the participant entity in the pasted location.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "*Copy*" to the end of the participant name.

The Paste functions are only available after a **Copy** or **Cut** action has been implemented.

To drag a participant from an address book group to another group:

1 Select the participant or participants you want to move.

2 Click and hold the left mouse button and drag the selection to the new group.

The participants are moved to the new address book group.

Adding Participants to Conferences

You can add a participant or multiple participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

Multiple selection of group levels is not available.

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

1 Select the participant or participants you want to move to the conference.

2 Click and hold the left mouse button and drag the selection to the Participants pane of the conference.

The participants are added to the conference.

To add a participant to a Conference Template:

1 Select the participant or participants you want to move to the *Conference Template*.

2 Click and hold the left mouse button and drag the selection to the Participants pane of the *Conference Template*.

The participants are added to the *Conference Template.*

Managing Groups in the Address Book

In the *Address Book,* you can use groups to manage clusters of participants that are in the same organizational structure. Groups can contain participants and sub-groups. You can define up to ten levels in the "Main" group.

The currently selected group, whose group members are displayed in the *Address Book List* pane is identified by the a special icon  .

To expand the group to view the group members:

>> Double-click the group name or click the **Expand** button.

The address book entities and sub-groups of the group is displayed in the right group list pane. You can drill down the sub-group to view address book entities in the sub-group.

To move up to the next level and view the members in the upper level:

>> Double-click the **navigation arrow** button in the group members pane.

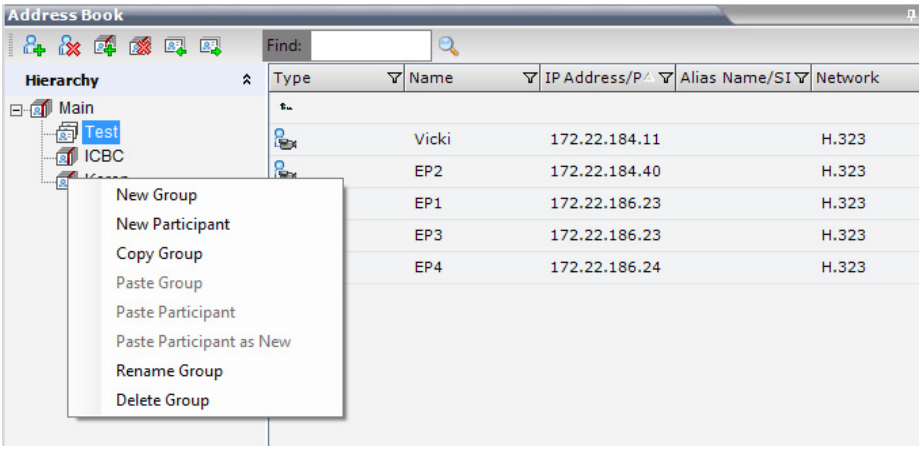
To collapse a group:

>> Double-click the group name or click the **Collapse** button.

To manage the groups in the Address Book:

1 In the *Address Book Navigation* pane, right-click the group you want to manage.

The *Groups* menu is displayed.



2 Select one of the following actions:

Table 2-41 Groups Drop-down Menu Actions

Action	Description
New Group	Creates a new group within the current group.
New Participant	Adds a new participant within the current group.
Copy Group	Copies the current group to be pasted as an additional group.
Paste Group	Places the copied group into the current group. The group name of the copied group is defined with "*Copy*" at the end of the group name. This action is only available after a **Copy Group** action has been implemented.
Paste Participant	Places the copied participant into the current selected group. This action is available after a **Copy** or **Cut** action was activated when selecting a single participant or multiple participants.

Table 2-41 Groups Drop-down Menu Actions

Action	Description
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "*Copy*" at the end of the participant name. This action is only available after a **Copy** action was activated for a single participant.
Rename Group	Renames the group name.
Delete Group	Deletes the group and all of its members. This action displays a message requesting confirmation to delete the group and all members connected with the group.

Additionally, you can drag a group from one location in the *Address Book* to another location, moving the group and all its members, including sub-groups, to its new location using the drag-and-drop operation. Moving a group to a new location can be done in the navigation pane or the list pane.

To drag a group from a location in the address book to another location:

1. Select the group you want to move.
2. Click and hold the left mouse button and drag the selection to the new location. The new location can be either the "Main" root level or another group level.

   The group and all its members (participants and groups) are moved to the new address book location.

Adding Groups to Conferences

You can add a group of participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

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

1. Select the group you want to move to the conference.
2. Click and hold the left mouse button and drag the selection to the *Participants* pane of the conference.

   The participants in the group level and all sub-levels are added to the conference.

To add a participant to a Conference Template:

1. Select the group you want to move to the *Conference Template*.
2. Click and hold the left mouse button and drag the selection to the *Participants* pane of the *Conference Template*.

   The participants in the group level and all sub-levels are added to the *Conference Template*.

Searching the Address Book

You can search the *Address Book* for a participant's name or a group name only on the level on which you are currently selected.

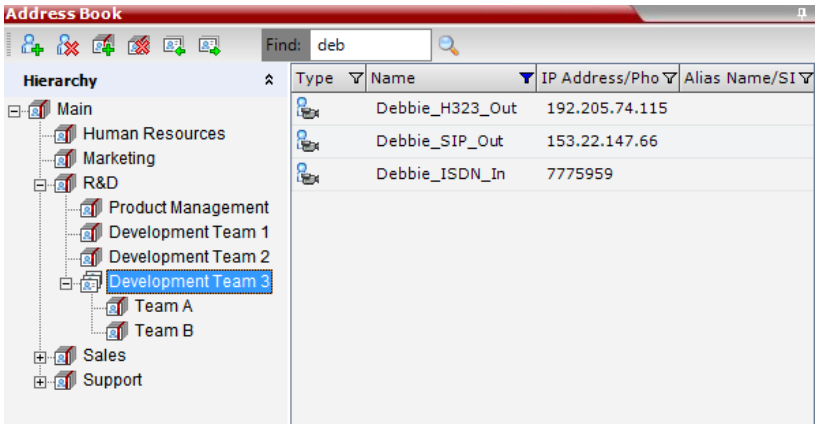
To search for participants or groups in the current selected level:

1. In the *Address Book Navigation* pane, select the group/level within to run the search.
2. In the *Address Book* toolbar, activate the search option by clicking the **Find** field.

The field clears and a cursor appears indicating that the field is active.

3 Type all or part of the participant's name or group name and click the search button.

The closest matching participant entries are displayed and the Active Filter indicator turns on.



Obtaining the Display Name from the Address Book

The MCU can be configured to replace the name of the dial-in participant as defined in the endpoint (site name) with the name defined in the Address Book.

In this process, the system retrieves the data (name, alias, number or IP address) of the dial-in participant and compares it first with the conference defined dial-in participants and if the endpoint is not found, it then searches for the endpoint with entries in the address book. After a match is found, the system displays the participant name as defined in the address book instead of the site name, in both the video layout and the RMX Web Client/ Manager.

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.

Guidelines

- Only Users with *Administrator* and *Operator* Authorization Levels are allowed to enable and disable the *Obtain Display Name from Address Book* feature.
- This feature is supported only for IPv4 participants.

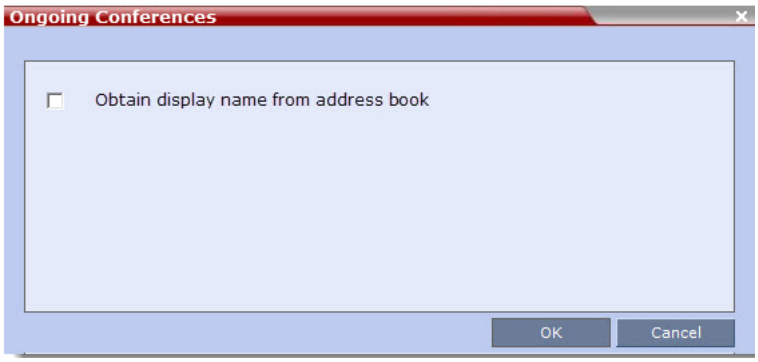
Enabling and Disabling the Obtain Display Name from Address Book Feature

The *Obtain Display Name from Address Book* option can be enabled for all participants connecting to the MCU if the name of the participants are defined in the Address Book.

To enable or disable the Obtain Display Name from Address Book option:

1 On the RMX main menu bar, click **Setup > Customize Display Settings > Ongoing Conferences**.

The *Ongoing Conferences* dialog box is displayed.

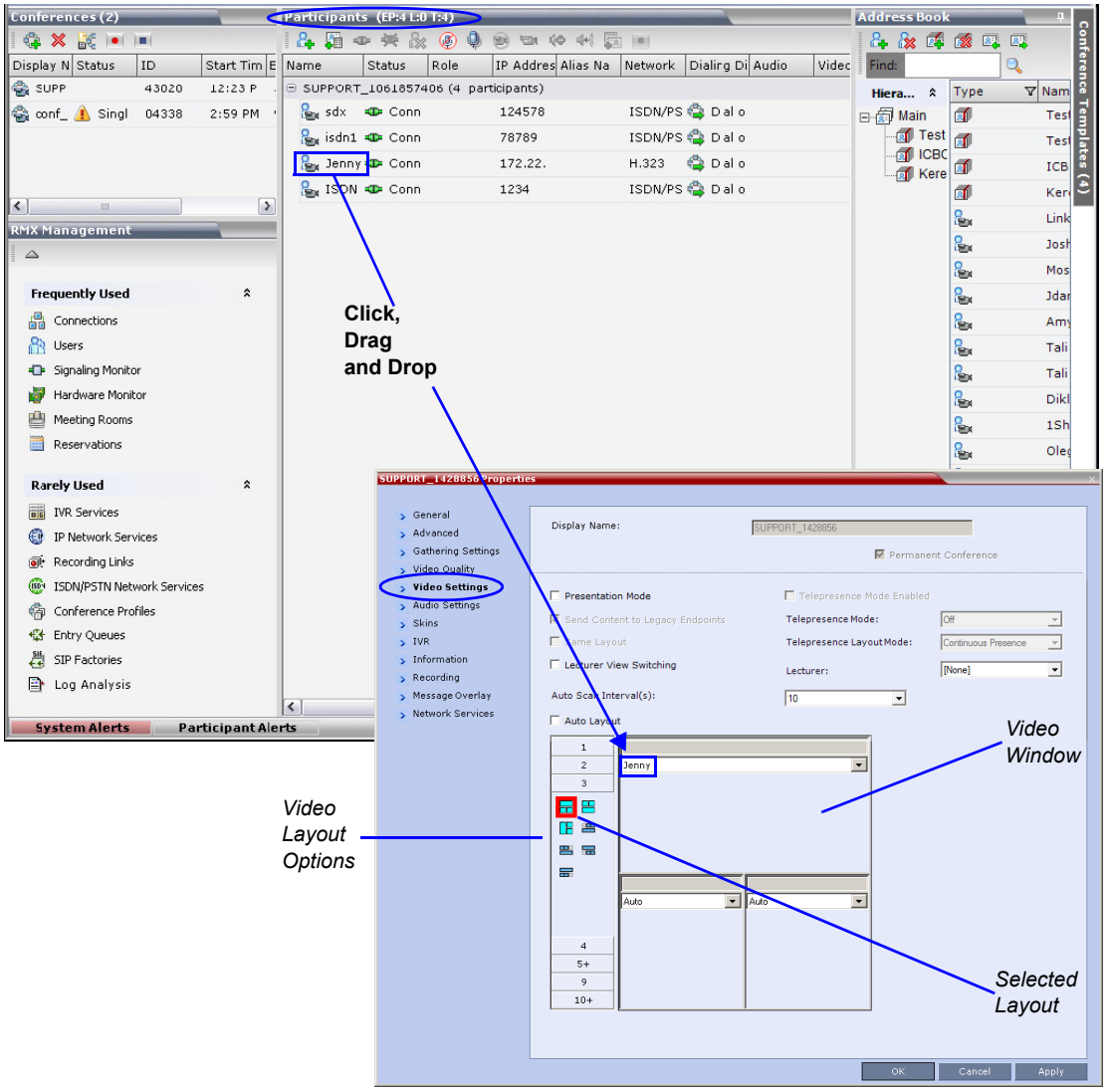


2 Select the **Obtain display name from address book** check box to enable the feature or clear the check box to disable the feature.

3 Click **OK**.

Interactive Video Forcing

Participants in ongoing conferences can be interactively forced to a *Video Window* in the conference layout by using *Drag and Drop*. The administrator can click, drag and drop a participant from the conference's *Participants* list into a specific window of an ongoing conference's *Video Layout*.



Guidelines

- A participant can only be placed in one window in the layout.
- The window header is updated with the participant's name.
- A participant that has been placed multiple times will appear in the last window selected. The window that the participant was previously placed in reverts to an **Auto** state.

- Only one participant at a time can be dragged into a *Video Layout*. If multiple participants are selected and dragged, only the first participant in multiple selections will be placed in the *Video Layout*.

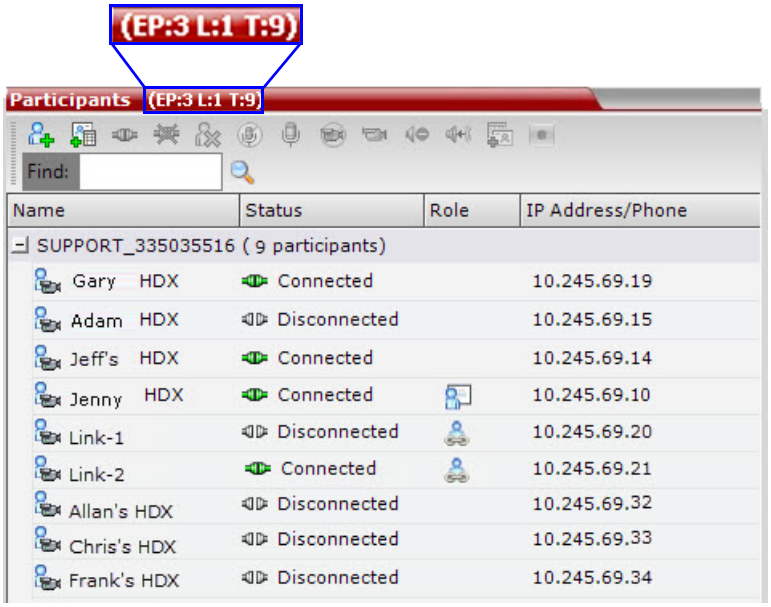
Dragging a Participant to the Video Layout Window

To drag a participant into a video layout window:

1. In the *Conferences* pane, right-click the conference that you want to modify.
2. In the drop-down menu, select **Conference Properties**.
3. In the *Conference Properties* dialog box, select the **Video Settings** tab.
4. Click and drag the participant from conference's *Participants* list into the required window of the *Video Layout*.

Participant Connection Status

Real-time connection status information of *Endpoints* and *Cascade Links* in the selected conference is provided to *Collaboration Server Web Client* and *Collaboration Server Manager* users.



The participant connection status is represented by three numbers in the *Participants* list header in the format **EP:n L:n T:n** where:

- **EP** = the number of *Endpoints* currently connected to the conference (both defined and undefined participants). This number includes participants whose status is *connected with problem*, *connected partially* or *connected as secondary*. Connected *Cascading Links* are not included and are detailed separately.
- **L** = the number of *Cascading Links* currently connected to the conference.
- **T** = the total number of all:
  - connected *Participants* - both defined and undefined participants
  - defined participants that are currently disconnected

- *Cascading Links* - both connected and disconnected

Guidelines

- If more than one conference is selected, the **EP:n L:n T:n** numbers reflect the cumulative connection status information of all the selected conferences.
- If no conference is selected, the **EP:n L:n T:n** numbers are all zeroed.

Customized Content Rate

Customized Content Rate is an additional *Content Setting* that allows manual definition of the *Conference Content Rate*.

This functionality can be implemented when a *Conference Content Rate*, that is automatically calculated by the *RMX*, may not be suitable in a *Cascaded Environment*, where conference line rates may vary widely between the cascaded conferences. For example, one conference may have a line rate of 4 Mbps, and the other a line rate of is 512 Kbps.

In previous versions the *Conference Content Rate* was selected from a predefined table according to the *Content Setting*:

- **Graphics** – default mode, for standard graphics
- **Hi-res Graphics** – requiring a higher bit rate, for high quality display or highly detailed graphics
- **Live Video** – highest bit rate, for video clips or live video display

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide "SIP BFCP Content Capabilities"* on page **3-2**.

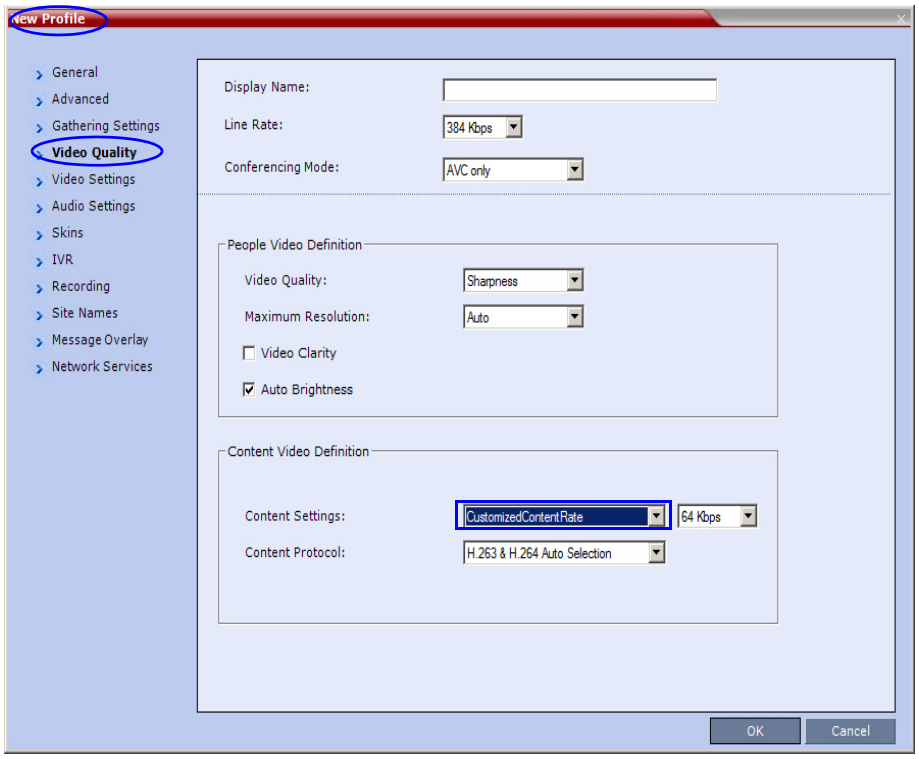
Guidelines

- Cascaded conferences may have different *Conference Line Rates*.
- The *Customized Content Rate* must be the same for all cascaded conferences.

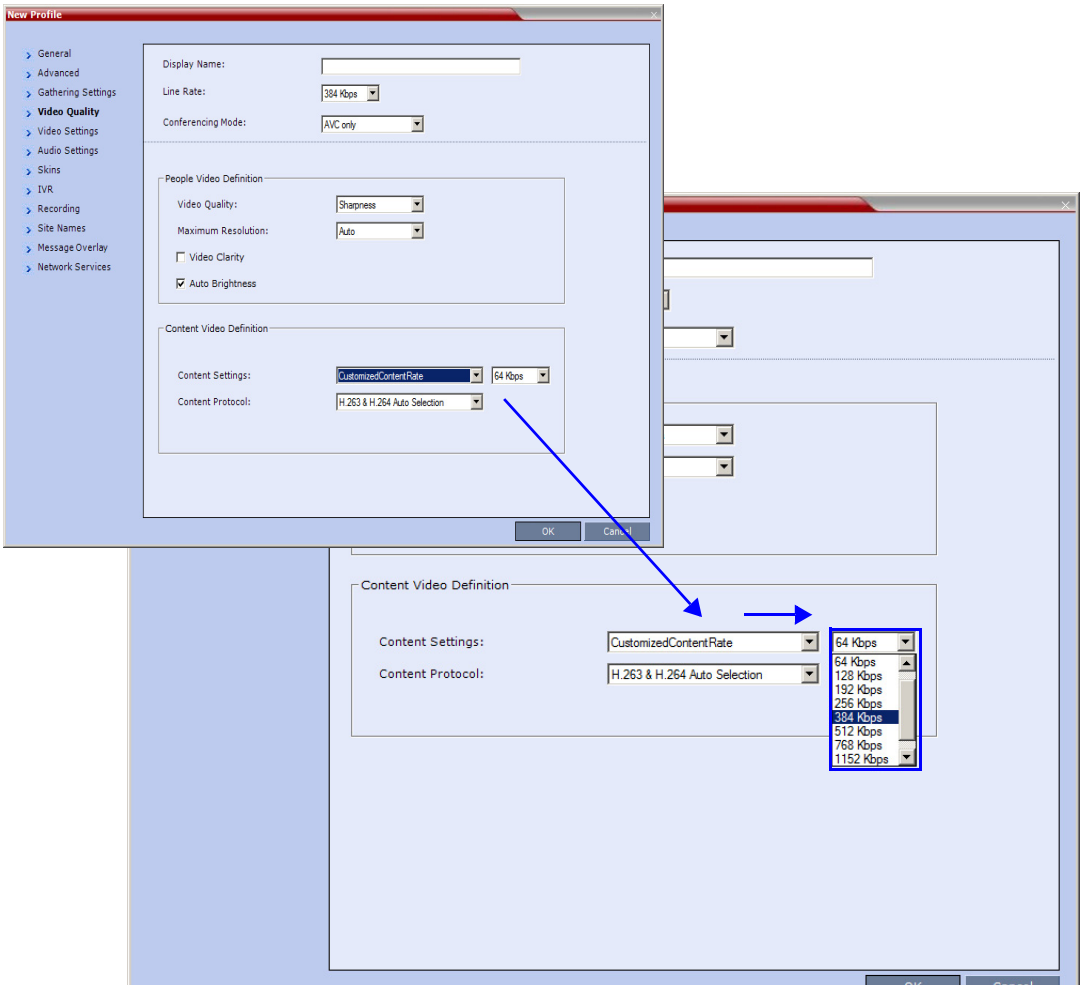
Selecting a Customized Content Rate

Selecting a Customized Content Rate

Customized Content Rate is enabled in the *New Profile - Video Quality* dialog box.



When *Customized Content Rate* is selected, a drop-down menu of the available *Conference Content Rates* is displayed. These *Content Line Rates* are based on and will vary according to the selected *Conference Line Rate*. The largest selectable *Content Line Rate* is 66% of the *Conference Line Rate*.



If the *Conference Line Rate* is 64 Kbps or 96 Kbps, the only available *Conference Content Rate* is **0**, indicating that *Content* is not supported at these rates.

If the administrator selects a *Conference Line Rate* (after selecting *Customized Content Rate)* that is too low to support the selected *Customized Content Rate*, the following error message is displayed:
The selected Conference Line Rate is too low to support the selected Content Line Rate. Click Cancel and reconfigure either of the Line Rates or click OK to return to the default Content Setting.

The administrator can then modify either the *Content Line Rate* or the *Conference Line Rate* or select another *Content Setting* option.

H.264 Cascade Optimized

If *H.264 Cascade Optimized* is the selected *Content Protocol*, a *Cascade Resolution* must be selected.

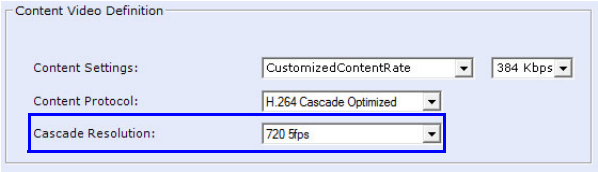


Table 2-42 lists the *Cascade Resolutions* available for the various *Conference Content Rates*.

Table 2-42 *H.264 Cascade Optimized - Cascade Resolutions*

H.264 Cascade Optimized			
Conference Content Rate (Kbps)	**Available Resolutions***		
64	HD720p5 Content Not Supported		
128	HD720p5		
192	HD720p5		
256	HD720p5		
384	HD720p5		
512	HD720p5	HD720p30	
768	HD720p5	HD720p30	HD1080p15
1152	HD720p5	HD720p30	HD1080p15
1536	HD720p5	HD720p30	HD1080p15

*The default resolution for all *Content Rates* is *HD720p5*.

Active Alarms Reduction

A better quality experience has been provided to reduce the number of Active Alarms generated by the RMX. Several of the Active Alarms have become faults, which does not affect the system stability.

The following alarm has been removed from the RMX Alarms:

- Incorrect Ethernet Settings

The following Active Alarms have been modified from Major Error level to System Message level:

- External NTP servers failure
- No ISDN/PSTN Network Services defined

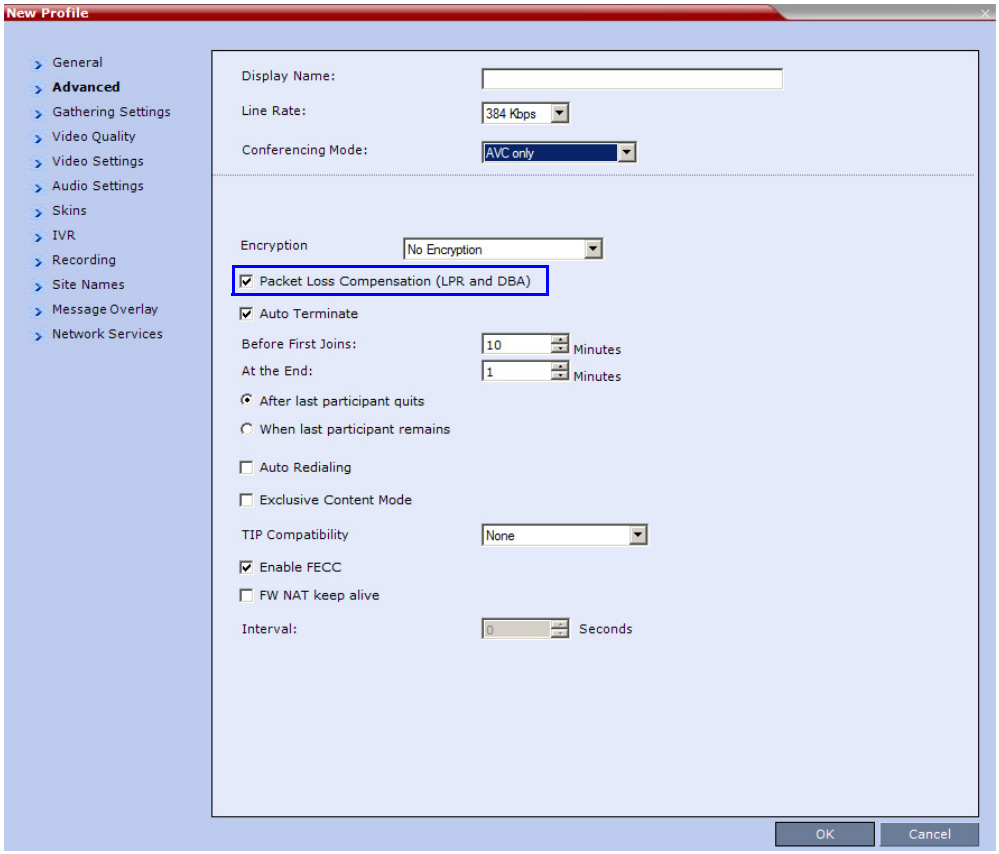
- Red Alarm
- Yellow Alarm
- Failed to connect to SIP registrar
- SIP registrations limit reached
- Failed to access DNS server
- Insufficient UDP Ports
- No clock source

The following Active Alarms have been moved to the Faults List:

- Resource process did not receive the Meeting Room list during startup
- Task terminated
- Low Processing Memory
- Low system Memory
- High system CPU usage
- Used for testing the Active Alarms mechanism
- High CPU utilization
- Process idle
- Failed to open Apache server configuration file
- Failed to save Apache server configuration file
- A private version is loaded
- NTP synchronization failure
- Invalid date and time
- Smart Report found errors on hard disk
- Invalid MCU Version
- Music file error
- Unspecified problem
- Unit not responding
- Failed to mount Card folder
- The Log file system is disabled
- Action redirection failure
- Process terminated
- Terminal initiated MCU reset
- Internal MCU reset
- MCU reset
- MCU reset to enable Diagnostics mode
- Startup process failure
- Polycom default User exists. For security reasons, it is recommended to delete this User and create your own User.
- Single clock source
- MCU is not configured for AVF gatekeeper mode

Packet Loss Compensation (LPR and DBA)

The *LPR* (*Lost Packet Recovery*) check box in the *New Profile - Advanced* and *Profile Properties - Advanced* dialog boxes has been renamed *Packet Loss Compensation* (*LPR and DBA*). The new name indicates that both mechanisms are used simultaneously to compensate for packet loss.



CDR Changes

Multi-part CDR

By default, the maximum CDR (Call Data Record) file size is limited to 1MB. When a *CDR* file reaches a size of 1MB the file is saved and further call data recording is stopped and the additional data is lost.

The Collaboration Server can be configured to keep recording the data in multiple CDR file set of 1MB each. *Multi-Part CDR* ensures that conference call data from long duration or permanent conferences is recorded and not lost.

Guidelines

- *Multi-Part CDR* is enabled by setting the value of the **ENABLE_MULTI_PART_CDR** *System Flag* to **YES**.

  The flag's default value is **NO**.

  When the flag value is **NO,** *CDR* file size is limited to one file of 1MB and further call data recording is stopped.

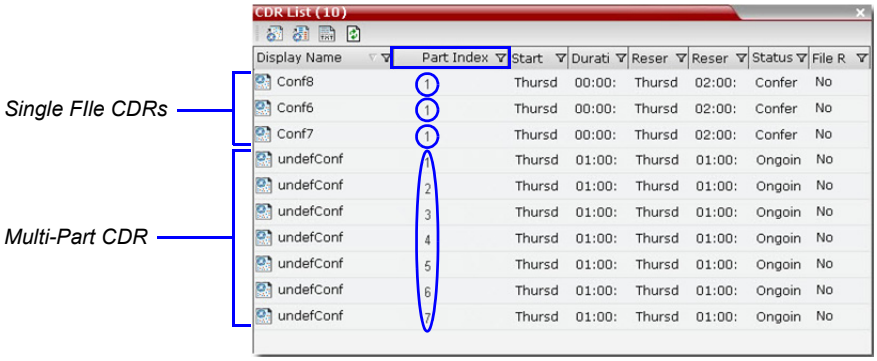
  To modify the default setting, the flag must be manually added to the *System Configuration*. For more information see the *RealPresence Collaboration Server 800s Administrator's Guide*, "*Modifying System Flags*" on page **1-1**.
- If the flag value is set to **YES**, when a *CDR* file reaches 1MB, an additional *CDR* file is created and added to the *CDR* file set for that conference.
- If the flag value is changed from **YES** to **NO** (or visa versa) all existing *CDR* files are retained.

Accessing Multi-Part CDR Files

The *CDR* files are accessed using the Collaboration Server menu by clicking **Administration > CDR** to display all the *CDR* records stored in the Collaboration Server.

Changes to the CDR list

An additional column, *Part Index*, has been added to the CDR list.



The *Part Index* column displays the *CDR* file's sequence in the CDR file set:

- *CDRs* that are up to 1MB consist of a single file. Each file has a unique *Display Name* and a *Part Index* of **1**.
- Files included in a *Multi-Part CDR* file sets have the same *Display Name*. The first file of the set is numbered **1** with each additional *CDR* file numbered in an ascending numeric sequence.

New CDR Event 34

A new *event*, **Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION** was added to the *CDR* file.

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.

The event includes the following fields:

Table 2-43 *Event fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Maximum Bit Rate	The maximum bit rate used by the participant during the call.
Maximum Resolution	The maximum resolution used by the participant during the call. **Note:** The reported resolutions are: CIF, SD, HD720, and HD1080. Other resolutions are round 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.

Gateway Redial

Additional *Redial* options and *IVR* messages have been included for *Gateway Calls* to numbers that are wrong, adding functionality to the *RMX's Gateway* capabilities when used in conjunction with communication servers (*H.323, SIP, ISDN)* such as *Polycom's CMA* and *DMA*.

Guidelines

- *Redial* with *IVR* is supported:
  - With *MPMx* cards.
  - In *CP* environments only.
  - For *H.323, SIP* and *ISDN* calls.
  - When using the *RMX's Inviting Participants using DTMF* functionality.
- *Redial* with *IVR* is not supported:
  - When using *PCM's Invite Participant* functionality.
  - Dialing multiple destination numbers.

Redial on Wrong Number

In previous versions, calls to wrong numbers were disconnected, with no redial attempts or IVR messages.

In this version, an *IVR* message is played requesting the user to enter a new number, followed by up to five redial attempts. If all redial attempts fail, the user is alerted by an *IVR* message that the dialed number is unreachable, followed by reorder tone and disconnection.

Wrong Destination Number

- The number of re-dial attempts is controlled by the **WRONG_NUMBER_DIAL_RETRIES** *System Flag.*

  The default number of redial attempts is **3**. To modify the number of redial attempts, manually add the flag to *system.cfg* and set its value to the number of redial attempts required.

  The flag value range is **0-5**. A flag value of **0** means that no redials are attempted. For more information about *System Flags* see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Manually Adding and Deleting System Flags"* on page **1-18**.
- Redial attempts follow the same order as defined in the *Gateway Profile*: *H.323,* followed by *SIP,* followed by *ISDN*. For more information about *Gateway Profiles* and *Gateway Dial out Protocols* see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Defining the Gateway Profile"* on page **19-18**.
- *Redial on Wrong Number* is activated if a *Gateway Call* fails, for all defined protocols, for any reason or combination of reasons listed in Table 2-44.

***Table 2-44** Call Failure Reasons - H.323, SIP, ISDN*

H.323	SIP	ISDN
Unreachable Destination	484 - Address Incomplete	3 - No Route to Destination
Bad Format Address	404 - Not Found	18 - No User Responding
Adaptive Busy	414 - Request-URI Too Long	28 - Invalid Number Format
Admission Rejected (ARJ) Reason: Request Denied Item 1: Cannot find location.	416 - Unsupported URI Scheme	41 - Temporary Failure
Admission Rejected (ARJ) Reason: Called Party Not Registered	420 - Bad Extension	
	421 - Extension Required	

The user receives the *Redial on Wrong Number IVR* message: "*Incorrect destination. Please enter the destination number*".

If all the redial attempts fail the user receives the *Disconnect on Wrong Number IVR* message: "*Destination could not be reached; call is disconnected*".

- *Gateway Re-dial* is not activated if the reason for call failure is *Busy* or *No Answer*, for any of the defined protocols.

Wrong Destination Number Time-out

- A *time-out* counter is started when the *Redial on Wrong Number* message is played. If the user does not enter another destination number within the time-out period it is considered a failed dial out attempt.

- The *Redial on Wrong Number* message and *time-out* are repeated according to the value of the **WRONG_NUMBER_DIAL_RETRIES** *System Flag*. If there is no input from the user, after completing the retries, the user receives the *Disconnect on Wrong Number IVR* message: "*Incorrect destination number*" followed by the *Reorder Tone.*

Disconnect on Busy

As in previous versions, redialing of calls to busy destination numbers can be selected. The number of redial attempts is dependent on the **NUMBER_OF_REDIAL** *System Flag*, the default value is **3**. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Defining New Profiles*" on page **2-20**.

In previous versions, if all retry attempts failed, there were no further call attempts with no notification.

When using this version, if all retry attempts fail, the user receives the *Disconnect on Busy* message in the form of *Busy Tone*. The call is then disconnected.

Disconnect on No Answer

In previous versions, if a call failed due to no answer at the destination, the call was disconnected with no notification.

When using this version, if all retry attempts fail, the user receives the *Disconnect on No Answer* message in the form of *Reorder Tone*. The call is then disconnected.

Disconnect on Wrong Number

In previous versions, if a call failed due to no answer at the destination, the call was disconnected with no notification.

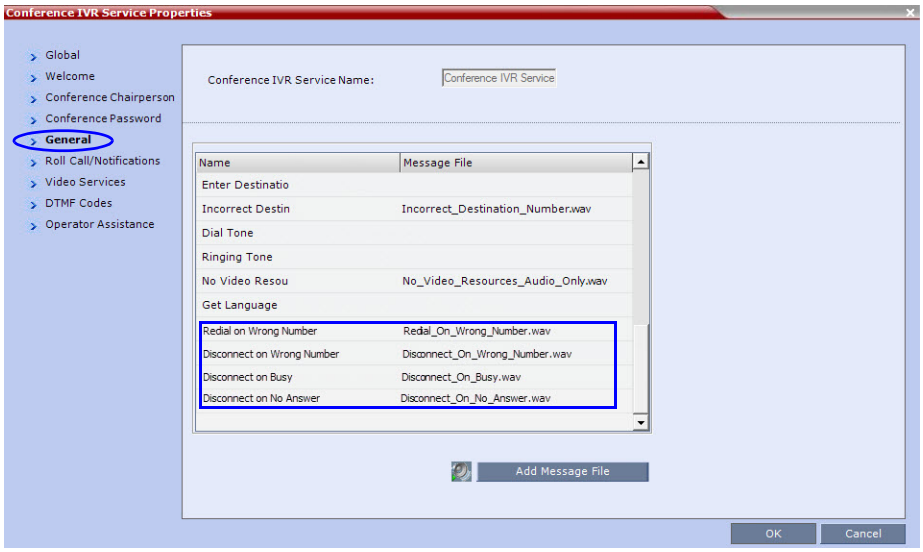
When using this version, the user receives the *Disconnect on Wrong Number IVR* message: "*Incorrect Destination Number*" followed by *Reorder Tone*. The call is then disconnected.

New IVR Messages

There are 4 new *IVR Messages*:

- *Redial on Wrong Number*
- *Disconnect on Wrong Number*
- *Disconnect on Busy*
- *Disconnect on No Answer*

IVR Messages are assigned and modified in the *General* tab of the *Conference IVR Service* or *Conference IVR Properties* dialog box.



For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"IVR Services"* on page **1-1**.

H.323 & SIP Protocol Flag Options

Changes have been made to the proprietary H.323, SIP protocols, and updates are provided to each of the protocols based on their standard.

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 RMX, 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, Table 3 lists the SIP timer types for each flag setting and their corresponding timeout values in milliseconds.

Table 3 *SIP Timer Types & their Values*

SIP TIMER Types	Value (in milliseconds)	
	POLYCOM (flag default)	Standard Recommended
T1	50000	500
T2	20000	4000
TimerB	35000	32000
TimerC	35000	60000
TimerD	32000	32000
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

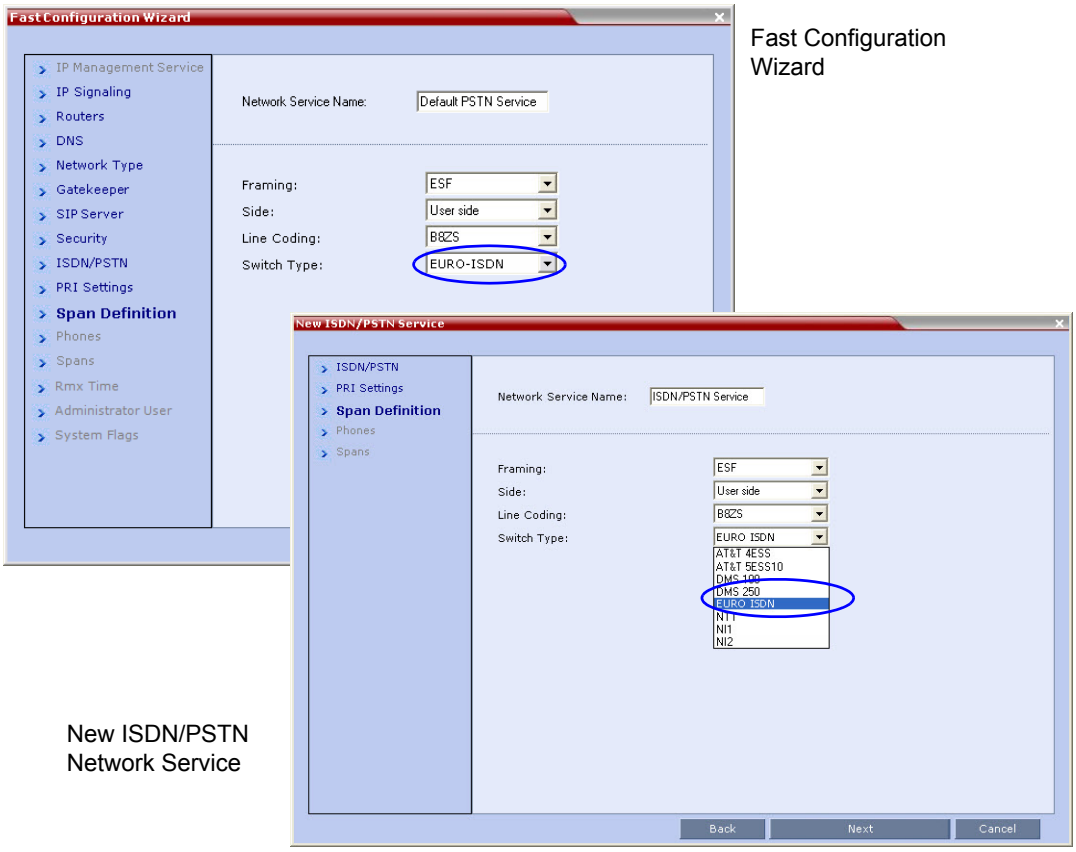
Possible values:

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.

New Euro ISDN Switch Type

A new T1 *Switch Type* has been added: EURO ISDN for Taiwan.
When configuring the Fast Configuration Wizard or a new ISDN/PSTN Network Service select the *Span Definition* tab and then select EURO ISDN from the *Switch Type* box. For T1 configurations in Taiwan, Framing must be set to *ESF* and Line Coding to *B8ZS*.



New ISDN/PSTN Network Service

For EURO ISDN use in Taiwan, *Framing* must be set to **ESF** and *Line Coding* to **B8ZS**.

CDR Changes

CDR List Additions

In the CDR List two new fields, *GMT Start Time* and *File Retrieved* have been added.

- The *GMT Start Time* CDR field registers the start time of each conference according to Greenwich Mean Time (GMT).

- The *File Retrieved* CDR field is updated whenever the record is downloaded using any of the file retrieval buttons in the CDR List pane. The *File Retrieved* CDR field indicates:
  - **Yes** - when the conference record was retrieved to any file or using the API.
  - **No** - when the conference record was not retrieved at all.

Unformatted CDR Files - GMT Offset

Two fields in the *Unformatted CDR* files, previously unsupported, are now supported.

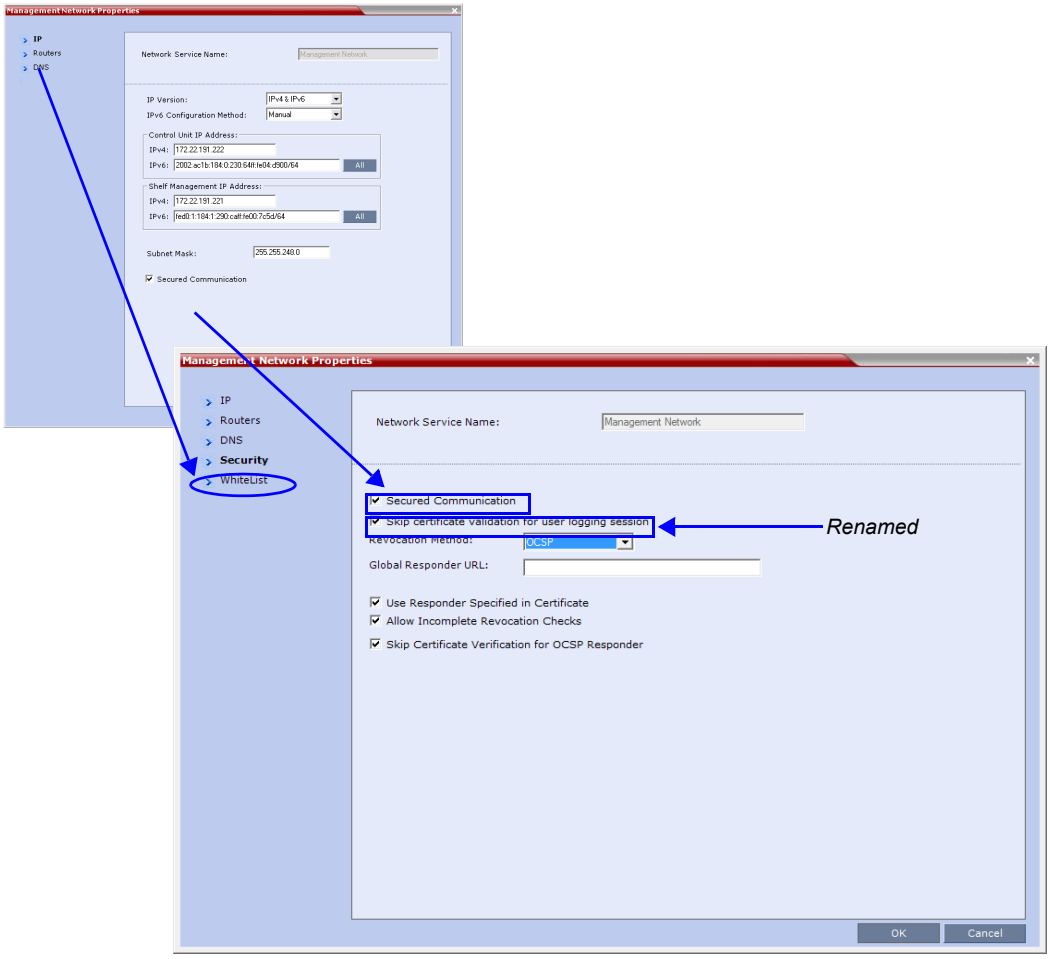
Table 4 *GMT Offset fields*

Field	Description
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.
GMT Offset	The time zone difference between Greenwich and the RMX's physical location in hours and minutes. Together with the *GMT Offset Sign* field the *GMT Offset* field is used to define the RMX local time. For example, if the *GMT Offset Sign* is 0 and *GMT Offset* is 3 hours then the time zone of the RMX'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 RMX's physical location is +4, which will be subtracted from the GMT time to determine the local time.

Changes to the Management Network Dialog Box

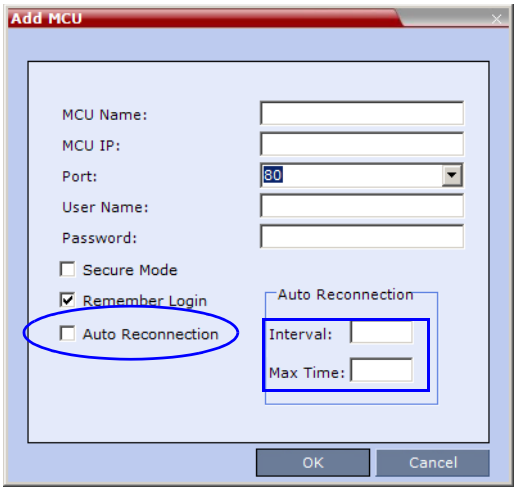
The following changes have been made to the *Management Network* dialog box:

- The *Secured Communication* check box has been moved to the *Management Network - Security* tab from the *Management Network - IP* tab.
- The *Request Peer Certificate* check box has been renamed *Skip certificate validation for user logging session*.



RMX Manager - MCU Auto Reconnection

The option to automatically reconnect an MCU that was disconnected from the RMX Manager was added to the *Add MCU* dialog box.



To enable the *Auto Reconnection* option, the following parameters are used:

Table 5 *New MCU Properties*

Field	Description
Auto Reconnection	Select this check box to automatically reconnect to the RMX if the connection between the RMX Manager and the MCU is broken.
Interval	Enter time in seconds between reconnection attempts to the RMX. For example, if you enter 10, the system will wait 10 seconds between the connection attempts.
Max Time	Enter the maximum amount of time in seconds that the RMX is allowed to try to reconnect. If the RMX reconnects before the allotted time frame the count down timer is halted. For example, if you enter 100, the system will stop trying to reconnect if it has failed to do so within 100 seconds.

Corrections and Known Limitations

Corrections Between Version 7.5.2.J and Version 8.1.4.J

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J*

#	Key	Category	Description	Detected in Version	Workaround
1	BRIDGE-243	Interoperability	In a conference with HDX and ITP endpoints registered to an IOS gatekeeper and a CTS endpoint registered to CUCM, after 30 minutes into the conference the CTS endpoint is disconnected.	V7.8.0	
2	BRIDGE-254	General	On the RMX, CUCM registered endpoints are listed with the conference name: "RMX CUCM" instead of listing the conference type display name.	V7.8.0	
3	BRIDGE-352	Recording	A recording link cannot be created using an IPv6 address.	V7.8.0	
4	BRIDGE-353	Audio	After an RMX is reset CTS rooms connect the first time without audio. Subsequent connections have audio.	V7.8.0	
5	BRIDGE-422	General	During a CP conference, when sending Closed Caption from an HDX endpoint to mixed SIP and H.323 endpoints, they do not receive Closed Caption.	V7.8.0	
6	BRIDGE-501	*RMX Manager*	RMX Manager failed to install from login page.The request is aborted with the message: “Could not create SSL/TLS secure channel”.	V7.5	1. Install RMX Manager before initiating Secured Communications Mode. *2. Install from a network.* 3. Install locally from RMX Manager folder.
7	BRIDGE-533 VNGR-25118	Interoperabilityx	A Sony PCS-G50 is unable to send content when connected over H.323 to a conference running on RMX 1500.	V7.8.0	
8	BRIDGE-587 VNGR-25041	Video	During a SD conference with a 256 Kbps line rate set to Video Quality Optimized, Sharpness and H.239 High Resolution Graphics, the Video Out Frame for many HDX 7000/HDX 9004 endpoints rate was 14.	V7.8.0	
9	BRIDGE-670	Software Version	Manual connection can take up to 30 seconds to begin in 2048kbps conference, with manual dial out to over 80 participants.	V7.8.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
10	BRIDGE-673 VNGR-25680	Interoperability	When the RMX 2000 and HDX and HDX endpoints are registered with a Siemens OSV when dialing out using SIP, OpenScape Desktop audio only endpoints disconnect.	V7.8.0	
11	BRIDGE-783	Interoperability	OTX layout changes in a Telepresence Enabled conference. OTX displays local video on two screens. CTS view of OTX is correct.	V7.8.0	
12	BRIDGE-817	Unified Communication Solution	Participant Properties Channel Status of CTS3000 Endpoint Slave video channels contain no information during conference. CTS3000 connects to non-encrypted, 1080p, 3584kbps, TIP Video+Content, CP, conference through DMA. Master Channel information is displayed.	V7.8.0	
13	BRIDGE-915 VNGR-20637	IP	On an RMX 1500 with Multiple Services enabled, when configuring the Network service to support LYNC and OCS servers, the Linux DNS configuration can support only a single network.	V7.8.0	
14	BRIDGE-1621	General	In Auto Scan, the order of the endpoints for customized polling is other than the order in which the endpoints connected to the conference.	V7.8.0	
15	BRIDGE-1657	Software Version	In Customized Polling, a disconnected and reconnected participant is not displayed last in the polling queue.	V7.8.0	
16	BRIDGE-1793	Interoperability	Video cannot be displayed on RPM v1.3.x when connecting to a conference running on RMX Version 7.8.	V7.8.0	
17	BRIDGE-1806	General	In an encrypted 384Kbps conference with 3 participants, when invoking DTMF, the DTMF tones can be heard by the other participants.	V7.8.0	
18	BRIDGE-2035	General	All RealPresence Desktop SVC clients in one SVC conference disconnect automatically after 4 hours.	V7.8.0	
19	BRIDGE-2041	General	In the Address Book, the Alias column is always blank regardless of what is defined in the participant properties dialog box.	V7.8.0	
20	BRIDGE-2250	General	When more than 20 SVC RPD participants are connected to SVC Only conference, an assert may be displayed after many frequent speaker changes.	V7.8.0	
21	BRIDGE-2302	General	Dial in H.323 endpoint in Video Switching conference is not moved from the Entry Queue to the Conference due to password failure.	V7.8.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
22	BRIDGE-2334	Interoperability	Siptask core dump occurs after several endpoints dial in to an AVC Virtual Meeting room via an RPAD Session Border Controller through 3G/wireless ADSL network.	V7.8.0	
23	BRIDGE-2391	Interoperability	When the RMX dials out to an Avaya One XC the call is disconnected immediately after being answered.	V7.8.0	
24	BRIDGE-2429	Partners - Microsoft	When MS ICE environment is enabled, HDX endpoint on a non-ICE call is disconnected from the conference due to MCU Internal Problem . Only one HDX can connect.	V7.8.0	
25	BRIDGE-2476	Video	Sometimes cyclic video freezes and predator video are seen on HDX endpoints and Polycom Group series endpoints when connected to an encrypted conference at a line rate of 768Kbps.	V7.8.0	
26	BRIDGE-2516	General	When creating two SVC only conferences, one set to a line rate of 768kbps and the other to 1920 kbps and connecting participants to both conferences simultaneously, after about 50 SVC participant connections, the MPMx card running the conferences crashed.	V7.8.0	
27	BRIDGE-3206	*Content*	Content cannot be shared due to BFCP UDP negotiation failure.	V7.7	
28	BRIDGE-3207	*Content*	Content cannot be shared due to BFCP UDP negotiation failure.	V7.7	
29	BRIDGE-3543	*CPU*	When the logger level is increased, high CPU usage occurs.	V8.1	
30	BRIDGE-3949	*Interoperability*	An endpoint connecting with TIP could not mode from the Entry Queue to a Meeting Room when the ID was entered while the prompt music was playing.	V8.1	
31	BRIDGE-4312	*Software Defect*	Slides are cropped when the resolution of the slide does not match that of the conference.	V7.8	
32	BRIDGE-4400	*General*	A conference password cannot have repeated characters.	V8.1	Change the MAX_CONF_PASSWORD_REPEATED_DIGITS flag to a higher number.
33	BRIDGE-4483	*Interoperability*	When a CTS 1300 dials into an encrypted VMR for the first time, in the *RMX Web Client* the endpoint's connection status is, "Connected With Problems".	V8.1	Dial back into the conference

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
34	BRIDGE-4534	*Interoperability*	When many participants dial into a conference all at once, one of the TIP endpoints heard participant music despite being in the conference.	V8.1	
35	BRIDGE-4582	*Interoperability*	A secure conference with only CTS participants displayed jumpy video.	V8.1	
36	BRIDGE-4694	*Interoperability*	An HDX dialing into a conference using ITP and was the first participant to join, did not receive the audio message, “You are the first person to join the conference.”	V8.1	
37	BRIDGE-4697	*Interoperability*	When an HDX 4500 connected to a conference with 2 CTS 3010 endpoints with encryption set to “encrypt when possible”, video quality was bad.	V8.1	
38	BRIDGE-4784	*Interoperability*	In a conference with 3 HDX’s mimicking an OTX connecting to a TIP HD1080 conference, the left and right endpoints’ connection statuses in the *RMX Web Manager* are, “Connected With Problem”.	V8.1	
39	BRIDGE-4786	*Interoperability*	An HDX using TIP did not see the welcome slide or hear an IVR messages.	V8.1	
40	BRIDGE-4889	*Interoperability*	In a dial-in SIP conference using SBC with a CTS3010, HDX, OTX, TX9000, and Lync endpoints, content sent from the CTS3010 was not received. In addition, a core dump was produced after 1.5 hours.	V8.1	
41	BRIDGE-4918	*Interoperability*	In a dial-in conference, the OTX sends choppy audio.	V8.1	Mute the slaves.
42	BRIDGE-4981	*MCU*	In a conference with a Chairperson required and passcodes needed for both chairpersons and regular participants, the regular participants were able to join the conference and hear each other before the chairperson joined.	V8.1	
43	BRIDGE-4982	*Interoperability*	Calls from OTX and CTS3010 using a passcode result in the side video screens connecting with the wrong payload type.	V8.1	
44	BRIDGE-4983	*MCU*	When the MCU hosted a 24 hour conference, participants were not able to connect to the MCU.	V8.1	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
45	BRIDGE-5535	Network	Call to AS-SIP registered RMX4000 meeting room, connected with problem when calling from AS-SIP registered GS endpoint.	8.1.4	Before plugging the network cables in, ensure sure that the network infrastructure containing all the devices (including the RMX) has two different networks: one for management; the other for signaling & media. Separation can be achieved either by two physical networks or by two virtual networks (VLANs).
46	BRIDGE-5386	*Software Defect*	In a mixed mode conference using a DMA, a Lync client with the CSS add-on enabled was disconnected after a RealPresence Desktop client connected as SVC.	V8.1.4	
47	BRIDGE-6157	*Software Defect*	In an SVC only 1920 kbps conference with 5 RealPresence Desktop participants connecting via an SVC only 1920 kbps Entry Queue, content could not be seen by any participant.	V8.1.6	
48	BRIDGE-6329	*Software Defect*	No video or audio on connected Tandberg C20 endpoint when FW NAT Keep Alive is enabled on MCU.	V8.1.6	
49	BRIDGE-6402	Software Defect	During a 2MB SVC conference launched from the DMA, after a blast dial-out of many endpoints, the MPMx card crashes.	V8.1.7	
50	BRIDGE-6420	Software Defect	During an AVC conference launched from the DMA, after an SIP RPD dial-in endpoint connects, audio, video and content problems occur.	V8.1.6	
51	BRIDGE-6591	Software Defect	Video speeds up intermittently on RP Desktop endpoint in SVC-only conference via DMA.	V8.1.7	
52	BRIDGE-6636	*Software Defect*	SVC GroupSeries endpoint with encryption cannot dial into ongoing call if call has Encrypt When Possible mode set.	V8.1.7	Conference should be Encrypted or Non-Encrypted.

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
53	BRIDGE-6661	*Software Defect*	Cascade link remains disconnected for approximately 2 minutes and resources are not released when ongoing conference is deleted on Master RMX.	V7.8.0	Re-connect after approximately 2 minutes.
54	BRIDGE-6789	*Interoperability*	In a mixed mode AVC-SVC 768 kbps non-encrypted conference with 12 dial-out HDX's connecting using AVC and 1 GroupSeries dialing in using SVC, the GroupSeries frequently does not see the AVC endpoints.	V8.1.7	
55	VNGR-23713	Security	Secure communications between RMX and Machine Account User cannot be established if FQDN field on the RMX does not match the FQDN name in the Machine Account User' certificate (including case) exactly.	7.5.1	
56	VNGR-20136	*Interoperability*	In an RMX 384Kb conference with a Cascaded MGC when H.323 and MPI participants connect to the conferences the cascaded link connects as Secondary.	7.5	
57	VNGR-20062	*Serial Gateway*	Only 108 out of 160 ports can connect to RMX4000 with MPM+80 cards. The next participant attempting connection is disconnected due to resource deficiency.	V7.5	
58	VNGR-19998	*Ultra Secure Mode*	MPM card becomes un-responsive after Card Software Recovery Procedure is performed while the RMX is in Ultra Secure Mode.		Remove and re-insert the MPM card while the system is running.
59	VNGR-19722	*General*	Audio card fails to initialize during startup on RMX4000 resulting in no utilizable unit for audio controller.	V7.5	Reset the RMX.
60	VNGR-18414	*RMX Manager*	Active Directory user cannot open the Hardware Monitor section in the RMX Manager.	7.5	
61	VNGR-18278	*Upgrade Process*	No access to RMX 2000 after software upgrade from version 7.0.2.61 to version 7.0.2.64.	V7.0.2	
62	VNGR-18257	*Diagnostics* FIX VERIFIED	Software verification failure is indicated when running diagnostics on RMX 1500 (MPMx card).	V7.0.2	
63	VNGR-18242	*Upgrade Process*	When upgrading RMX4000 with 4 MPM+ cards from Version 7.0.0.162 to Version 7.0.2.61 Two of the MPM+ cards remain in startup mode and do not complete the upgrade.	V7.0.2	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
64	VNGR-18106	*Video*	Empty cells are displayed in the video layout when connecting 30 HDX 8006 endpoints at a line rate of 4MB and resolution of 1080p to a conference running on RMX 2000 with 2 MPMx-D cards.	V7.0.2	
65	VNGR-17881	*Hardware*	RTM IP does not reconnect to logger port.	V7.0.2	
66	VNGR-17869	*Hardware*	When inserting a Control Unit in Slot 4, in Hardware Monitor it is shown as inserted in slot 3	V7.0.2	
67	VNGR-17861	*RMX Manager*	RMX Manager fails to install from RMX Web Client login page.The request is aborted with the message: "Could not create SSL/TLS secure channel".	7.5	1. Install prior to initiating Secured Communica-tions Mode 2. Install from a network. 3. Install locally from RMX Manager folder.
68	VNGR-17857	*Video*	Sometimes the Gathering text is not displayed when connecting SIP and H.323 endpoints to a conference running on RMX 2000 with MPMx at a line rate of 1920kbps.	V7.0.2	
69	VNGR-17851	*Hardware*	Sometimes connection with RTM ISDN is lost.	V7.0.2	
70	VNGR-17841	*Video*	Lip sync occurred when an endpoint connected at 512kbps to a conference running at line rate of 2MB on RMX 2000 with 2 MPM+80 cards, and LPR enabled and active due to packet loss.	V7.0.2	
71	VNGR-17833	*IVR*	RadVision Scopia XT1000 and Lifesize Room 200 remain in the IVR Welcome stage when connecting to a CP conference running at 4096kbps with Encryption and LPR enabled. Other endpoints connected normally.	V7.0.2	
72	VNGR-17823	*Interopera bility*	No cropping, no border and shrunken video is displayed on the VVX endpoint when connecting a VVX endpoint, HDX endpoint and a Telepresence endpoint to a conference set to telepresence mode that is running on RMX 2000 with MPMx cards.	V7.0.2	
73	VNGR-17796	*Video*	A thin gray line is present at the bottom of the cells when connecting TPX and RPX endpoints to a conference running on RMX 2000/4000 with MPMx cards at a line rate of 3MB or higher and video quality is set to sharpness.	V7.0.2	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
74	VNGR-17768	*Upgrade Process*	When upgrading or downgrading the RMX 1500 software version and adding the activation key, the RMX Web Client disconnects from the RMX.	V7.0.2	
75	VNGR-17762	*Content* FIX VERIFIED	Sometimes Content is sent during the gathering phase and is shown through the gathering phase slide background (it is displayed as a layer underneath it) when the Sent Content to Legacy Endpoint option is enabled in a conference running at 384kbps.	V7.0.2	
76	VNGR-17753	*Partners - Microsoft*	In Microsoft Lync environment with ICE enabled, when the RMX 4000 with MPM+80 dials out to two Lync Clients (MOC1 with Creative Camera connected and MOC2 with CX5000 RoundTable connected), MOC1 does not receive video from MOC2.	V7.0.2	
77	VNGR-17749	*Interoperability*	Flickering video is displayed for a few seconds on Lifesize Room 200 screen when connecting to a conference running on RMX 4000 at 4MB with Encryption and LPR enabled.	V7.0.2	
78	VNGR-17742	*Video*	Poor video quality due to low frame rate is viewed on HDX systems when connecting to a CP conference running on RMX 2000 with MPMx at a line rate of 6MB, with LPR, Video Clarity and Gathering options enabled.	V7.0.2	
79	VNGR-17729	*Content*	Video freeze was experienced by many participants when content was sent from a PC to 160 CIF participants connected to a conference running on RMX 2000 with MPM+80 at a line rate of 384kbps and LPR and Encryption options enabled.	V7.0.2	
80	VNGR-17714	*General*	Occasionally, RMX 4000 with MPM+ automatically resets when running conferences. The system displays the Active Alarm: NEW_VERSION_INSTALLED: A new version was installed. Reset the MCU, although a new version was not installed.	V7.0.2	
81	VNGR-17708	*IVR*	HDX8006 and HDX9006 remain in the IVR Welcome stage when connecting to a Video Switching conference running at 4MB with Video Quality set to Motion and video resolution set to 720p 60 fps.	V7.0.2	
82	VNGR-17671	*Content* FIX VERIFIED	Content sent from a VSX7000A system. is displayed frozen on the far end VSXs when connected over H.323 to a conference with 9 H323 VSX endpoints running on RMX4000 with the MPM+ at a line rate of 768kbps and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
83	VNGR-17657	*Video*	The VVX takes over a minute to resume live video on other endpoints in conference after releasing the hold when connected over H.323 to a conference running on RMX 1500 at a line rate of 128kbps.	V7.0.2	
84	VNGR-17652	*Interoperability*	After resuming the call that was placed on hold, VVX 1500 display does not return to Auto Layout and remains small in the top right corner of the display. The VVX is connected via H.323 to a conference running at 128Kbps.	V7.0.2	
85	VNGR-17646	*Video*	H.261 participant video is not seen by other conference participants and the Gathering text did not appear on the H.261 participant's screen when connected to a conference running at 512kbps. The H.261 participants sees the conference video correctly.	V7.0.2	
86	VNGR-17645	*ISDN*	Video artifacts (video stream is superimposed on the IVR Welcome slide) when an ISDN participant connects to a conference running on RMX 2000 with MPMx at a line rate of 384kbps.	V7.0.2	
87	VNGR-17636	*Interoperability*	VVX is displayed in two conference video layout cells when connected over H.323 to a conference that includes two VVX endpoints when the VVX comes off hold while in the gathering screen. One cell is live video and the other cell is frozen video.	V7.0.2	
88	VNGR-17635	*ISDN*	The video of ISDN participants freezes during a conference running at a line rate of 256kbps on RMX 2000 with MPMx and Encryption and LPR options enabled.	V7.0.2	Set the conference to a Line rate other than 256Kbps.
89	VNGR-17633	*SIP*	Incorrect display name of the RMX is displayed on SIP endpoints. RMX Display name includes additional characters and not just the URI.	V7.0.2	
90	VNGR-17631	*Partners - Microsoft*	RMX does not identify the OC/4 version (Lync Server 2010/OCS-W14), hence the wrong video settings are used (4CIF instead of CIF).	V7.0.2	
91	VNGR-17616	*Audio*	HDX H.323 endpoint receives G.722 audio instead of Siren22 (as the SIP endpoints) when connected to a conference running at a line rate of 384kbps on RMX4000 with MPM+ and the CS_ENABLE_EPC flag is set to YES.	V7.0.2	
92	VNGR-17615	*IVR*	iPower 9000 remains in the IVR Welcome stage when connecting to a CP conference running at 384kbps with Video Quality set to Motion and Video Clarity, Encryption, LPR and Send Content to Legacy Endpoint options enabled.	V7.0.2	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
93	VNGR-17611	*Video*	Video seen on HDX8006/7006 screen looks superimposed and blotchy after changing the video layout to full screen when connected via H.323 to a conference running on RMX 2000 with MPMx at a line rate of 384kbps and Encryption and LPR options enabled.	V7.0.2	
94	VNGR-17606	*Interoperability*	LifeSize systems are sometimes locking up and disconnecting when connected to a CP conference running on RMX 4000 with MPM+ at a line rate of 1920kbps, video quality set to Sharpness and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	
95	VNGR-17602	*RMX Manager*	Double clicking on a card in Hardware monitor of the RMX Manager application displays the Card Properties dialog instead on the Processor Properties dialog box.	V7.0.2	
96	VNGR-17589	*Interoperability*	RadVision Scopia XT1000 is connected with a problem to a conference running on RMX 2000 with MPMx at a line rate of 4MB and LPR and Encryption enabled after viewing the IVR Welcome slide.	V7.0.2	
97	VNGR-17580	*Video*	Site names are blinking when connecting H.261/263 participants to the conference.	V7.0.2	
98	VNGR-17574	*ISDN*	Internal ISDN\PSTN Audio Only calls get a loud noise (static/pop) prior to the start of the IVR message.	V7.0.2	
99	VNGR-17562	*SIP*	The QDX6000 SIP endpoint is connected with problem to a conference running on RMX 4000 with MPM+ at a line rate of 768kbps and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	
100	VNGR-17559	*Interoperability*	Sony PCS-XG80 cannot connect to RMX 2000/1500 with MPMx over SIP.	V7.0.2	
101	VNGR-17520	*General*	In MPMx Card Configuration Mode, the High Profile Sliders in the Resolution Configuration dialog box are set to the minimum and do not show the actual values for the predefined Resolution Configurations.	V7.0.2	
102	VNGR-17517	*General*	"Insufficient resources" with "Power off problem" errors occur when 15 HDX 8006 and 10 HDX 9004 that are connected to a conference at a line rate of 4096kbps are muted and unmuted individually and then the conference layout is changed.	V7.0.2	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
103	VNGR-17514	*Video*	An empty cell is displayed in the video layout when muting and then unmuting individual endpoints that are connected to the conference as follows: 10 ISDN at a line rate of 128kbps, 7 HDX 8006 at a line rate of 4096kbps, 15 HDX 9004at a line rate of 1024kbps and 15 VSX 384kbps.	V7.0.2	
104	VNGR-17496	*General*	DSP recovery and asserts occur, endpoints are disconnected or lose both audio and video on RMX4000 running V7.0.1.16 with 4*MPM+80 cards.	V7.0.1	
105	VNGR-17484	*Video*	Periodic video freezes on H.323 endpoints when connected to a CP conference running on RMX 1500 at a line rate of 4096kbps and AES and LPR options enabled.	V7.0.2	
106	VNGR-17471	*Audio*	Loss of audio for 2-3 seconds or bursts of static noise on HDX6000 endpoint in calls dialed via DMA to RMX4000 running V7.0.1.16 with, 4*MPM+80 cards	V7.0.1	
107	VNGR-17436	*General*	Unit recovery of unit 14, board 1 occurred.	V7.0.1	
108	VNGR-17377	*Video*	High Profile enabled HDX 8000 remains in the Gathering layout with frozen video inside the cells after blast dial out to several endpoints of type HDX 8000/ HDX 9004 / HDX 4000/ VSX 8000/ VSX 3000 from a CP conference at a line rate of 512kbps and LPR enabled.	V7.0.2	
109	VNGR-17363	*Video*	Endpoint connects at a higher resolution than expected according to the Resolution Slider configuration when line rate of the endpoint is forced to a lower rate than the conference rate. For example, if the conference line rate is 1024kbps and the endpoint line rate is forced to 512kbps, the endpoint resolution upon connection will be 720p instead of SD (as if it was connected at 1024Kbps).	V7.0.2	
110	VNGR-17302	*Video*	Black screen with normal audio occurs on HDX8002 endpoint that dialed via DMA to RMX2000 running V7.0.1.16 with 2*MPMX cards.	V7.0.1	
111	VNGR-17291	*Video*	In a Dial-in Meeting Room, endpoints viewed impaired video and occasionally received bad audio.	V7.0.1	
112	VNGR-17282	*Video*	In a DMA Dial-in Meeting Room with several HDX8000 endpoints, video transmission stopped.	V7.0.1	
113	VNGR-17272	*Video*	In a DMA Dial-in Meeting Room with several endpoints, HDX9004 viewed distorted video from other endpoints	V7.0.1	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
114	VNGR-17221	*Interoperability*	Video from CMA-D participant was not displayed in call dialed via DMA to RMX4000 running V6.0.0.105 with 4*MPM+80 cards.	V6.0	
115	VNGR-17220	*Video*	documentation: Horizontal black lines are displayed across the video window on all endpoints in calls dialed via DMA to RMX4000 running V6.0.0.105 with, 4*MPM+80 cards.	V6.0	
116	VNGR-17215	*Video*	In a Dial-in Meeting Room with mixed (HDX8000/ 9004) endpoints, the endpoints viewed zebra video.	V7.0.1	
117	VNGR-17156	*Video*	In a DMA dial-in Meeting Room with several endpoints, a few endpoints viewed Zebra video artifacts.	V7.0	
118	VNGR-17148	*Video*	Participant is seen blurred when connecting with QVGA resolution to a conference layout of 1+7.	V7.0.1	
119	VNGR-17139	*Video*	In a DMA 2Mb dial-in conference with LPR enabled and 20 mixed endpoints (HDX, VSX, CMAD H323, PSTN), three DSP video failures occurred and frozen video was viewed on two HDXs.	V7.0	
120	VNGR-17099	*General*	Extraneous "Total Number of Event Mode Resources" field is displayed in the System Information properties box.		
121	VNGR-17073	*Interoperability*	Loss of lip sync occurs on HDX9004 endpoint talking to an HDX9000 endpoint in 2Mbps conference with the following mix of endpoints: H323, PSTN, PVX, CMAD, HDX, dialed in via DMA with LPR on, Gathering Off, Echo suppression on.	V7.0	
122	VNGR-17070	*Audio*	On an RMX 4000 with MPM+ cards, when running a 512 Kbps conference with mixed HDX 8000 and VSX 3000 endpoints, audio cuts ON and OFF.	V7.0	
123	VNGR-16968	*PCM*	PCM is not supported with MPMx Cards.	V7.0	
124	VNGR-16960	*Interoperability*	Call on RMX 2000 with MPMx using HDX endpoint connects at 128Kbps with resolution HD720p even if RMX call rate is set for 8Mb.	V7.0	
125	VNGR-16958	*Video*	During a 128Kbps conference with AES, Gathering, Motion, Send Content to Legacy Endpoints and Auto Layout enabled, empty layout cells, poor video and video stills occur in HDX, VSX, Lifesize endpoints.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
126	VNGR-16955	*Interoperability*	iPower 9000 endpoint in H.323 call with RMX with MPM+ or MPMx does not transmit audio in encrypted calls.	V7.0	
127	VNGR-16954	*Upgrade Process*	On an RMX4000 after upgrading to version 7.0, build 148, the RMX "Could not complete MPM Card startup procedure".	V7.0	
128	VNGR-16952	*Video*	During a 1472Kbps conference with LPR, AES, Gathering, Send Content to Legacy Endpoint and Auto Layout enabled, the video of VSX7000 and HDX8006 endpoints does not appear in the conference layout.	V7.0	
129	VNGR-16947	*Recording*	In a conference running at 384Kbps and Gathering is enabled, recording is set to "Upon request" the recording is started once the gathering phase ends, resulting in the display of the Gathering slide and layout without text details and after 15 seconds the Gathering slide and layout remain and appear in the recording.	V7.0	
130	VNGR-16944	*Video*	Conferences running at a line rate of 768 and 1024Kbps with Gathering enabled may display distorted font and discolored background at 432x240, 512x288, 848x480 and 720x400 resolutions.	V7.0	
131	VNGR-16943	*Interoperability*	The Gathering slide turns green after changing layout on ViewStations when ViewStation SP Release 7.5.4.16 SP and ViewStation 512k Release 7.5.4.17 are connected to a conference running on RMX2000 with MPM+ at a Line Rate of 384Kbps, LPR, Same Layout and Auto Layout are enabled.	V7.0	
132	VNGR-16938	*Interoperability*	Using Tandberg MXP endpoints, artifacts and choppy occur in video for 10 seconds after 1mbps H.323 or SIP connection to RMX 1500.	V7.0	
133	VNGR-16935	*Audio*	On RMX 1500, running 384kbps conference, an endpoint connected with ##FORCE_MEDIA_ASIREN14_24K or ##FORCE_MEDIA_ASIREN14_32K connects with a SIREN14_48K audio algorithm. An endpoint connected without force connects using G.711 audio algorithm.	V7.0	
134	VNGR-16934	*General*	When a H.323 call is released without lobby conn_id parameter, call memory is possibly not released.	V7.0	
135	VNGR-16928	*ISDN*	On RMX 1500, dial out from 256kbps conference to ISDN endpoint forced to 1920 kbps displays green screen and disconnects with "Internal MCU Problem".	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
136	VNGR-16925	*Interoperability*	Avaya 1XC Softphone intermittently partially connects to conference RMX when connecting as 2nd or subsequent participant.	V7.0	
137	VNGR-16924	*Interoperability*	In DMA, when a SIP endpoint is connected to a certain MCU, and the user chooses to stop using it, the call is routed to a different MCU while the call rate is reduced by 64k.	V7.0	
138	VNGR-16919	*Audio*	On RMX with MPMx using H.323 with HDX endpoint, sites do receive Siren14 instead of Siren22 Stereo audio algorithm 6Mbps VSW conferences.	V7.0	
139	VNGR-16894	*Interoperability*	When the privacy shutter of a VVX1500 endpoint is closed, a mosaic is displayed instead of a black screen.	V7.0	
140	VNGR-16890	*General*	Log Analyzer output from RMX 1500/2000 with MPMx contains numerous CRT ART errors.	V7.0	
141	VNGR-16889	*Interoperability*	On RMX 1500 Video Preview - View Participant Received Video of VSX3000 endpoint is displayed as a green screen. Problem occurs at 384kbps, feature works correctly at higher call rates.	V7.0	
142	VNGR-16886	*Upgrade Process*	On an RMX 1500/2000/4000 with MPMx cards, when upgrading to version 7.0 to build 139 and implementing the Diagnostic mode the MPMx card status remains in a "startup" phase.	V7.0	
143	VNGR-16880	*Video*	When connecting HDX & VSX endpoints to a mixed ISDN & IP 4096Kbps conference with Auto Terminate, Encryption, LPR, Sharpness, Auto Layout, Same Layout and Video Clarity enabled, running on an RMX 2000 with MPM+ cards, and muting and unmuting them, HDX endpoints encounter flickering video.	V7.0	
144	VNGR-16877	*Interoperability*	Avaya 1XC Softphone endpoints connected to conference on RMX do not receive content, while HDX endpoints do.	V7.0	
145	VNGR-16867	*RMX 1500 Video*	On RMX 1500 with MPMx, when the endpoint displayed in the large video window in 2+8 layout disconnects, the large video window is not re-allocated to another endpoint.	V7.0	
146	VNGR-16861	*General*	On an RMX 2000 with 2 MPM+80 and 2 RTM ISDN Cards (5 T1/PRI connecting to each RTM ISDN card), only 70 CIF dial-out endpoints can connect to the 128 Kbps conference.	V7.0	
147	VNGR-16857	*RMX 1500 Audio*	On RMX 1500 metallic audio is heard periodically on PVX endpoint.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
148	VNGR-16856	*Interoperability*	Artifacts displayed on ISDN endpoints connected to RMX 1500 when content is started or stopped.	V7.0	
149	VNGR-16841	*Interoperability*	Connect to the network using VPN and then start a conference with LPR enabled, connect endpoints using CMAD, the video of the endpoints was very fragmented.	V7.0	
150	VNGR-16839	*SIP*	On RMX with MPMx in High-Profile Motion conference at 512kbps, HDX endpoints connected via SIP only transmit H.264 HP / 4SIF at 15 frames per second.	V7.0	
151	VNGR-16825	*Interoperability*	Using RMX 2000 with MPMx, H.320 call to VSX8000 endpoint fails with Call Disconnection Cause listed as "No net connection - 0 ".	V7.0	
152	VNGR-16817	*Upgrade Process*	After upgrading to version 7.0.0.135 the RMX Web Client shows that RMX is no longer in the "Startup" phase even though Faults list states: "Configuring".	V7.0	
153	VNGR-16807	*Content*	Bad audio quality experienced on PVX endpoint while it sends content when connected to RMX 1500.	V7.0	
154	VNGR-16806	*Interoperability*	On RMX 1500, a macro block is displayed in the large video window of the video layout when PVX endpoint is the speaker.	V7.0	
155	VNGR-16798	*Audio*	Medium volume horn-like sound heard for several minutes on HDX4000 endpoint connected to RMX 4000 with MPM+ via DMA Meeting Room.	V7.0	
156	VNGR-16794	*Audio*	On RMX 4000 with MPM+, G.728 endpoint isn't declared 1st endpoint in conference at 96kbps.	V7.0	
157	VNGR-16793	*General*	On an RMX 2000 with MPM+, start an 4096Kbps 1x1 Layout conference from a template with Encryption, LPR, Auto Termination, Sharpness, Same Layout, Audio Clarity enabled, an "mcu internal problem: 32212" message appears in conference properties - connection status tab.	V7.0	
158	VNGR-16791	*Interoperability*	In a 1024Kbps conference with Auto layout, Sharpness, AES, H.239 Content to Legacy Endpoints and LPR enabled, Lifesize endpoints encounter poor video.	V7.0	
159	VNGR-16776	*Interoperability*	Undefined HDX endpoint cannot be added to the Address Book on RMX with Avaya Call Manager. Second attempt yields message that participant name already exists in Address Book.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
160	VNGR-16751	*General*	When creating a second conference with a display name that is already used by another conferencing entity, the conference properties dialog box re-opens with a redundant check box next to the routing name field.	V7.0	
161	VNGR-16745	*General*	In the RMX manager 7.0, the "new conference" icon suddenly appears in the conferences properties window.	V7.0	
162	VNGR-16742	*Diagnostics*	On an RMX2000 with MPMx_D cards when performing an Power ON Self Test (POST), the MPMx card runs the card monitoring test in an endless loop.	V7.0	
163	VNGR-16724	*Video*	On RMX 1500, video display freezes momentarily during Video Layout changes before the new Video Layout is displayed.	V7.0	
164	VNGR-16722	*Video*	On RMX 2000 with one MPM-H, small artifacts are displayed in the Gathering Slide when the configuration is changed to Presentation Mode during the Gathering Phase.	V7.0	
165	VNGR-16708	*Video*	The displayed resolution of the gathering slide differs between H.323 participant (432x240) and H.320 participant (480x352) when both endpoints are connected to a CP conference running at a line rate of 384Kbps with video quality set to Motion and LPR is enabled. Once the Gathering phase ends, all participants connect with 2SIF resolution.	V7.0	
166	VNGR-16695	*Video*	Using MPMx, frame rate in motion conference is less than 60fps on HDX endpoints that connect at HD resolution at 1920kbps and are not allocated on the Turbo DSP.	V7.0	
167	VNGR-16677	*RMX Manager*	Progress bar missing in RMX manager during upgrade.	V7.0	
168	VNGR-16674	*SIP*	In ICE environment, when connecting endpoints from all NAT environments (corporate/branch/federated) to an encrypted CP conference running at a line rate of 2Mbps, video quality set to sharpness, and video clarity and auto layout are enabled, some of the endpoints fail to connect due to TB_MSG_OPEN_PORT MCU internal problem or SIP HW MCU internal problem.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
169	VNGR-16663	*SIP*	In ICE environment, when connecting endpoints from all NAT environments (corporate/branch / enterprise) to an encrypted, 720p VSW conference, running at a line rate of 2M bps with video quality set to sharpness and video clarity and auto layout enabled, endpoints fail to connect to the conference with a disconnection cause "SIP request timed out".	V7.0	To overcome the problem do one of the following: * Connect the endpoints one by one. * Run a non encrypted 2M VSW conference * Run the conference at a lower line rate (768Kbps)
170	VNGR-16657	*Video*	In a 4MB HD1080p conference with Content, Video Clarity, Auto Termination, Encryption, LPR, Echo Suppression and Auto Layout enabled, when dialing out to six HDX8006 endpoints and changing the speaker, all endpoints had bad video.	V7.0	
171	VNGR-16646	*Interoperability*	In a conference started from the default Profile, when the RMX dials-out to an H.320 iPower 9000 endpoint, the endpoint's video layout is shifted to the bottom right of the monitor with black borders on the left and top of the screen.	V7.0	
172	VNGR-16643	*Interoperability*	A conference started from the default video conference, an H.320 Sony PCS-G50 endpoint transits the Entry Queue and when accessing the conference it connects with no video.	V7.0	
173	VNGR-16625	*General*	Sometimes when upgrading to version 7.0 and resetting the RMX 2000, an active alarm "CPU slot ID not identified - McuMngrCPU board id was not received from ShelfManager" is displayed.	V7.0	
174	VNGR-16621	*General*	Run two conferences that support Content for Legacy Endpoints, connect all types of endpoints to each conference and then send content from a non Legacy endpoint to each conference. The conference layout on the Legacy endpoint is changed to the flag's CP_LAYOUT_1P4VER configuration, the default layout. Move one legacy EP to the second conference - the layout of it changes to conference layout	V7.0	
175	VNGR-16618	*Video*	On an RMX with MPM+ cards, when configuring the resolution of Configuration Slider to HD 1080p60/ HD 720p60 - in the participant properties you should not be able to select HD1080/HD 720p as the Maximum Resolution (People Video Definition).	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
176	VNGR-16610	*General*	The Column width displayed in Web Client and in the RMX Manager UI need to be made broader.	V5.0.1, V5.0.0, V4.6.1, V6.0, V7.0	
177	VNGR-16607	*Gateway* FIX VERIFIED	When a Gateway call is started from a video endpoint (CMAD or HDX) and endpoints connect to the conference, SIP endpoints view a blurry gathering slide with artifacts.	V7.0	
178	VNGR-16604	*Gateway* FIX VERIFIED	In a Gateway call started from a video endpoint (CMAD or HDX) when other endpoints connect, the endpoint that initiates the call initially views the Gathering slide but then it disappears.	V7.0	
179	VNGR-16600	*General*	On an RMX2000 & MPMx card running a mixed H.323 & SIP 1920Kbps conference with AES, Sharpness and Gathering enabled, when the RMX dials-out to 10 endpoints, the border layouts are "speckled" and miss their edges.	V7.0	
180	VNGR-16599	*Interoperability*	On an RMX 2000 in a H.261 video conference, when a Tandberg MXP6000 connects using H.261 there is no video.	V7.0	
181	VNGR-16595	*Interoperability*	On an RMX 4000 & MPM+ cards, running an 1920Kbps conference with Video Clarity, Auto Terminate, Video Quality, Sharpness, Encryption, LPR, Echo Suppression, Auto Layout, Gathering and Content for Legacy Endpoints enabled, when connecting 20 HDX, Tandberg 17000 and edge95 MXP & 3 Tandberg C series endpoints the MFA card error occurs.	V7.0	
182	VNGR-16582	*General*	On an RMX 2000 & MPM+ cards, running an 384Kbps CIF conference, with Auto Terminate, Encryption, LPR, Echo Suppression, Sharpness and Same Layout enabled, when sending content from an HDX to 160 other endpoints, an "Software assert failure" appeared.	V7.0	
183	VNGR-16581	*General*	On an RMX 2000 & MPM+ cards, running an 384Kbps CIF conference, with Auto Terminate, Encryption, LPR, Echo Suppression, Sharpness and Same Layout enabled, when sending content from an HDX to 160 other endpoints, an "Software assert failure" appeared.	V7.0	
184	VNGR-16560	*General*	After log-in to the RMX 1500 Web Client, a Microsoft .NET Framework error message appears.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
185	VNGR-16556	*IVR*	In a mixed H.323 & SIP 128Kbps conference with Gathering, Sharpness and the Welcome Slide defined as "High Profile optimized", when connecting HDX8000 endpoints, the H.323 HDX video has artifacts on the Gathering slide.	V7.0	
186	VNGR-16523	*FECC*	On the RMX 1500 running a mixed H.323 & SIP 384Kbps conference, when connecting an Tandberg SIP endpoint, FECC does not work.	V7.0	
187	VNGR-16506	*Interoperability*	Lip sync is noticeable on HDX 7000 rev. B that dials into a conference running at a line rate of 1Mbps.	V7.0	
188	VNGR-16471	*General*	Extraneous MCMS version number is displayed in the detailed faults list.	V7.0	
189	VNGR-16466	*General*	On RMX 2000 with MPM, "MCU Internal Problem - 32112" occurs during mini-load smoke on MPM when 20 video participants are connected at 384kbps.	V7.0	
190	VNGR-16460	*IVR*	On RMX 2000 with MPMx, H.261 endpoint that displays the default slide does not access nor displays a new slide that is added to the IVR Service.	V7.0	
191	VNGR-16429	*Multilingual*	On RMX with Operator Conference selected in profile, when trying to delete a running conference, the popup message is displayed in mixed English and Japanese.	V7.0	
192	VNGR-16427	*General*	On RMX 1500 with two conferences running and Legacy Content enabled, line artifacts are displayed in the middle of the CMAD screen after it is disconnected from the first and reconnected to the second conference.	V7.0	
193	VNGR-16387	*Interoperability*	On an RMX2000 with the MPM+ card, when connecting with an HDX9000 endpoint to the Entry Queue using a line rate of 384Kbps, the IVR slide blinks.	V7.0	
194	VNGR-16383	*Interoperability*	On the RMX2000 with an MPMx card in a 512Kbps conference with High Profile, Gathering, IVR, Echo Suppression enabled and resources set to a Flexible Mode, when dialing-out using H.261, connection problems are encountered in VSX endpoints after about 10 seconds.	V7.0	
195	VNGR-16378	*Interoperability*	In a SD conference (1024 resolution) with motion, auto layout enabled, when connecting HDX and dial in from Life Size endpoint, the endpoints do not connect in SD with 60 FPS as required.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
196	VNGR-16363	*Interoperability*	On the RMX2000 with an MPMx card, when starting a new a 2MB conference, Ipower endpoints take a long time to connect.	V7.0	
197	VNGR-16313	*IVR*	On an RMX2000 with an MPMx card running a 512Kbps conference with Gathering, IVR, Echo Suppression enabled and resources set to a Flexible Mode, when dialing out using H.261 the IVR slide flashes.	V7.0	
198	VNGR-16296	*General*	The Host name is not defined in the Fast Configuration Wizard during the initial system configuration. Therefore when trying to configure either the "Control" or the "Shelf" IP address (or both), the error message "Invalid Host Name" is displayed when clicking OK.	V7.0	
199	VNGR-16283	*General*	In a conference with a few participants, when opening the video preview pane and previewing the next participant without closing the pane, the pane becomes minimized, and does not show video of the next participant.	V7.0	
200	VNGR-16272	*Audio*	RMX 4000 using HDX endpoints in 2048Kpbs HD Video Switching conference using Siren22Stereo exceeds conference bit rate by sending data to endpoints at 2112kpbs.	V7.0	
201	VNGR-16237	*General*	Connect to an RMX as Operator using the RMX Manager. Then connect an Administrator to same RMX the following message appears: "cannot login to MCU x.x.x.x with the user name and password entered”.	V7.0	
202	VNGR-16215	*Upgrade Process, Video*	Create conference set to High Profile and connect Durango endpoints, the Durango and HDX8000 Video preview is in a green color.	V7.0	
203	VNGR-16210	*RMX Web Client*	On an RMX 1500 with a conference and connected participants, when multiple web clients are opened on different PC's and Video Preview is activated, when opening another browsing session and viewing Video Preview, all the browsers close though some view a "failure status" message.	V7.0	
204	VNGR-16120	*General*	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	
205	VNGR-16050	*Video*	When using the MPMx card to run a conference with Auto Brightness enabled, no difference can be seen in the video between a light and darkened room.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
206	VNGR-15953	*General*	When copying and pasting conferences based on a Profile, the pasted conference is added to conference templates.	V7.0	
207	VNGR-15938	*Audio*	RMX 4000 using HDX endpoints in 2048Kpbs HD Video Switching conference using Siren22Stereo exceeds conference bit rate by sending data to endpoints at 2112kpbs.	V7.0	
208	VNGR-15937	*Interoperability*	In a conference with HDX8006A, HDX8006B, HDX9000, VSX7000 and ViewStation512 endpoints, the site names of the ViewStation endpoints are switched.	V7.0	
209	VNGR-15935	*Gateway*	In the RMX Web Client, when creating a new gateway profile and setting the Gateway ID to "#1234" then click OK, no confirmation message appears.	V7.0	
210	VNGR-15907	*Upgrade Process*	When upgrading RMX4000 MPM+ from version 6.0.0.105 to version 7.0.0.91, the Fabric Switch name is missing from the Hardware Monitor.	V7.0	
211	VNGR-15906	*Interoperability*	In a 384Kbps conference with no IVR and resources set to a Fixed Mode when connecting SIP/H.323 HDX & PV dial-in and dial-out endpoints, the SIP receives bad video.	V7.0	
212	VNGR-15837	*General*	In 768Kbps conference set to AES, CP, Full Layout and two HDXs Chairperson, when the SIP HDX invokes PCM Camera Control only segmented video can be seen.	V7.0	
213	VNGR-15822	*PCM*	When PCM is activated in a Gathering-enabled conference, the PCM menu is displayed on top of the gathering slide instead of the display of the Gathering Slide being terminated before the PCM menu is displayed.	V7.0	
214	VNGR-15798	*Partners - Microsoft*	In ICE environment, a green overlay is displayed on top of one of the video layout in the Gathering slide when a dial out MOC or HDX endpoint connect to the conference.	V7.0	
215	VNGR-15755	*General*	During an active Telepresence conference, click the Video Settings tab, the "Telepresence Mode enabled" check box appears when it should not.	V7.0	
216	VNGR-15750	*General*	In a conference set to 512kbps with Auto Layout enabled, when starting PCM from several endpoints, - you will receive an Message Overlay: "no available PCM resources". The message overlay cannot be closed.	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
217	VNGR-15746	*General*	When downloading and installing version 7.0, the Download window lists version 6.0.	V7.0	
218	VNGR-15738	*Video*	When monitoring a conference and right-clicking a participant, the participant's video and audio freezes.	V7.0	
219	VNGR-15718	*General*	Incorrect disconnection cause after pulling LAN cable from RMX. The endpoints reports that the "call close normal".	V7.0	
220	VNGR-15709	*Video*	In a 2MB CP conference with LPR, Gathering, Sharpness, Video Clarity and Auto Brightness enabled, when connecting SIP & H.323 PVX/HDX endpoints, when starting PCM and selecting 1*1 Layout, the conference video has video artifacts.	V7.0	
221	VNGR-15707	*ISDN*	An RMX 4000 with a 384K H.320 conference with Motion and AES enabled, when a Tandberg 6000 MXP connects, the endpoint encounters video freezes.	V7.0	
222	VNGR-15649	*Interoperability*	In a continuously running conference, after disconnected two HDX7000 and VSX7000 endpoints, the HDX4000 endpoint's video freezes.	V7.0	
223	VNGR-15554	*General*	Numerous missing Japanese translations in the RMX Web Client.	V7.0	
224	VNGR-15386	*Video*	Artifacts present in the Gathering Slide in 2560kbps, CP conference with Motion selected.	V7.0	
225	VNGR-15366	*General*	Sometimes when Restore Factory Defaults is performed, the active alarm "CPU slot ID not identified- McuMngrCPU board id was not received from ShelfManager" is displayed.	V7.0	
226	VNGR-15324	*General*	o When monitoring a CP conference with 5 or more endpoints from 5 Web Client sessions on separate workstations, Video Previews can be opened from 4 workstations. Attempting to open a fifth Video Preview causes an error "Failed to Preview Video: Failure Status" instead of "The Preview cannot be displayed. The maximum number of previews per MCU has been reached."	V7.0	
227	VNGR-15320	*General*	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	
228	VNGR-15281	*Interoperability*	Aethra VegaStar Gold endpoint, when connecting via ISDN to 384kbps conference creates CDR Event - Participant status "Connected with problem".	V7.0	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
229	VNGR-15256	*Encryption*	In a conference with an IVR Service with endpoints, when using DTMF (*71/#71/*88) codes to secure/ unsecure the conference there is no text/icon indication.	V7.0	
230	VNGR-15155	*Video*	In a conference with a line rate of 4096kbps, set to Sharpness, 1+5 layout, after connecting a few endpoints, when an endpoint dials out, video In & Out freeze.	V7.0	
231	VNGR-15131	*IVR*	In a conference started from a Profile, when an ISDN call is forced to Audio algorithm G722_1_C_24k a buzzing noise can be heard before the IVR starts.	V7.0	
232	VNGR-15129	*Interoperability*	In a conference set to a line rate of 4096kbps with Sharpness, 1+5 layout, with a number of endpoints present, when a H.323 HD720p30 Tandberg 1700MXP endpoint dial-outs, Video In & Out freeze.	V7.0	
233	VNGR-15101	*IVR*	In a Video Switched 4Mbps conference, only the last part of DTMFs *6 (mute) and #6 (unmute) messages are heard.	V7.0	
234	VNGR-14778	*RMX Web Client*	ISDN/PSTN fields are disabled (grayed out) although Enable ISDN/PSTN Dial-in check box is selected in RMX Management > Entry Queues > Default EQ.	V6.0	
235	VNGR-14720	*Upgrade Process*	After software Upgrade is completed, an Active Alarm "Connection to Exchange Server failed" appears in the Alarms List on the RMX4000.	V6.0	
236	VNGR-14386	*RMX 4000*	Display information for Slot 5, FSM (Fabric Switch Module), in the RMX 4000 Hardware Monitor is incomplete.	V5.1	
237	VNGR-12257	*RMX Web Client*	When upgrading the RMX Web Client with software changes, Internet Explorer needs to be closed and opened before the upgrade can take place.	V5.0.0	
238	VNGR-11701	*General*	Sometimes a system error "SOFTWARE_ASSERT_FAILURE" appears when the RMX is running under load (repetitive connecting and disconnecting participants).	V4.5	
239	VNGR-11543	*CMA*	When creating a conference using the CMA, the Conference Management UI displays the participants as disconnected, even though they are connected.	V4.1	
240	VNGR-10989	*Interoperability*	In a ISDN dial-in conference with a line rate of 384 Kbps, Tandberg MXP ISDN endpoints cannot view content.	V4.1	

Table 6 *Corrections Between Version 7.5.2.J and Version 8.1.4.J (Continued)*

#	Key	Category	Description	Detected in Version	Workaround
241	VNGR-17743	*Partners - Microsoft*	In an environment that includes the Microsoft Lync server and RMX 4000 MPM+80 with ICE enabled, when the RMX dials out to two Lync clients with HDX connected, the second Lync client is disconnected from the conference that is running at 384kbps, with Encryption and LPR enabled due to a SIP HW internal MCU problem.	V7.0.2	
242	VNGFE-3246	*Partners - Microsoft*	RMX disconnects MOC ICE Call between federated sites when RMX is not installed in the same site as the OCS Pool.	V7.0	Install the RMX on a main domain or federate the sub domain.
243	BRIDGE-3080	*Software Defect*	In a conference set to Encrypt When Possible, Send Content to Legacy Endpoints enabled, and the FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE flag set to NO, an HDX will sometimes display black instead of Content, and a CSS plug-in will sometimes display blue instead of Content.	V8.1.1	

Version 8.1.4.J - System Limitations

Table 2-1 *Version 8.1.4.J - System Limitations*

NO	Key	Category	Description	Detected in Version	Workaround
1	BRIDGE-322	*RMX Manager*	Active Directory user cannot open the Hardware Monitor section in the RMX Manager.	V7.5	
2	BRIDGE-400	Security	In Multiple Networks Configuration, Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default network Service to enable the recording.	7.8.0	
3	BRIDGE-500	*Video*	The video display is “jumpy” when endpoints connect to a conference running on RMX with MPMx at a line rate of 512Kbps and SD resolution.	V7.0.2	
4	BRIDGE-645	*General*	RMX 4000 prompts for an extra reset during “Restore Factory Defaults” procedure (after insertion of the Activation Key). Reset should only be performed after the Fast Configuration Wizard has completed.	V6.0	
5	BRIDGE-706	*General*	An unclear message “No utilizable unit for audio controller” is displayed when removing all Media cards from the RMX.	V7.1	
6	BRIDGE-711	*Upgrade Process*	On the RMX 2000/4000 with an ISDN card installed, after configuring the IP Fast Configuration Wizard, the system requests a reset and not to configure the ISDN Service.	V7.0	
7	BRIDGE-976	*IVR*	When two Avaya 1XC Softphone endpoints join a conference, the IVR Service “first to join conference” music continues to play as if there is just one person in the conference.	V7.0	
8	BRIDGE-978	*Interoperability*	In 768Kbps conference with RMX H.264 HighProfile resolution settings, the H.320 HDX endpoint views fragmented video as it cannot support HighProfile resolutions at 520 Kbps and above.	V7.0	
9	BRIDGE-1813	*Software Defect*	When the CAC_ENABLE flag is set to "YES", only 13 endpoints can connect to the conference.	V7.7	
10	BRIDGE-1977	*Interoperability*	When an RMX dials out to an Aethra X7 endpoint, the Aethra requires 20 seconds to receive audio and video..	V7.8	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
11	BRIDGE-3301	Security	Default protocol version for SNMP Agent and Traps is Version1instead of Version 3 on RMX with Ultra Secure Mode enabled.	8.1.1	
12	BRIDGE-3381	Security	IPv6 address remains active and user can log in to RMX using IPv6 address after addressing mode is changed from IPv6 only to IPv4&IPv6. Reset from Hardware Monitor using IPv4 address fails after RMX IP addressing mode is changed to IPv4 only.	8.1.1	
13	BRIDGE-3636	Security	Dial out SIP call to group series EP may not connect because of incorrect handling of Glare condition in RMX. Setup: RMX configured in dual addressing mode (IPv4&IPv6), registered with TLS on IPv4.	8.1.1	
14	BRIDGE-3680	*General*	A core dump was produced.	V8.1	
15	BRIDGE-3684	Software Defect	When the Encryption mode is "encryption when possible" is enabled in the RMX Collaboration Client, the HDX fails to share content and sometimes other endpoints view a blue screen instead of content.	V8.1.5	
16	BRIDGE-3699	*Interoperability*	A CTS could not be put on hold and resume when music from the CUCM was on hold.	V8.1	
17	BRIDGE-3865	Security	MLD is not supported by RMX configured for IPv6.	8.1.2	
18	BRIDGE-3866	Security	PRACK request is not supported by RMX configured for AS-SIP.	8.1.2	
19	BRIDGE-3868	Security	Early media is not supported by RMX configured for AS-SIP.	8.1.2	
20	BRIDGE-3872	Security	SUBSCRIBE and NOTIFY requests are not supported by RMX configured for AS-SIP.	8.1.2	
21	BRIDGE-3873	Security	H.263-2000 video coding is not supported by RMX configured for AS-SIP.	8.1.2	
22	BRIDGE-3875	Security	SDP H.264 optional parameters are not supported by RMX configured for AS-SIP: sprop-parameter-sets / parameter-add / sprop-interleaving-depth / sprop-deint-buf-req / deint-buf-cap / sprop-init-buf-time / sprop-max-don-diff / max-rcmd-nalu-size	8.1.2	
23	BRIDGE-4090	Security	SNMP Traps Security Levels are not within acceptable range on RMX with Ultra Secure Mode enabled.	8.1.2	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
24	BRIDGE-4101	*Interoperability*	A TIP endpoint which was the first participant heard the standard, “You are the first participant to join the conference.” message, but did hear the waiting music.	V8.1	
25	BRIDGE-4105	Security	MLPP: With "Use Precedence" selected, participant’s Precedence Level is not recorded in CDR.	8.1.2	
26	BRIDGE-4113	*Interoperability*	In a conference with 2 CTSs with music provided by CUCM, when one of the CTSs was put on hold and then resumed, it was disconnected from the conference.	V8.1	
27	BRIDGE-4141	*Interoperability*	In a 4 mbps conference with “Prefer TIP” enabled that uses an external IVR service, the IVR message is heard on an OTX before the slide is shown. Music is heard 3-5 seconds before the slide is shown.	V8.1	
28	BRIDGE-4212	*Interoperability*	When the SIP_ENCRYPTION_KEY_EXCHANGE_MODE flag is set to SDES, endpoints that attempt to hold and then resume are disconnected.	V8.1	
29	BRIDGE-4275	*Interoperability*	Video quality degrades after an hour in a conference with a TX9000.	V8.1	Do not use content at a rate of 30fps.
30	BRIDGE-4296	*Interoperability*	In a conference with 1 HDX connecting using SIP and 1 CTS using TIP, when the HDX was the chairperson the *5 DTMF code (mute all except me) did not mute the CTS.	V8.1	Manually mute other endpoints.
31	BRIDGE-4320	*Interoperability*	When the Video Quality setting of a conference is motion, the connection status of endpoints using TIP is, “Connected With Problem.”	V8.1	
32	BRIDGE-4386	Security	SNMP Authentication and Privacy passwords are not encrypted.	8.1.2	
33	BRIDGE-4402	*DTLS*	When the SIP_ENCRYPTION_KEY_EXCHANGE_MODE flag was set to SDES, when a CTS3010 was put on hold and then resumed, a core dump was produced.	V8.1	
34	BRIDGE-4407	*IVR*	When a user attempted to enter a PIN for the 4th time after entering it wrong 3 times, the call failed to transfer to the help desk. The user hung up after 30 seconds.	V8.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
35	BRIDGE-4474	Security	Line rate set to 4096 Kbps in New Profile - General tab reverts to default 384 Kbps in New Profile - Video Settings tab.	8.1.2	
36	BRIDGE-4508	*Interoperability*	CTS3010 fails to negotiate TIP when dialing into an encrypted conference.	V8.1	
37	BRIDGE-4587	Security	Active Alarm to delete or rename the POLYCOM default user is not cleared when the POLYCOM default user is deleted or renamed.	8.1.2	
38	BRIDGE-4589	Security	Install of CRL file (generated with Personal Certificate) fails after MCU reset.	8.1.2	
39	BRIDGE-4590	Security	System Reset prompt acknowledgement is not actioned (system does not reset) after PKI change of Certification Revocation Method from None to OCSP.	8.1.2	
40	BRIDGE-4651	*Network*	After a call started, network traffic meant for the MPMx card is sent to all network ports on the subnet.	V8.1	
41	BRIDGE-4674	*General*	When two participants simultaneously attempt to enter an Entry Queue with the same PIN are rejected.	V8.1	
42	BRIDGE-4687	Security	Wrong number (N-2 instead of N-1) of participants displayed in layout of DMA Virtual Meeting Room on all endpoints after one of the endpoint's video is suspended.	8.1.2	
43	BRIDGE-4696	*Interoperability*	In a conference with 2 CTS1300's and 1 CTS500, if 1 CTS places a call on hold and then resumes it, then tries to send content, and then another CTS tries to send content, content is seen locally only.	V8.1	
44	BRIDGE-4754	*Interoperability*	An HDX connecting using TIP to a DMA was disconnected when moving from a VEQ to a VMR.	V8.1	
45	BRIDGE-4756	*Interoperability*	An HDX connecting using TIP to a DMA was unable to move from a *Entry Queue* to a *Meeting Room*.	V8.1	
46	BRIDGE-4783	*Interoperability*	An HDX connected for 3 to 4 minutes to a TIP call crashed.	V8.1	
47	BRIDGE-4835	*Interoperability*	The center screen of a TX9000 displayed distorted video when the participant moved.	V8.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
48	BRIDGE-4845	Software Defect	A GS300 endpoint view pixelated video and encounters audio loss on a WAN network with considerable packet loss.	V.8.0	
49	BRIDGE-4890	Security	Management Network Service name populated into Common Name (DNS) field of Create Certificate Request dialog box for IP Network Service.	8.1.4	
50	BRIDGE-4977	Security	False alarms: 'Secured SIP communication failed', 'Failed to connect to SIP Registrar' displayed when RMX conference fails to reach LSC-registered Meeting Room because of wrong account information in conference configuration. Setup: RMX (SIP-registered) in Ultra Secure Mode with Secure Communication enabled.	8.1.4	Deleting one of the registered meeting rooms removes the alarms.
51	BRIDGE-5252	Software Defect	During a mixed mode (AVC&SVC) conference when an endpoint switches from audio to video and then back again, additional ART resources are used, but later when reverting to audio these video resources remain occupied.	V8.1.4	
52	BRIDGE-5311	Security	With RMX and XMA working in MSM, incorrect Audio Status of dial out Group Series, AS-SIP participant endpoint is shown in Participants pane of MSM. The audio status icon is always green whether the participant is muted or unmuted from the endpoint side.	8.1.4	
53	BRIDGE-5526	*Software Defect*	In an AVC SIP 1920 kbps conference set to Encrypt When Possible, a Cisco SX20 and EX90 connecting as encrypted received bad video, no FECC, and Content appeared was displayed for only 1 second.	V8.1.4	• Do not use SIP. • Do not use encryption.
54	BRIDGE-5709	*Software Defect*	An incorrect major Active Alarm “Bios version unsuitable for JITC.” is displayed on Collaboration Servers 2000 and 4000.	8.1.4	None needed. The BIOS is suitable for Ultra Secure Environments.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
55	BRIDGE-5744	Security	Meeting Room status remains as 'Registered' in SIP Registration field of RMX UI after SIP Server is set to 'Off'. Meeting Room previously registered to LSC with LSC info and OCSP specified. Setup: RMX: IPv6 mode; Ultra Secure Mode; Secure Communication enabled; Certificates loaded.	8.1.4	
56	BRIDGE-6038	Security	When configuring Radvision Serial Gateway on RMX, and changing IP Network Services to IPv4&IPv6: IPV6 not configured on the Gateway Service and a fault is displayed: “Could not complete MPM Card startup procedure. Card ID:4, Card Type:mpm, Description: MPM startup incomplete: Media IP Configuration confirmation was not received.”	8.1.4	
57	BRIDGE-6040	*Software Defect*	In an AVC conference with 56 HDX 8000 participants running at 4096 kbps using 1080 resolution, after 10 minutes, 11 participants disconnected.	V8.1.6	
58	BRIDGE-6199	*Software Defect*	In a 1920 kpbs AVC conference with a LifeSize Team 200 endpoint, a Group Series G500 endpoint, and an HDX 9006 endpoint, only the LIfeSize endpoint displayed Content.	V8.1.6	
59	BRIDGE-6307	*Interoperability*	When an HDX 8000 SIP client registered to an Avaya Session Manager SIP server dials into an RMX meeting room with a 6 digit password, the RMX interrupts the entry of the password with an announcement saying to please wait for the operator.		
60	BRIDGE-6345	*Software Defect*	AVC participant Content audio is also muted by microphone mute setting when dialing into SVC/AVC Mixed mode conference.	V8.1	Un-mute microphone and reduce volume on content sharing endpoint.
61	BRIDGE-6393	Software Defect	During a 2MB conference launched from the DMA, after a blast dial-out of many endpoints, some DSPs on the MPMx card crash.	V8.1.7	
62	*BRIDGE-6442*	Software Defect	A VVX 1500 endpoint registered with the DMA does not see video after the RMX dials out to the endpoint.	V7.7	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
63	BRIDGE-6448	Software Defect	When the VMR profile is set to prefer TIP and LPR enabled, after connecting to the conference, a SIP RPX has video problems.	V8.1.1	
64	BRIDGE-6450	*Software Defect*	Cisco endpoint are not able to join Virtual Meeting Room after terminating conference. Frequency: Rare.	V8.1.1	Do not terminate conference from RMX. Call after 5 minutes.
65	BRIDGE-6490	Software Defect	Create an ISDN/PSTN Entry Queue enabled conference in the conference properties, after conference start ISDN/PSTN is not enabled	V8.1.6	
66	BRIDGE-6492	Software Defect	When the RMX is used as ISDN-Gateway (H.320) with OpenScapeVoice (Siemens SoftMCU), after connecting Tandberg MXP6000 & Tandberg Edge95 ISDN endpoints, Sip endpoints hear only audio and cannot view the Welcome screen.	V7.8	
67	BRIDGE-6518	Software Defect	A CSS client cannot share and receive content while LPR is enabled in the conference running on an RMX.	V8.1.7	
68	BRIDGE-6519	Software Defect	On a conference set to LPR and content, the CSS clients sends content to the RPD endpoint at 380Kbps, however the RPD negotiated content line rate settings should be set to 192 Kbps.	V8.1.7	
69	BRIDGE-6540	Software Defect	On an RMX with many types of conferences, when an RPD endpoint connects to an AVC only conference, in the 2x2 layout, 2 video layouts show video and the other 2 cells appear blue.	V8.1.7	
70	BRIDGE-6560	*Software Defect*	ITP endpoint's Slave endpoints do not connect in RMX dial out call.	V7.8.0	Dial in again.
71	BRIDGE-6579	Software Defect	When an RPD is sharing content and applications, VVX endpoints failed to receive content.	V8.1.7	
72	BRIDGE-6582	Software Defect	Up to 10 participants out of 25, including RP Desktop, RP Mobile, HDX Lync client are disconnected from a call of 30 minutes duration. Occurs after hang up/re-join call operations from endpoints.	V8.1.7	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
73	BRIDGE-6650	*Software Defect*	Call from Cisco CTS3010 to RMX Virtual Meeting Room Call disconnects at beginning. Frequency: Rare.	V8.1.7	Re-connect.
74	BRIDGE-6686	*Software Defect*	Ongoing conference cannot be deleted or users cannot be removed from the conference. Frequency: Rare.	V7.6.1	Reboot is required.
75	BRIDGE-6814	*Security*	When using HDX as ISDN endpoint, PSTN to ISDN Gateway Call via IVR on RMX, in Ultra Secure Mode with Secure Communication enabled, does not connect.	8.1.4	
76	BRIDGE-8180	*Security*	Automatically generated Engine ID for SNMPv3 trap is not displayed in the UI.	8.1.4	Using the UI, manually set the Engine ID to a known and unique value.
77	BRIDGE-8182	*Security*	RMX crashes when changing Video Quality parameters in the Factory Gateway Profile.	8.1.4	
78	BRIDGE-8308	*Security*	One way audio followed by conference drop after Hold/Resume from Nortel 1140 IP Phone. Setup: RMX1500 / RMX4000; Active Directory enabled; AS-SIP; ANAT Off; Encryption SHA1_32; SIP_BFC_DIAL_OUT_MODE=UDP; Registered to Redcom SLICE 2100.	8.1.4	
79	BRIDGE-11350	*Security*	A major Active Alarm "'0' isn't a valid value for the flag: MAX_CONF_PASSWORD _REPEATED_DIGITS" is displayed after setting the ULTRA_SECURE_MODE System Flag to =YES requiring, the user to manually modify the MAX_CONF _PASSWORD_REPEATED_DIGITS System Flag's value.	8.1.4	Manually modify the System Flag's value.
80	VNGR-10104	*LPR*	When an H.323 HDX endpoint sends Content, the endpoint disables the LPR.	V4.0.1	
81	VNGR-10162	*Interoperability*	An HDX 2.5.0.2-3395 endpoint cannot control a Sony XG80 endpoint using FECC.	V7.2	
82	VNGR-10239	*Video*	In a 4Mb conference set to Sharpness and the IVR Welcome Message enable video appears in a 4x3 format. Disable IVR Welcome message and the video appears in 6x9 format.	V4.0.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
83	VNGR-10922	*General*	Dial out to participants assigned to a Meeting Room will only start when the dial-in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.	V4.1	
84	VNGR-11324	*General*	When moving many participants simultaneously from one conference to the other (both with a line rate of 1920 Kbps), a number of HDX8000 endpoints connect secondary. When trying to disconnect and reconnect the participants connected as Secondary, an MCU Internal error 32122 is displayed.	V4.1	
85	VNGR-11341	*Interoperability*	During H.320 calls, Lip Sync issues occur when content is being sent.	V4.1	
86	VNGR-11351	*Video*	When the video from an endpoint is blocked, inconsistent video resolution settings are implemented.	V4.1	
87	VNGR-11382	*Video*	Legacy endpoints receive Content in 1+7 layout with black stripes on the sides (for aspect ratio fitting), selecting a different layout using Click&View (**) causes the black stripes to disappear.	V4.1	
88	VNGR-11383	*General*	When updating the Profile assigned to a Conference Template, changes are not applied when the conference becomes ongoing.	V4.1	
89	VNGR-11401	*Encryption*	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	V4.1	
90	VNGR-11417	*Interoperability*	On an RMX 2000 running a 1472 kbps conference with Auto Layout, Sharpness and Graphics enabled, the Tandberg 6000 MXP endpoint does not negotiate using 720p HD with the RMX.	V7.1	
91	VNGR-11425	*Interoperability*	When Tandberg MXP sends Content using H.323, ISDN endpoints cannot view Content.	V7.1	
92	VNGR-11463	*Interoperability*	In a conference running at a line rate of 128 Kbps that includes Content sent by H.323 endpoint, Lifesize ISDN endpoints cannot view the Content.	V7.7	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
93	VNGR-11489	*Interoperability*	In a conference running at a line rate of 384 kbps, when HDX 8006 endpoint that sends Content is moved to another conference, Content is still viewed for a number of seconds on the HDX.	V4.1	
94	VNGR-11523	*Interoperability*	In a conference started using the default factory profile, when connecting to the conference with a MOC Client or HDX SIP endpoint, there is no indication on the RMX if audio is muted or unmuted.	V4.1	
95	VNGR-11531	*IVR*	After upgrading the RMX to a software version that includes the gateway and the maximum number of IVR services reached 40 in RMX 2000 and 80 in RMX 4000, the default Gateway IVR Service is not created.	V4.1	
96	VNGR-11563	*Interoperability*	Legacy endpoints occasionally cannot switch to Content when Content switched from H.264 to H.263.	V4.1	
97	VNGR-11746	*CDR*	GMT Time Offset is written to the unformatted CDR as 0.	V4.1	
98	VNGR-11767	*Interoperability*	In a 6 Mb, Video Switched conference, HDX endpoints that declare 2 Mb capability may only connect at a line rate of 896 Kbps after 30 seconds.	V4.1.1	
99	VNGR-11798	*Interoperability*	When Tandberg C20 endpoint sends Content, the far end indicates that Content is being received but received Content is black.	V5.0.0	
100	VNGR-11810	*H.323*	The following assert may appear when H.323 participant connects to a 2 Mb Continuous Presence conference: File:AuditorApi.cpp, Line:112, Code:1.; ASSERT:Audit_free_Data_is_too_long_20882,_max_is_20480data_size_is_:_20882	V5.0.0	
101	VNGR-11830	*Interoperability*	Sony XG80 endpoint cannot send Content in H.323 384 Kbps call.	V6.0	
102	VNGR-11843	*Video*	In a 2 Mb Video Switched conference with 10 or more H.323 endpoints connected, random video refreshes may occur.	V5.0.0	
103	VNGR-11883	*General*	After software upgrade, it is necessary to close and reopen Internet explorer.	V5.0.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
104	VNGR-11920	*Interoperability*	In a 4 Mb RPX conference with LPR enabled, video-out bit rate decreases to 128 Kbps due to packet loss and does not increase.	V5.0.0	
105	VNGR-11949	*SIP*	The maximum number of Meeting Rooms, Entry Queues, SIP Factories and ongoing conferences that can be registered to the Proxy, is limited to 100.	V5.0.0	
106	VNGR-11953	*Cascading*	When connecting to a cascaded CP conference with a 768Kpbs line rate and the video quality set to Sharpness, HDX endpoints experience bad video quality.	V5.0.0	
107	VNGR-11963	*Interoperability*	In a conference running at a line rate of 384 Kbps with AES, LPR and Video Clarity enabled, HDX ISDN participants connect with SIF resolution while HDX IP endpoints connect using a 4SIF resolution.	V5.0.0	
108	VNGR-11965	*Video*	In a conference running at a line rate of 384 Kbps, with AES and LPR enabled, calls connect using the H.263 instead of the H.264 video protocol.	V5.0.0	
109	VNGR-11987	*General*	When upgrading from V4.0.3 to V5.0, after inserting the activation key an invalid key message appears.	V5.0.0	Logout and login to the web browser or reopen the Internet Explorer.
110	VNGR-12006	*SIP*	With SIP defined and undefined dial-in participants you cannot change the layout type from “conference layout” to “personal layout”.	V5.0.0	
111	VNGR-12007	*ISDN*	Occasionally, when ISDN participants connect to a conference with line rate 384kbs, multiple asserts appear in the log file.	V5.0.0	
112	VNGR-12011	*ISDN*	Occasionally, an ISDN participant fails to connect to the conference due to the following error - “MCU internal problem - 50020".	V5.0.0	
113	VNGR-12031	*IVR*	A conference running at a line rate of 1920Kbpsand IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	V5.0.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
114	VNGR-12033	*General*	Rarely a system error (BridgePartyVideoOut.cpp, Line:1458, Code:1701.; DEBUG-ASSERT:) is written to the log file if a change is made to the conference layout while participants are disconnecting.	V5.0.0	
115	VNGR-12034	*ISDN*	In a conference running at a line rate of 384 Kbps, H.320 encrypted participant cannot connect and an assert appears.	V5.0.0	
116	VNGR-12100	*General*	Occasionally, after upgrading to version 5.0 (from 4.0.3, 4.1.0, 4.1.1), the soft reset fails.	V5.0.0	First try to reset from the SHM if possible. Otherwise hard reset the system.
117	VNGR-12116	*General*	When a participant is moved from one conference to another and becomes the single participant in the destination conference, the participant does not hear music.	V5.0.0	
118	VNGR-12172	*RMX Web Client*	In the RMX Web Client, the main window opens up as full screen and cannot be resized.	V5.0.0	
119	VNGR-12177	*Interoperability*	In a conference with AES, LPR and Video Clarity enabled, H.320 Tandberg MXP endpoints connect with resolution of 960x720, while identical H.323 MXP endpoints connect with resolution of 720p.	V5.0.0	
120	VNGR-12178	*Content*	RMX does not support H.264 Content in ISDN calls.	V5.0.0	
121	VNGR-12202	*Encryption*	Rarely, in an encrypted conference, H.323 encrypted dial-in and dial-out participants cannot connect and an assert appears (File:EncryptionKeyServerManager.cpp).	V5.0.0	
122	VNGR-12257	*RMX Web Client*	When upgrading the RMX Web Client with software changes, Internet Explorer needs to be closed and opened before the upgrade can take place.	V5.0.0	
123	VNGR-12266	*Interoperability*	Tandberg MXP endpoint receives ghosted video from HDX9004 endpoint during H.323 conference.	V5.0.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
124	VNGR-12355	*Interoperability*	DST K60 endpoint receives tiled video from HDX9004 endpoint during H.323 conference.	V7.1	Set the system flag SEND_WIDE_RES_TO_IP to NO to force the system to send 4CIF.
125	VNGR-12369	*Interoperability*	Tandberg C20 endpoint periodically displays fast updates in HD1080p conferences.	V5.0.0	
126	VNGR-12372	*Interoperability*	Tandberg 6000 E and B series, H.320 endpoints do not connect to conferences when encryption is enabled.	V5.0.0	
127	VNGR-12373	*Interoperability*	HDX endpoint connected via H.320 does not receive Content from Tandberg MXP endpoint connected via H.323.	V5.0.0	
128	VNGR-12732	*Upgrade Process*	After upgrading the system from version 5.0 to version 4.6, the Users list is deleted and the default POLYCOM User is created. For security reasons, it is recommended to delete this User and create your own User.	V4.6	
129	VNGR-13001	*Video*	Video display freezes momentarily with every speaker or layout change in a conference with HDX and SVX endpoints.	V4.6	
130	VNGR-13152	*Video*	Message overlay is limited to 32 Chinese characters OR 96 ASCII characters.	V4.6	
131	VNGR-13314	*Partners - Microsoft*	When resetting the RMX after loading the certificate and registering the RMX with the OCS, two active alarms appear: “SIP registration transport error” and “No response from Registration server”.	V6.0	
132	VNGR-13729	*Unified Communication Solution*	When connecting from a MOC endpoint using the link sent in the meeting invitation to an ongoing conference that was scheduled via the Polycom add-in for Microsoft Outlook on the RMX 4000 (standalone) with Gathering and Recording enabled, the conference is not started as a Meeting Room/Conference Reservation or ongoing conference with the same name already exist in the MCU.	V6.0	
133	VNGR-13808	*General*	On an RMX 2000, you able to enter an invalid flag (CS_TUNNELING instead of H245_TUNNELING) onto the system.	V4.1.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
134	VNGR-13832	*RMX Manager*	When the RMX is in an Ultra Secure Mode, the RMX Manager window appears “Maximized”. After changing the layout settings, after re-login the latest settings are not implemented.	V5.0.1	
135	VNGR-13951	*RMX Manager*	On the RMX 2000/4000, on the RMX Manager - IP Network Service, open the Properties window and then click Management Network, the Management Network pane UI remains offset.	V5.0.1	
136	VNGR-14047	*Interoperability*	Artifacts appear on LifeSize _RM1_4.5.1(15) endpoint connected via SIP or H.323 to a 2Mbps conference with Video Quality set to “Sharpness” running on the RMX 2000 in MPM mode. The LifeSize endpoint is using 4SIF 30 resolution while Polycom endpoints are using 720*400 resolution.	V6.0	
137	VNGR-14062	*General*	On a fully loaded RMX 4000, endpoint may disconnects with Call Disconnection Cause stated as “ MCU internal problem - 11122".	V6.0	
138	VNGR-14124	*Video*	On rare occasions in 2Mbps ISDN calls, ISDN participants connected without their endpoints sending video for a few seconds.	V6.0	
139	VNGR-14151	*General*	A Shelf Voltage problem is always displayed in the System Alerts pane regardless of the actual status.	V6.0	
140	VNGR-14159	*General*	Operator assistance function is blocked when the TelePresence mode is enabled.	V6.0	
141	VNGR-14175	*RMX Manager*	When using the RMX Manager, a Message Alert “500” is displayed when an RMX running Version 4.6 is selected in the MCU's list.	V6.0	
142	VNGR-14417	*General*	On an RMX 2000, when QoS is selected in the IP Network Service and connecting more than 5 HDX endpoints in an HDCP call, packet loss occurs when sending audio and video.	V5.0.1	
143	VNGR-14578	*Audio*	On an RMX with a license for 800 audio only participants, a disconnection cause always occurs after connecting the 767th participant.	V6.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
144	VNGR-14624	*General*	After changing the conference profile assigned to a conference template that includes participants, some of these participant are randomly deleted from the conference template.	V7.0	
145	VNGR-14667	*General*	When defining a New Profile in the Video Settings tab and selecting a Layout, in the Conference Profiles list there is no indication of the selected layout and the layout icon is missing.	V6.0	
146	VNGR-14687	*Audio*	When connecting 800 VOIP using 4 Entry Queues and 396 Ad Hoc conferences, when adding Dial out participants to the conferences they could connect. An MCU error message appears: MCU INTERNAL PROBLEM - 65012.	V6.0	
147	VNGR-14688	*General*	When a conference is deleted in the RMX Manager, conference participants are not deleted in the participants list.	V6.0	
148	VNGR-14767	*General*	H.323 party disconnect due to MCU Internal Problem 32212.	V6.0	
149	VNGR-14778	*RMX Web Client*	ISDN/PSTN fields are disabled (grayed out) although Enable ISDN/PSTN Dial-in check box is selected when modifying an existing Entry Queue. Does not happen when creating a new EQ.	V6.0	
150	VNGR-14780	*Interoperability*	RMX4000 using 4Mb, Same Layout, Sharpness, Video Clarity in profile and Entry Queue becomes inaccessible when called via an Entry Queue from H.323 LifeSize endpoint.	V6.0	
151	VNGR-15101	*IVR*	In a Video Switched 4Mbps conference, only the last part of DTMFs *6 (mute) and #6 (unmute) messages are heard.	V7.0	
152	VNGR-15131	*IVR*	In a conference started from a Profile, when an ISDN call is forced to Audio algorithm G722_1_C_24k a buzzing noise can be heard before the IVR starts.	V7.0	
153	VNGR-15155	*Video*	In a conference with a line rate of 4096kbps, set to Sharpness, 1+5 layout, after connecting a few endpoints, when an endpoint dials out, video In & Out freeze.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
154	VNGR-15222	*RMX Manager*	After disconnecting the AC power or physically removing the power supply, an alarm is not generated on the RMX and the RMX Manager Hardware Properties show the disconnected power supply status as "Normal".	V5.0.1	
155	VNGR-15256	*Encryption*	When using DTMF codes (*71/#71/*88) to secure and unsecure a conference in which these codes are enabled for everyone in the IVR Service, there is no text/icon indication on the HDX 8000/9000, VSX 3000, Tandberg and Lifesize endpoints.	V7.0	
156	VNGR-15281	*Interoperability*	When Aethra VegaStar Gold endpoint connects via ISDN to 384kbps conference, the created CDR Event shows the participant status as "Connected with problem" .	V7.0	
157	VNGR-15320	*General*	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	
158	VNGR-15324	*General*	When monitoring a CP conference with 5 or more endpoints from 5 Web Client sessions on separate workstations, Video Previews can be opened from 4 workstations. Attempting to open a fifth Video Preview causes an error "Failed to Preview Video: Failure Status" instead of "The Preview cannot be displayed. The maximum number of previews per MCU has been reached.	V7.0	
159	VNGR-15386	*Video*	Artifacts present in the Gathering Slide in 2560kbps, CP conference with Motion selected.	V7.0	
160	VNGR-15523	*Partners - Microsoft*	Primary and Secondary dial in numbers entered in the Polycom Conferencing Add-in to Microsoft Outlook are always displayed on the Gathering slide (during the gathering phase) for reference, even if the participant connected using the invitation link.	V6.0	
161	VNGR-15541	*Video*	Create a conference on the RMX using the default factory video profile, connect a Sony PCS-G50 endpoint, and then try to control the XG80's camera. There is no response.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
162	VNGR-15649	*Interoperability*	In a continously running conference, after two HDX7000 and VSX7000 endpoints disconnect, the HDX4000 endpoint's video freezes.	V7.0	
163	VNGR-1569	*CDR*	When the conference termination time is changed, the CDR is not updated.	V1.0.0	
164	VNGR-15700	*Software Version*	When PCM is initiated, site names are displayed over the PCM menu.	V7.0	
165	VNGR-15704	*Content*	Tandberg 6000 MXP H.320 endpoint receives poor quality content from Tandberg Edge95 MXP H.323 endpoint during a 384 kbps, CP, encrypted conference.	V5.1	
166	VNGR-15706	*Video*	Tandberg H.320 6000 MXP endpoint displays video freezes throughout the duration of a conference set to motion & encryption.	V5.1	
167	VNGR-15707	*ISDN*	When a Tandberg 6000 MXP connects over H.320 to a 384kbps conference running on RMX 4000 with Motion and AES enabled, the endpoint encounters video freezes.	V7.0	
168	VNGR-15718	*General*	When pulling the LAN cable from the RMX, incorrect disconnection cause is displayed on the endpoints: "call close normal".	V7.0	
169	VNGR-15719	*Interoperability*	Tandberg C20 endpoint stops receiving video when the HDX8006 sends content during 6 mbps HD1080p encrypted conference.	V5.1	
170	VNGR-15724	*Software Version*	On RMX with MPMx, when a skin without background is selected, the Polycom skin background is displayed. When a skin with a background is selected, the speaker notation color is incorrect.	V7.0	
171	VNGR-15737	*General*	In the Resolution Configuration Slider, the CIF30 slider is absent from the UI.	V7.0	
172	VNGR-15755	*General*	During an active Telepresence conference, when clicking the Video Settings tab, the "Telepresence Mode enabled” check box appears to indicate the status of the Telepresence Mode.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
173	VNGR-15757	*Software Version*	Initiating PCM when there is only one endpoint connected to a conference that is receiving music results in the music being interrupted.	V7.0	
174	VNGR-15798	*Partners - Microsoft*	In ICE environment, a green overlay is displayed on top of one of the video layout in the Gathering slide when a dial out MOC or HDX endpoint connect to the conference.	V7.0	
175	VNGR-15822	*Software Version*	When PCM is activated in a Gathering-enabled conference, the PCM menu is displayed on top of the gathering slide instead of the display of the Gathering Slide being terminated before the PCM menu is displayed.	V7.0	
176	VNGR-15831	*IVR*	When uploading a number of high and low resolution slides to an IVR service, there is only option to choose one slide.	V7.0	
177	VNGR-15939	*Interoperability*	In a “Fixed resource Capacity” mode, Legacy endpoints can still receive content when they should not.	V7.0	
178	VNGR-15953	*General*	When copying an on going conference that is based on a Profile that was deleted while the conference is running, when pastig the conference, it is added to conference templates.	V7.0	
179	VNGR-16103	*General*	After running diagnostics on the RMX, LED functionality is not documented.	V7.0	
180	VNGR-16120	*General*	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	
181	VNGR-16210	*RMX Web Client*	When trying to open the video Preview from a fifth computer's Web browser connected to a conference running on the RMX 1500, all the other four browsers that were running from four different computers close, and the error message"failure status" is displayed on some of the browsers.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
182	VNGR-16281	*Content*	Content sent from HDX (in H.264) is automatically stopped when a second participant that does not support H.264 Content (for example, CMAD that only supports H.263) joins the conference. When the content is sent again, the Content protocol is H.263+ to enable all conference participants to receive content.	V7.0	
183	VNGR-16283	*General*	When opening the video preview pane during a conference and previewing the next participant without closing the previous preview pane, the pane is minimized and does not show video of the next participant.	V7.0	
184	VNGR-16313	*IVR*	When running a 512kbps conference with Gathering, IVR and Echo Suppression enabled on RMX 2000 with MPMx card and the resource allocation is set to Flexible Mode, the IVR slide flashes when dialing out using H.261.	V7.0	
185	VNGR-16363	*Interoperability*	When starting a new 2MB conference on the RMX2000 with MPMx card, Ipower endpoints take a long time to connect.	V7.0	
186	VNGR-16377	*General*	On an RMX with MPM+ card, when starting a VSW conference from the Profile, the maximum line rate that can be selected is 6144kbps.	V7.0	
187	VNGR-16378	*Interoperability*	In a SD conference (1024 resolution) with motion, auto layout enabled, when connecting HDX and dial in from Life Size endpoint, the endpoints do not connect in SD with 60 FPS as required.	V7.0	
188	VNGR-16387	*Interoperability*	On an RMX2000 with the MPM+ card, when connecting with an HDX9000 endpoint to the Entry Queue using a line rate of 384Kbps, the IVR slide blinks.	V7.0	
189	VNGR-16422	*Software Version*	RMX 2000 logs off during upgrade procedure when network is under stress.	V7.0	When the network is busy, use the RMX Manager application instead of the RMX Web Client to control the MCU.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
190	VNGR-16427	*Software Version*	On RMX 1500 with two conferences running and Legacy Content enabled, line artifacts are displayed in the middle of the CMAD screen after it is disconnected from the first and reconnected to the second conference.	V7.0	
191	VNGR-16460	*IVR*	On RMX 2000 with MPMx, H.261 endpoint that displays the default slide does not access nor display a new slide that is added to the IVR Service.	V7.0	
192	VNGR-16462		When downgrading to software V6.0.0.105 and performing “Comprehensive restore” to Factory default, followed by upgrade to version V7.0.0.115 the upgrade procedure is stuck in “Software Loading” phase. System Reset (hard or soft) is required to resolve the problem.	V7.0	
193	VNGR-16523	*FECC*	When connecting a Tandberg SIP endpoint to a conference running on RMX 1500 at a line rate of 384kbp, FECC does not work.	V7.0	
194	VNGR-16535	*SIP*	SIP HDX sites (Version 2.6.1 and 2.6.0) receive video in resolution of 432x240 instead of 720p when connecting to a CP conference running on RMX 4000 at a line rate of 1920Kbps with 10+ layout selected and LPR is enabled.	V7.0	
195	VNGR-16539	*IVR*	In a mixed H.323 & SIP 128Kbps conference with Video Clarity, Sharpness, IVR Service and Welcome Slide settings set to “High profile optimized”, when connecting HDX 8000 endpoints, the H.323 HDX endpoint does not view the IVR slide but a black screen for 15 seconds.	V7.0	
196	VNGR-16560	*General*	Sometimes after log-in to the RMX 1500 Web Client, a Microsoft .NET Framework error message may appear.	V7.0	
197	VNGR-16562	*Gateway*	Gateway sessions are always running in CP mode. If Video Switching is selected in the Profile, the system will change it to CP mode, using the closest possible video settings. However, 60fps may not be supported in CP mode for the selected line rate.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
198	VNGR-16595	Interoperability	On an RMX 4000 & MPM+ cards, running at 1920Kbps conference with Video Clarity, Auto Terminate, Video Quality, Sharpness, Encryption, LPR, Echo Suppression, Auto Layout, Gathering and Content for Legacy Endpoints enabled, when connecting 20 HDX, Tandberg 17000 and edge95 MXP & 3 Tandberg C series endpoints an MFA card error occurs.	V7.0	
199	VNGR-16624	General	In the RMX Manager, when attempting to upgrade two RMX simultaneously, the Install Software window only appears for one RMX, when you should view both.	V7.0	
200	VNGR-16722	Video	On RMX 2000 with one MPM-H, small artifacts are displayed in the Gathering Slide when the configuration is changed to Presentation Mode during the Gathering Phase.	V7.0	
201	VNGR-16724	Video	On RMX 1500, video display freezes momentarily during Video Layout changes before the new Video Layout is displayed.	V7.0	
202	VNGR-16742	Diagnostics	On an RMX2000 with MPMx_D cards when performing an Power ON Self Test (POST), the MPMx card runs the card monitoring test in an endless loop.	V7.0	
203	VNGR-16754	Diagnostics	The following message appears: “connection with shelf management is lost, please log in again”. You can only exit the Diagnostic mode after physically turning the RMX Off and On.	V7.0.2	
204	VNGR-16757	RMX Manager	When starting a new conference from a conference template, the new conference is not selected or highlighted in the conferences pane.	V6.0	
205	VNGR-16794	Audio	On RMX 4000 with MPM+, G.728 codec isn't declared 1st codec in conference at 96kbps.	V7.0	
206	VNGR-16809	IVR	DTMF Code *71 (Secure Conference) sent to RMX 1500 displays Gathering Slide Text instead of "Secured" indicator text.	V7.0	
207	VNGR-16841	Interoperability	Connect to the network using VPN and then start a conference with LPR enabled, connect endpoints using CMAD, the video of the endpoints was very fragmented.	V7.0	A CMAD issue.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
208	VNGR-16871	*Software Version*	When LPR is activated in a conference, the actual HDX endpoint's “Used Call Rate” is approximately 100kbps lower than expected.	V7.0	
209	VNGR-16901	Software Version	On RMX 1500 Video Preview is preceded by a green screen momentarily before Video Preview starts.	V7.0	
210	VNGR-16919	Audio	On RMX with MPMx using H.323 with HDX endpoint, sites receive Siren14 instead of Siren22 Stereo audio algorithm in 6Mbps VSW conferences.	V7.0	An endpoint issue (VIDEO-88345) .
211	VNGR-16924	Interoperability	In DMA, when a SIP endpoint is connected to a certain MCU, and the user chooses to stop using it, the call is routed to a different MCU while the call rate is reduced by 64k.	V7.0	May be a DMA issue.
212	VNGR-16955	*Interoperability*	iPower 9000 endpoint in H.323 call with RMX with MPM+ or MPMx does not transmit audio in encrypted calls.	V7.0	
213	VNGR-16974	*ISDN*	Dial-in or dial-out ISDN endpoints do not connect at line rates higher than 768kbps, irrespective of profile setting.	V7.0	
214	VNGR-16981	*Audio*	Audio volume of PSTN audio-only participants connecting via GW is approximately three times lower than that audio volume of video participants.	V6.0	
215	VNGR-16997	*LPR*	LPR is enabled by default in the conference profile when CP mode is selected. LPR is disabled by default in the conference profile when VSW mode is selected. Changing between CP and VSW modes causes LPR to be enabled/disabled.	V7.0	
216	VNGR-17001	*Hardware*	MPMx card remains in startup mode instead of Major state after restoring the RMX to factory defaults and without configuring the IP address of the media card(s) in the Fast Configuration Wizard.	V7.0.1	
217	VNGR-17104	*FECC*	In a 512 kbps H.323 conference with two HDX endpoints, FECC is extremely slow.	V7.0	
218	VNGR-17395	*Interoperability*	During a video conference between 3 ST client s and a video Desktop endpoint, zebra video artifacts appear on the conference layout of all endpoints.	V7.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
219	VNGR-17409	*Upgrade Process*	Sometimes, when upgrading an RMX 2000 with two MPM cards from version 6.0.2 to 7.0.2, the Software Loading process remains stuck at 22%.	V7.0.2	An IBM Lotus Sametime Client issue.
220	VNGR-17509	*Hardware*	Sometimes during a conference, the error message “no LAN connection” appears as a result of momentary network problems. However, the endpoints remain connected to the MPM card.	V7.0.2	Check the network.
221	VNGR-17525	*Video*	A black vertical line is displayed between cells where usually there is a border when OTX and RPX 400 endpoints are connected to a conference running on RMX system with MPMx at a line rate of 4MB and video Quality set to Sharpness.	V7.0.2	An endpoint issue (VIDEO-86473)
222	VNGR-17616	*Audio*	HDX H.323 endpoint receives G.722 audio instead of Siren22 (as the SIP endpoints) when connected to a conference running at a line rate of 384kbps on RMX4000 with MPM+ and the CS_ENABLE_EPC flag is set to YES.	V7.0.2	Not an RMX issue; Endpoint issue (VIDEO-88386) .
223	VNGR-17668	*Interoperability*	Sony PCS-XG80 receives video at a resolution of 432x240 instead of 720p when connected to a CP conference running on RMX 2000 with MPM+ at a line rate of 1920kbps with LPR, Video Clarity and Send Content to Legacy Endpoint options enabled.	V7.0.2	
224	VNGR-17689	*ISDN*	Blurred (Predator) video is displayed on the HDX endpoint that is in self view when a movement occurs while the endpoint is connected via ISDN to a conference running at a line rate of 1472kbps, with encryption enabled.	V7.0.2	
225	VNGR-17724	*General*	After Comprehensive Restore to Factory Defaults, an active alarm displayed, indicating voltage problem on MPM-f - card.	V7.0.2	
226	VNGR-17746	*Partners - Microsoft*	In an environment that includes the Microsoft Lync server and RMX 4000 MPM+80 with ICE enabled, when the Lync client escalates to video after connecting as Audio Only to a Meeting Room that is running at 384kbps, with Encryption and LPR enabled, artifacts appears at the start of the video.	V7.0.2	Not an RMX issue; Microsoft Lync Server issue.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
227	VNGR-17818	*General*	Video Preview cannot be disabled.	V7.0	
228	VNGR-17888	*Video*	Full screen layout is displayed instead of 3x3 layout when the 3x3 layout is selected using Click&View from HDX9004 version 2.7.0-5547. Conference is running on RMX 2000 with either MPM+ or MPMx.	V7.0.2	
229	VNGR-17889	*RMX Manager*	The RMX Web Client does not show the status of the link between the client and the MCU correctly when it is failing. A manual reset was required to reestablish the link.	V7.1	
230	VNGR-17944	*ISDN*	ISDN HDX endpoints may disconnect from ongoing conferences following a recovery of the processing unit.	V7.1	
231	VNGR-18021		In DMA, when a SIP endpoint is connected to a certain MCU, and the user chooses to stop using it, the call is routed to a different MCU while the call rate is reduced by 64k.	V7.0	
232	VNGR-18102	*RMX Manager*	In Event mode, the Lecture mode is not disabled.	V4.7	
233	VNGR-18116	*Interoperability*	In a 384 Kbps CP conference with LPR and AES enabled, when Touch Control changes the layouts, HDX endpoints hear a string of DTMF tones after each change.	V7.1	
234	VNGR-18211	*RMX Manager*	On RMX2000 with MPMx-S, when two ViewStation endpoints connect to the conference using H.263, the Video Port Usage display on the RMX Manager displays 3 ports used. The Administrator guide states 4 ports.	V7.0	
235	VNGR-18330	*Resource Capacity*	On the in RMX 4000, the maximum number of video participants in one conference is limited to 180.	V7.2	
236	VNGR-18344	*RMX Manager*	After changing the status of an Ongoing Meeting Room to “Permanent Conference”, in the Meeting Room pane the status remains unchanged.	V4.7	
237	VNGR-18357	*Multilingual*	When the PCM menu is set to the Japanese language, Click & View appears in English as it is Polycom registered name for this feature.	V7.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
238	VNGR-18370	*Interoperability*	In Meeting Rooms where the conference line rates are higher than 384 kbps, Sony PCS1600 endpoints connect as Audio Only.	V7.0.1	
239	VNGR-18438	*Upgrade Process*	When upgrading to version 7.5 the following error message appears: “installation of MCU version failed”. This is caused when the bin file exceeds 200MB.	V5.0.2	
240	VNGR-18443	*Security*	RMX Manager is designed not to Remember Login, Username and Password when in Ultra Secure Mode.	V7.5	
241	VNGR-18497	*Interoperability*	On a Radvision Scopia XT1000 endpoint the PCM menu appears on screen, however you cannot select or execute some of the menus.	V7.1	
242	VNGR-18522	*Interoperability*	When using PCM to use Click & View, the menu appears in the middle of the screen.	V7.1	
243	VNGR-18528	*FECC*	Documentation has been updated to reflect time out behavior for PCM and FECC remote camera control.	V7.1	
244	VNGR-18554	*CMA*	On an RMX registered to the IOS/CMA, when an VVX endpoint connects to the conference, no video is seen.	V7.1	
245	VNGR-18622	*RMX Manager*	An RMX 2000 in the MPM+ mode recognizes in the Hardware Monitor the MPMx card and displays a “normal” status when the card is in fact disabled.	V4.7	
246	VNGR-18637	*Interoperability*	When content is sent from an ISDN HDX7006 endpoint, Lifesize Room 200 endpoint cannot view the content.	V7.1	Not an RMX issue; LifeSize issue.
247	VNGR-18679	*Interoperability*	Endpoints defined in the Global Address Book of the CMA with both H.323 and ISDN numbers, will be called by the RMX using only the H.323 number and not the ISDN.	V7.1	
248	VNGR-18718	*General*	After starting Basic Diagnostic Mode on the system, in the Hardware Monitor the Estimated Duration field lists an inaccurate number of minutes that remain until completion.	V7.1	
249	VNGR-18772	*General*	Incorrect timing values in Release Notes 7.0.2 have been corrected for version 7.0.3 Release Notes.	V7.0.2	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
250	VNGR-18918	*Recording*	Display of recording icon when recording an ongoing conference is not supported in MPM+ Card Configuration mode.	V7.1	
251	VNGR-18936	*Interoperability*	In a conference on an RMX with MPMx cards, H.320 LifeSize Room endpoints do not receive content.	V7.1	
252	VNGR-18943	*Interoperability*	In a 4096 kbps CP conference with Auto Layout, LPR and Graphics enabled, when an Sony XG80 endpoint sends content, HDX endpoints do not see video.	V7.1	
253	VNGR-18985	*Content*	When Serial endpoint sends content, the H.323 endpoint views a black screen, when serial endpoint stops content, content remains frozen for 10-20 seconds and then endpoints view frozen video.	V5.1	
254	VNGR-18990	*Video*	On an RMX 2000 with MPM+ cards and a 4Mb conference with Motion enabled, 2 OTX-306, 1 RPX-400 endpoints, horizontal black lines appear.	V7.1	
255	VNGR-19038	*Software Version*	On an RMX 2000/4000 with Ultra Secure Mode/ Secure Communication enabled, after a system restart; the system date sometimes reverts back to a previous date or incorrect date.	V7.5	
256	VNGR-19068	*H.323*	In an 512 Kbps SIP/H.323 VSW conference with LPR, Sharpness, Graphic Auto Layout and Video Clarity enabled, when sending content from an HDX endpoint, VSX endpoints cannot view content.	V7.1	
257	VNGR-19076	*Gateway*	When an IP call is forwarded from the RadVision Gateway to RMX over ISDN, bad video can be seen.	V7.1	
258	VNGR-19077	*Content*	In a ISDN cascaded conference that places a call using the Codian Gateway, after sending Content the call disconnects.	V7.1	
259	VNGR-19085	*Content*	In a conference with mixed H.323 and ISDN endpoints, when content switches between participants, the ISDN participant can receive the content token but cannot resend it. As a result all participants view black screen for a few seconds, and then the view returns to normal video.	V7.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
260	VNGR-19109	*SIP*	In an 768 Kbps CP conference with Auto Layout, Gathering, LPR, Sharpness Graphics and Video Clarity enabled, the SIP call negotiates H.263 instead of H.264.	V7.1	
261	VNGR-19262	*ISDN*	On an RMX 2000 with MPMx cards, the maximum capacity of 40 ISDN participants could not be attained when participants connected at 256Kpbs to a conference running at a line rate of 512Kbps as downspeeding of the conference line rate is not supported.	V7.1	Set the Conference line rate to 256Kbps
262	VNGR-19323	*Content*	After setting up a conference and sending content, while connected to a RSS4000 the content's resolution dropped from H.264 to H.263.	V4.7.1	
263	VNGR-19364	*General*	Changing the font size display of the workstation monitor does not change the size of the fonts displayed in the RMX Documentation and Utilities screens provided on the Polycom USB key shipped with the RMX.	V7.1	
264	VNGR-19422	*Content*	The Tandberg 6000 E does not receive content from the HDX9004 in H320 conferences. The Tandberg displays a black screen on its content monitor.	V7.1	
265	VNGR-19423	*Content*	When two 512 kbps conferences are created and cascaded with an ISDN link with Content enabled, when ISDN & IP endpoints connected, the IP endpoint attempts to snatch the token from an ISDN endpoint.	V7.1	
266	VNGR-19459	*General*	When the workstation's screen resolution is set to 1280 x 720, the Accept Agreement button in RMX Documentation and Utilities screen provided on the Polycom USB key is cut and the screen becomes corrupted when enlarging the display using Ctrl, +, +.	V7.1	
267	VNGR-19505	*Interoperability*	Tandberg MXP endpoints connect as Audio Only to Video Switching conferences running at a line rate of 768 kbps and resolution of SD 30 fps on RMX Version 7.0.x with MPM+ card installed.	V7.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
268	VNGR-19507	*Video*	During a 1728 Kbps COP Cascaded conference with 10 dial-in and dial-out endpoints, Video Sites Names appear too small.	V4.7.1	
269	VNGR-19536	*General*	The Default IP Network Service configured using the Fast Configuration Wizard is not saved if no media cards are installed in the RMX during the configuration process.	V7.1	
270	VNGR-19541	*Interoperability*	Tandberg C20 and C90 endpoints, version TC4.0.1.240265 connect as audio only to a VSW HD conference running at a line rate of 6Mb on RMX version 7.1. Issue is not reproduced when Tandberg release 3.1.2 is installed on the endpoints.	V7.1	
271	VNGR-19606	*Cascading*	During a 2Mb/384 kbps cascaded conferences with H.239 People+Content enabled, both conferences cannot view content.	V7.0.2C	
272	VNGR-19628	*SIP*	The RMX system changes the Call-ID for each new registration. This may trigger a boot cycle on certain SIP Servers.	V7.0.2	
273	VNGR-19767	*Encryption*	A Tandberg 6000 DMA registered endpoint requires several attempts to connect to an AES encrypted ISDN conference.	V7.6	
274	VNGR-19782	*Resource Capacity*	On an RMX 2000 running a 1024 kbps CP conference with Auto Layout, Auto Brightness, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, after connecting H.263 CIF VSX endpoints, each endpoint used 1.5 resources instead of 1.	V7.2	
275	VNGR-19952	*Upgrade*	On an RMX 1500, a Power Supply voltage active alarm is triggered in error on sensor 8.	V4.7.1	
276	VNGR-20056	*General*	On an RMX in with the flag; ULTRA_SECURED_MODE and Multiple Services enabled, when attempting to configure additional IP Network services (when the default IP Network service already configured), all IP address slots appear as available even though these slots are already occupied by the default IP Network Service.	V7.5	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
277	VNGR-20223	*ISDN*	In a 1920 Kbps CP conference with Auto Layout, Gathering, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, after connecting H.320 Sony PCS-XG80 endpoint no video can be seen.	V7.2	
278	VNGR-20247	*Video*	During a conference with Telepresence endpoint connected, endpoints view black backgrounds with no borders. After the disconnection of the Telepresence endpoint, the video layout background and borders remain as if in Telepresence mode. The display is updated after the next layout change	V7.2	
279	VNGR-20269	*ISDN*	In a 384 Kbps CP conference with Auto Layout enabled, the H.320 Tandberg Edge95 MXP displays bands of green and purple video.	V7.2	
280	VNGR-20276	*Audio*	Keyboard Noise Suppression and Echo suppression options do not suppress the noise as expected.	V7.2	
281	VNGR-20317	*Partners - Microsoft*	Microsoft Lync client disconnected from a conference running on an RMX2000 with MPMx cards several minutes after connecting to the Meeting Room.	V7.2	
282	VNGR-20353	*Interoperability*	The Tandberg C90 endpoint cannot connect to a conference set to a line rate of 6144Kbps as the Tandberg C90 maximum connection line rate is 6000Kbps.	V7.2	Change the conference line rate to 4096Kbps to fully connect the Tandberg C90.
283	VNGR-20416	*General*	In the Network Traffic Capture (Administration-->Tool-->Network Traffic Capture) pane select Start Network Traffic Capture. When the cyclic check box is not selected, older files are still being deleted.	V7.2	
284	VNGR-20432	*Diagnostics*	On an RMX 1500 after attempting to access the Diagnostic mode manually, the CTNL card remains in a "normal" mode while other cards are in a "Diagnostic" mode.	V7.2	
285	VNGR-20434	*General*	When Hot Swapping MPM+/MPMx cards, Port Usage and Resource reports do not display correctly.	V7.2	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
286	VNGR-20478	*RMX Manager*	Internet Explorer 8 crashed while loading the RMX Manager.	V7.2	Not an RMX issue - an Internet Explorer issue.
287	VNGR-20534	*Content*	In a 128Kbps conference with content started from a Profile, when 20 ISDN endpoints connected the video froze.	V7.2	
288	VNGR-20572	*Interoperability*	On an RMX 1500, after configuring the SIP server & domain, registration failed with the Cisco VSC.	V7.2	
289	VNGR-20574	*Software Version*	After enabling multiple services on the RMX and resetting the RMX system starts up with the message “failed to read MCU time configuration file. (file does not exists)” and an active alarm appears.	V7.2	
290	VNGR-20723	*Software Version*	When a participant accesses an Entry Queue and he/she is then moved from to a conference with a profile different from the Entry Queue, the call is disconnected.	V4.7.2	
291	VNGR-20732	*General*	When stereo is disabled on an QDX endpoint and the QDX dials-in using SIP into an Entry Queue, the QDX endpoint is prompted to enter the conference ID, however the DTMF tones to are not detected by the RMX.	V7.2	
292	VNGR-20829	*Content*	Content is stopped and has to be resent when the Content protocol changes following the connection or disconnection of a participant from the conference.	V4.7.2	
293	VNGR-20855	*SIP*	When resetting the RMX from the Hardware Monitor, SIP endpoints may remain connected, although the conference ended.	V7.2	
294	VNGR-20864	*Diagnostics*	On any type of RMX after accessing Basic Diagnostics and resetting the RMX, after restart the RMX switches to the Advanced Diagnostic mode.	V4.7.2	
295	VNGR-20945	*Partners - Microsoft*	In a conference running at a line rate of 1MB with HDX and Microsoft OC client connected using RTV, Content sent by the HDX was blurred on the Microsoft OC client.	V7.2.1	Not RMX issue. Lync issue.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
296	VNGR-21024	*Partners - Microsoft*	Video with corrupted edges is displayed on MOC clients when connected to a conference running at a line rate of 1MB using RTV.	V7.2.2	Not RMX issue. Lync issue.
297	VNGR-21396	*Recording*	Cannot use an Audio Only Recording Link to record a conference if there are no Voice resources allocated in the Video/Voice Port Configuration.	V7.6	
298	VNGR-21429	*Audio*	HDX endpoints with versions prior to 3.0.3 fail to connect to conferences when SirenLPR is enabled on the RMX.	V7.6	
299	VNGR-21514	*Software Version*	When inserting an MPM card into an RMX 2000 with version 7.6 that does not support MPM card, an active alarm did not appear.	V7.6	
300	VNGR-21729	*General*	The ISDN/PSTN value (true/false) listed in the System Information dialog box are only taken from the activation key according to the license, regardless if the RTM-ISDN card is installed in the RMX.	V7.0.2C	
301	VNGR-21781	*General*	During a conference with Message Overlay enabled, any connected participant can view the overlay message, however connecting participants do not.	V7.0.2C	
302	VNGR-21878	*Video*	Participant's video preview and the CMAD window cannot be open and running simultaneously on the same PC as both require the same DirectDraw resource.	V7.6	
303	VNGR-22018	*Partners - Microsoft*	Click to Conferences is supported only with Microsoft OCS R2 and Lync clients. HDX endpoints are not supported.	V7.6	
304	VNGR-22100	*Hot Backup*	In Hot Backup configuration, the SIP Authentication and configuration of the User Name and Password in the IP Network Service Properties - Security tab of the Master RMX are not backed up in the Slave RMX.	V7.6	
305	VNGR-22181	*General*	In the Hardware Monitor, Slots 1 & 2 may sometimes appear as duplicates in the Slot list.	V7.6	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
306	VNGR-22197	*Cascading*	On two cascaded RMX 4000, after enabling Hot Backup and completing synchronization, the Slave conference displays an alarm: “IP Network Service was modified please reset MCU”.	V7.0.2C	
307	VNGR-22252	*Cascading*	When Hot Backup is enabled between two cascaded RMX 4000s, the Slave's SNMP settings are not synchronized with the Master.	V7.0.2C	
308	VNGR-22290	*General*	When an Operator enters "Awaiting Individual Assistance" queue, after a participant exists the queue and the operator moves to a regular conference, the operator is still in the "Awaiting Individual Assistance" queue.	V7.0.2C	
309	VNGR-22390	*General*	After changing the gatekeeper registration on the RMX 4000 and then restarting the RMX, the IPv6 signaling address field appears empty in the GUI. Retrieval of the External IPv6 signaling address takes time and there is considerable delay before it is loaded onto the GUI.	V7.6	
310	VNGR-22407	*General*	The first 10 OTX systems that connect to the same MPMx card receive video at 1080p 30fps. Any additional OTX system that connects to the same MPMx card will receive video at a lower frame rate.	V7.6	
311	VNGR-22456	*RMX Manager*	Login with the RMX Manager as an Administrator and then select Hardware Monitor, and press the System Reset button. After system reset, the RMX Manager does not remove items from the Administration and Setup menus when the user is not connected to the MCU which can cause a .Net exception to occur when accessing the CDR.	V7.6	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
312	VNGR-22504	*Upgrade Process*	During any software upgrade or downgrade process, if the system identifies that an intermediate version installation is required, the Safe Path Enforcement warning is displayed and the current installation process is aborted. At this point the browser will block any attempt to install any other software version. This applies to all software versions, except for version 7.6 which will still enable a new version downgrade process without closing the browser.	V7.6	Close and then re-open a new browser session.
313	VNGR-22550	*Cascading*	Endpoints failed to receive and view content when an RMX 4000 is in a 384 Kbps cascaded conference with an MGC.	V7.0.2C	
314	VNGR-22617	*General*	When running the Call Generator and the RMX Client on a laptop/computer when PC CPU Usage reaches 100%, the RMX Client disconnects. Workaround: Use the RMX Manager.	V7.0.2C	
315	VNGR-22627	*IVR*	In a conference with the Operator Assistance options enabled, a HDX defined as the operator could not hear the general welcome nor view the video messages. As designed.	V7.5.1	
316	VNGR-22631	*Content*	In Exclusive Content Mode, if an endpoint attempts to send Content a few seconds after another endpoint sent content, the Content stream it is receiving is momentarily interrupted by a slide which is displayed for a few seconds before the normal Content stream is resumed.	V7.0.2C	
317	VNGR-22647	*Interoperability*	A Polycom Immersive TelePresence (ITP) system registered with the CUCM server, after dialing out using SIP and connecting to the primary endpoint, the secondary endpoints must be connected manually.	V7.6	
318	VNGR-22676	*General*	When connecting several participants using blast dial out, the participant that connects using the last available video resource may fail to connect due to lack of video resources.	V7.7	Connect the disconnected participant manually.

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
319	VNGR-22724	*Security*	In Directory Services, the IP Address or DNS Name field will only accept a DNS Name. Entering an IPv4 address in the field results in an error message stating that the Directory Service is not available.	V7.5.1	
320	VNGR-22734	*General*	When running the Call Generator and the RMX Manager on a laptop/computer when PC CPU Usage exceeds 80%, this can result in RMX Manager disconnections.	V7.0.2C	
321	VNGR-22749	*General*	On the RMX with an MPMx card, H263 4CIF(SD) endpoints are allocated as HD resources, which can lead to insufficient resources being allocated to a conference.	V7.2.2	
322	VNGR-22796	*General*	When the RMX is in a Diagnostic mode, in the Hardware Monitor, Loop Tests fail on the ISDN card.	V7.6	
323	VNGR-23060	*Cascading*	A Cascading Link is “connected with problem” when connected to a conference with no other endpoint connected to it and there is no video source to display. Connection is restored to normal (“connected”) once an endpoint connects to that conference.	V7.0.2C	
324	VNGR-23061	*Cascading*	A Slave conference cannot be connected to two Master conferences simultaneously.	V7.0.2C	
325	VNGR-23123	*General*	During a conference, many endpoints could not connect, and intermittently viewed the Welcome Slide for just a few seconds.	V7.1	
326	VNGR-23177	*Interoperability*	Occasionally, when Lifesize endpoint is connected over IPv4 to a conference running on RMX 2000 set to Ultra Secure Mode, the video becomes unstable after several minutes, experiencing frozen video or blank screen and resets itself. This occurs, in both dial-in and dial-out calls to/from RMX.	V7.5.1	
327	VNGR-23182	*General*	In cascaded conferences with Message Overlay enabled, participant line rate and frame rate may decrease.	V7.0.2C	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
328	VNGR-23204	*General*	After the configuration on the NTP servers and system startup, only one NTP server status appears as OK while the two others appears as failed. The NTP server that is listed as “OK” then keeps changing.	V7.5.1	
329	VNGR-23267	*General*	Message Overlay parameters are not saved when saving the ongoing conference to a template.	V7.6.1	
330	VNGR-23335	*General*	For a conference with a short duration (for example 20 minutes), when the conference duration is shorter than the settings of the flag EXTENSION_TIME_INTERVAL, the RMX will add the additional time interval (from the flag) to the conference.	V7.6.1	
331	VNGR-23418	*SIP*	When muting a SIP participant during an ongoing conference, the mute participant icon does not appear in the Participants pane of the RMX Client/RMX Manager.	V7.6.1	
332	VNGR-23423	*IVR*	In version 7.6.1. Event Mode, when pressing DTMF codes, *6 & #6 to mute and unmute the endpoint, the IVR audio file can only partly be heard and cuts off mid-sentence.	V7.6.1	
333	VNGR-23534	*FECC*	During a 768 H.323 conference with FECC, Tandberg endpoints are unable to control Tandberg 6000E using FECC.	V.7.6	
334	VNGR-23627	*IVR*	Cannot add a customized video welcome slide to the IVR Service. Windows 7 operating system crashes.	V7.6H	
335	VNGR-23755	*Interoperability*	During a TIP CP conference set to 1080p resolution, CTS, OTX and HDX endpoints send 720p instead of 1080P.	V7.6.1	
336	VNGR-23764	*IP*	After starting 2 conferences with 600 VoIP dial-out participants, the RMX is unresponsive and an “Internal communication Error” message appears.	V7.6.1	
337	VNGR-23767	*Partners - Microsoft*	Microsoft R1 is not supported with the RMX systems.	V7.6.1	
338	VNGR-23888	*Interoperability*	During ongoing conferences, VSX7000 endpoints cannot open the Content channel as they do not support the BFCP protocol (token management protocol for SIP.	V7.6.1	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
339	VNGR-23892	General	On different RMX's with multiple networks enabled, a number of Internet ports were found to be open and readily accessible by unauthorized parties.	V7.2	
340	VNGR-24009	*Security*	In Ultra Secured Mode, Audio becomes very noisy, when an IP participant connects via the RMX SGW gateway to a conference running on the RMX 2000 with MPM+ card and configured to Multiple Networks.	V7.6.1	
341	VNGR-24071	*Video*	In a CP conference with a Lync client connected, the clients video jumps between HD and QCIF VGA.	V7.6.1	
342	VNGR-24209	*General*	The ACT LED on the FSM (Fabric Switch module) is ON when there is IP packet activity, however when the conference terminate, the ACT LED may remain active (ON) if the card is used for other packet traffic such as run other conferences.	V7.6.1	Reset the RMX from the Hardware Monitor.
343	VNGR-24249	*Interoperability*	A conference passcode created on the DMA system may not conform to the passcode rules enforced by the MCU hosting the conference, causing calls to fail. For example, the maximum number of permitted repeated characters in password is different on the DMA and RMX.	V7.6	Make sure that the passcodes created on the DMA system meet the requirements of the MCUs that the system uses.
344	VNGR-2473	*RMX Web Client*	Sometimes when installing the RMX Web Client, Windows Explorer >Internet Options> Security Settings must be set to Medium or less.	V1.1.0	
345	VNGR-25490	Interoperability	A Sony PCS-G50 endpoint stops sending video when the Sony PCS-XG80 sends content while both endpoints are connected via H.323 to the conference.	V7.7	
346	VNGR-25499	SIP	When the "auto connection" check box is unchecked in the SIP factory's properties and endpoints dial into a SIP Factory, multiple conferences are started but the endpoints never connect.	V7.7	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
347	VNGR-25556	Partners - Microsoft	When a participant attempts to call a Meeting Room using the Lync client, the participant might receive a "Call was not completed or has ended" message. This can occur when the MCU is shut down and the Lync client displays the Meeting Room as Busy and not as Offline. A few minutes after the MCU shutdown, the Meeting Room status will change to Offline. A participant cannot connect to a meeting room when the status is Offline.	V7.7	
348	VNGR-25559	Interoperability	When a number of Lync endpoints dial-in to a Meeting Room, when a Lync endpoint wants to share the desktop, error 488 appears.	V7.7	
349	VNGR-25582	General	Cannot send Content from a RealPresence Mobile endpoint to a conference via a Session Border Controller (SBC).	V7.7	Manually add the flag NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT to the System configuration and setits value to 3.
350	VNGR-26235	Partners - Microsoft	Meeting Room Presence remains "busy" (instead of "available") after all participants disconnected from the meeting.	V7.7	The AVMCU meeting must be manually terminated either by the Lync user who initiated the call or by the RMX Manager.
351	VNGR-26290	Partners - Microsoft	When a Lync participant connected to a Meeting Room running on the RMX tries to invite a third participant to the meeting, a message indicating that the participant has left the conference is played although all three participants are connected to the conference.	V7.7	
352	VNGR-26336	Partners - Microsoft	When a Lync endpoint using SIP is muted during a CP conference, there no indication in RMX Client that the endpoint is muted.	V7.7	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
353	VNGR-26413	Interoperability	M100 endpoint that connected via dial out over *SIP to RMX 1500 cannot send or receive content.*	V7.7	An endpoint issue *(CMAD-8799)*
354	VNGR-26441	Interoperability	When RMX4000 dials out to Avaya SIP endpoints (HDX or AV10xx) registered to ASM via the DMA, endpoints did not connect.	V7.7	DMA issue (DMA-9163)
355	VNGR-26460	Content	Rarely, content sharing session dropped unexpectedly during the conference and a SIP participant was disconnected from the conference followed by the error message "MCU internal problem".	V7.7	
356	VNGR-26687	Partners - Microsoft	When a Lync endpoint that is connected to a Meeting Room running on the RMX escalates the call from audio to video and back to audio many times within a short period, all the Lync participants disconnect from the conference.	V7.7	To suspend and resume the video display during the conference, use the Pause/ Resume video button.
357	VNGR-3089	*HD*	In HD Video Switching conferences, Tandberg endpoints may connect as Secondary when HD frame rate capabilities are less than 7.5 frames per second.	V1.1.0	Create a CP conference
358	VNGR-3276	*SIP*	SIP participants cannot connect to a conference when the conference name contains blank spaces.	V1.1.0	
359	VNGR-3824	*General*	The Click & View menu doesn't appear in 64 Kbps calls.	V1.1.0	Use the RMX Web Client.
360	VNGR-3977	*Interoperability*	Faulty connection status is indicated when the RSS 2000 recording link is the only participant in a conference and its video stream is not synchronized.	V1.1.0	The video stream is synchronized when the first participant connects to the conference.
361	VNGR-4405	*ISDN*	When a busy signal is returned by a PSTN dial-out participant, the RMX does not redial but disconnects the participant with “party hung-up-0” status.	V2.0.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
362	VNGR-4652	*Interoperability*	HDX/VSX endpoints cannot connect directly to conferences while registered with Cisco Gatekeeper using the IP##NID string.	V1.1.0	Connect directly using the MCU IP Address via the Transit Entry Queue.
363	VNGR-5151	*Multilingual*	The Display Name of undefined dial-in participant using HDX and VSX 7000 endpoints is displayed in English in the RMX Web Client.	V2.0.0	
364	VNGR-5310	*Multilingual*	Multilingual Settings are not reflected on the Shelf Management login page and the multilingual flags appear in the Shelf Manager window even when they have not been selected in the Multilingual Settings pane.	V2.0.0	
365	VNGR-6809	*Interoperability*	iPower endpoints are transmitting H.263 video instead of H.264 video in 384Kbps conferences while other endpoints transmit H.264 video.	V7.1	
366	VNGR-6902	*Interoperability*	Sony PCS G70 (v2.61) and Sony PCS-1(v3.41) endpoints cannot connect to conferences using SIP connections.	V5.1	Force the endpoints to connect using H.323 connection.
367	VNGR-7557	*RMX Web Client*	When connecting directly to the Shelf Manager and selecting Diagnostic Mode the CNTL module does not enter the diagnostic mode and stays “Normal”.	V3.0.0	Reset the MCU and then switch to Diagnostic Mode.
368	VNGR-7597	*Interoperability*	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
369	VNGR-7598	*Interoperability*	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
370	VNGR-7734	*IP*	Static Routes table in IP Network Service does not function.	V3.0.0	
371	VNGR-8259	*Software Version*	If an RMX operating in Secure Communication Mode, is downgraded to a version that does not support Secure Communication Mode (V2.0, V1.1), all connectivity to the RMX is lost.	V3.0.0	Cancel the Secure Mode before downgrading

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

NO	Key	Category	Description	Detected in Version	Workaround
372	VNGR-8605	*Interoperability*	The video of Sony G70 endpoint that is connected to a conference over ISDN at line rate of 128Kbps freezes when receiving Content from an HDX endpoint.	V3.0.0	
373	VNGR-9015	*Interoperability*	Radvision ECS Gatekeeper set to Routed Mode is not forwarding the LPR parameters as required, causing HDX calls with LPR enabled to connect with no video.	V3.0.0	
374	VNGR-9228	*Software Version*	When trying to restore last version, after upgrading from version 3 to version 4, the RMX prompts for an activation key.	V4.0.0	
375	VNGR-9340	*CDR*	When a conference was terminated by an MCU reset, an incorrect status “Ongoing Conference” will be displayed in the CDR List pane.	V4.0.0	
376	VNGR-9565	*Upgrade Process*	When downgrading from version 4.0 to version 3.0, the MPM card does revert to normal.	V4.0.0	
377	VNGR-9677	*Interoperability*	When switching Content sending from an HDX9004 to Aethra X7 and back, Content is not received by Aethra X7.	V4.0.0	
378	VNGR-9729	*General*	When moving from MPM+ to MPM mode (with only MPM cards installed in the MCU), the Card Configuration Mode, indicated in the System Information dialog box, remains in MPM+ Mode.	V4.0.0	Logout and then login to the RMX Web Client.
379	VNGR-9740	*Upgrade Process*	When upgrading from version 2.0.2 to version 4.1, and then Restoring the Factory Defaults, during system restart sometimes MPL failure is encountered.	V4.0.0	Turn the MCU off and then turn it on (“hardware” reset).
380	VNGR-9803	*General*	When using the restore to factory defaults, after inserting the Activation key, the system requires a reset when the reset is not required.	V4.0.0	
381	VNGR-9829	*RMX Web Client*	Occasionally, during an ongoing conference, when selecting the Hardware Monitor menu the message “No connection with Switch” appears.	V4.0.0	

Table 2-1 *Version 8.1.4.J - System Limitations (Continued)*

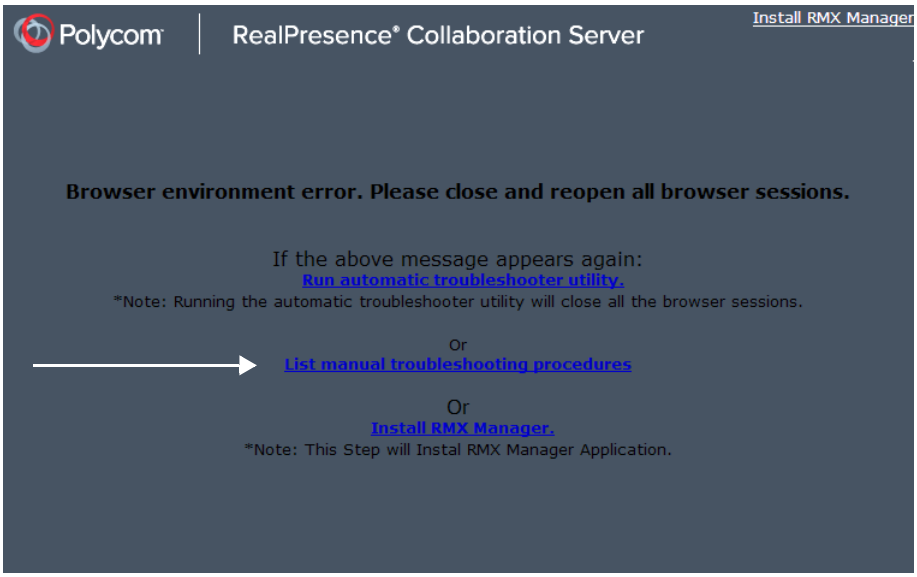
NO	Key	Category	Description	Detected in Version	Workaround
382	VNGR-9830	*Interoperability*	HDX endpoints may experience packet loss when the HDX endpoint's LAN Speed is configured to 100MB.	V4.0.0	Set the endpoint LAN Speed and Duplex Mode to Auto.
383	VNGR-9834	*IVR*	When DTMF codes have been entered by the participants, the volume of the IVR Message may be suppressed or the message may be cut.	V4.0.0	
384	VNGR-9843	*Interoperability*	During an H.323 call, Tandberg 6000 B10 endpoint receives corrupted H239 content from an HDX.	V7.1	
385	VNGR-9844	*Interoperability*	During an H.320 call, Tandberg 6000 B10 endpoint does not receive content from an HDX9004.	V7.1	
386	VNGR-9909	*Interoperability*	When dialing out to a Tandberg MXP ISDN endpoint, the IVR slide is not displayed, although the IVR message is played.	V4.0.0	

Troubleshooting Instructions

RMX Web Client Installation - Troubleshooting Instructions

If a *Browser Environment Error* occurs, close all the Internet Explorer sessions and reconnect to the MCU.

If the problem persists, you can run the *Automatic Troubleshooting Utility* or perform the *Troubleshooting Procedures* manually.



The *Manual Troubleshooting Procedures* include several procedures that can be performed in order to solve the connection error. At the end of each procedure, check if you can connect to the MCU and if the problem persists, perform the next procedure.

In *Secured Mode* (*https//:*), the *DNS* name specified in the RMX's *Certificate* must correspond with that of the *DNS Server* used by the *Client* that is connecting to the RMX.

The following troubleshooting procedures can be performed manually:

- Procedure 1: Ending all Internet Explorer Sessions
- Procedure 2: Deleting the Temporary Internet Files, Collaboration Server Cookie and Collaboration Server Object
- Procedure 3: Managing Add-ons Collisions
- Procedure 4: Add the Collaboration Server to the Internet Explorer Trusted Sites List
- Procedure 5: Browser Hosting Controls (Optional)

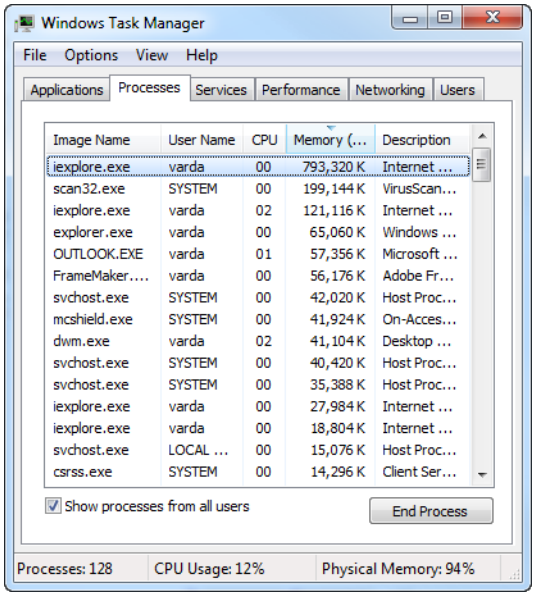
Procedure 1: Ending all Internet Explorer Sessions

In some cases, although all the Internet Explorer sessions were closed, the system did not end one or several IE processes. These processes must be ended manually.

To end all Internet Explorer sessions:

1 Start the **Task Manager** and click the **Processes** tab.

2 Select an **iexplore** process and click the **End Process** button.



3 Repeat this process for all **iexplore** processes that are currently active.

4 Close the *Windows Task Manager* dialog box.

5 Open the Internet Explorer and connect to the MCU.

If the problem persists, continue with Procedure 2.

Procedure 2: Deleting the Temporary Internet Files, RMX Cookie and RMX Object

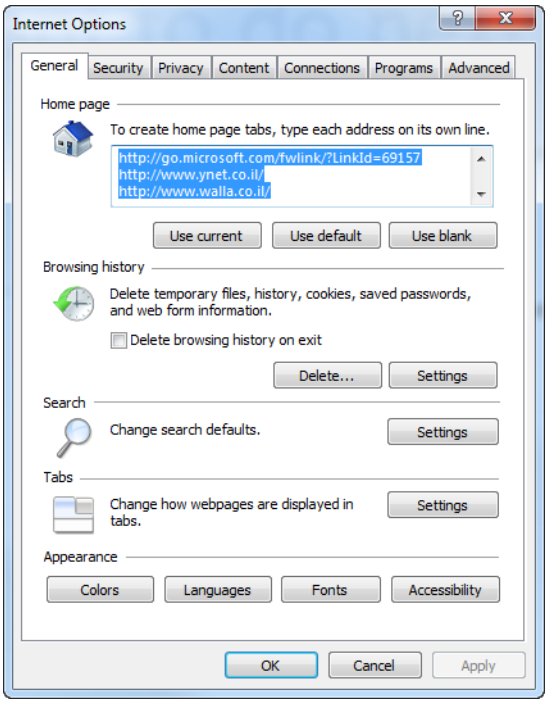
If at the end of Procedure 1 the error message is still displayed, and you cannot connect to the MCU, perform the following operations:

- Delete the Temporary Internet files
- Delete the RMX/Collaboration Server Cookie
- Delete the RMX/RMX ActiveX Object

Deleting the Temporary Internet Files

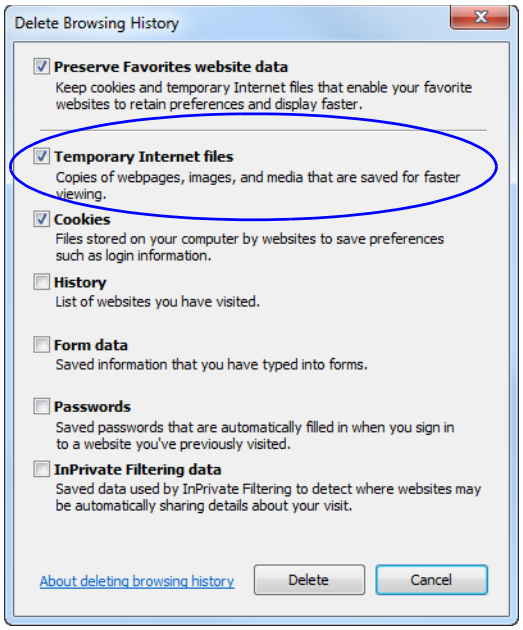
To delete the Temporary files:

1. In the *Internet Explorer*, click **Tools > Internet Options**. The *Internet Options* dialog box opens.
2. In the *Browsing history* pane, click the **Delete** button.



The *Delete Browsing History* dialog box opens.

3 It is recommended to delete only the **Temporary Internet files**.
By default, the **Cookies** option is also selected. Clear it if you do not want to clear the cookies from your computer.



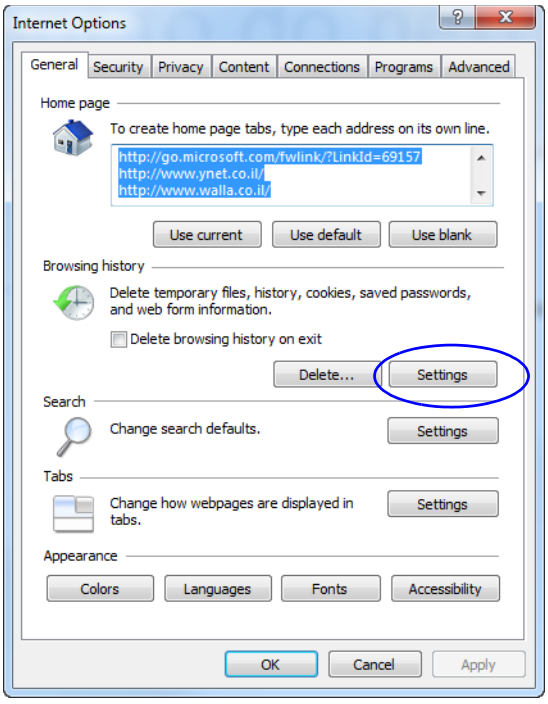
4 Click the **Delete** button.

5 When the process is complete, the system return to the *Internet Options* dialog box.

Deleting the RMX/Collaboration Server Cookie

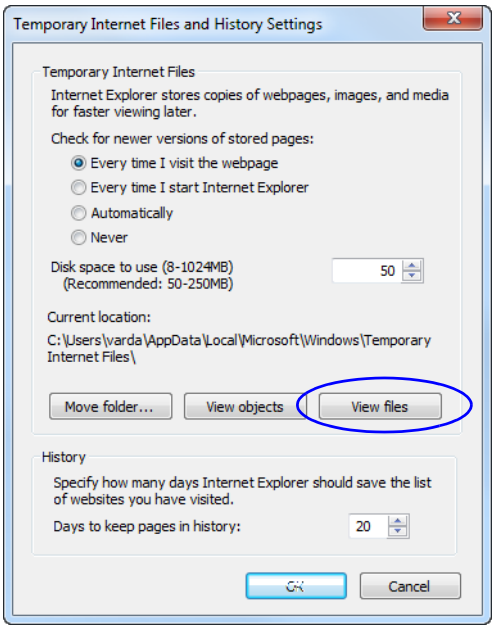
To delete the RMX Cookie:

6 In the *Internet Options* dialog box - *Browsing History* pane, click the **Settings** button.



The *Temporary Internet Files and History Settings* dialog box opens.

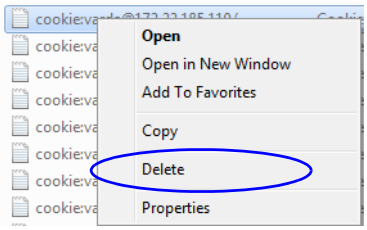
7 Click the **View files** button.



The Windows Explorer screen opens, listing Windows *Temporary Internet Files*.

8 Browse to the RMX/ RMX cookie.
The cookie is listed in the format: **cookie:user name@RMX/RMX IP address**. For example: cookie:valerie@172.22.189.110.

9 Right-click the RMX cookie and click **Delete**.



The system prompts for confirmation.

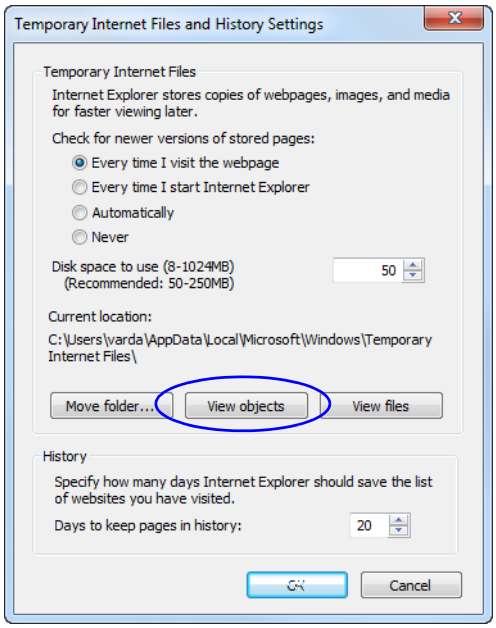
10 Click **Yes**.
The cookie is deleted.

11 Close the Windows Explorer screen.

Deleting the RMX/Collaboration Server ActiveX Object

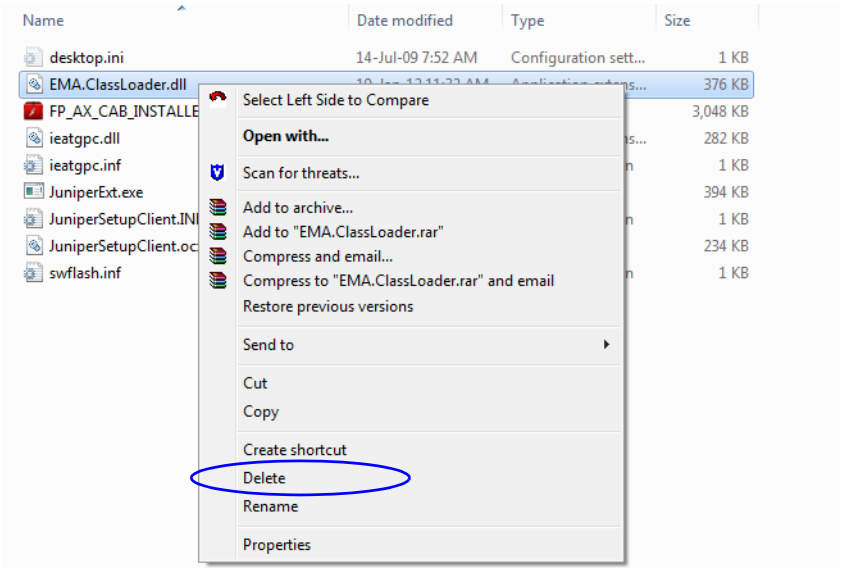
To delete the RMX/RMX ActiveX Object:

12 In the *Temporary Internet Files and History Settings* dialog box, click the **View objects** button.



The Windows Explorer screen opens, listing the Windows *Downloaded Program Files*.

13 Right-click the **EMA.ClassLoader.dll** and then click **Delete**.



The system prompts for confirmation.

14 Click **Yes**.
The RMX object is deleted.

15 Close the Windows Explorer screen.

16 In the *Temporary Internet Files and History Settings* dialog box, click **OK**.

17 In the *Internet Options* dialog box, click **OK** to close it.

18 Close the Internet Explorer session and reopen it.

19 Connect to the RMX.

If the problem persists, continue with Procedure 3.

Procedure 3: Managing Add-ons Collisions

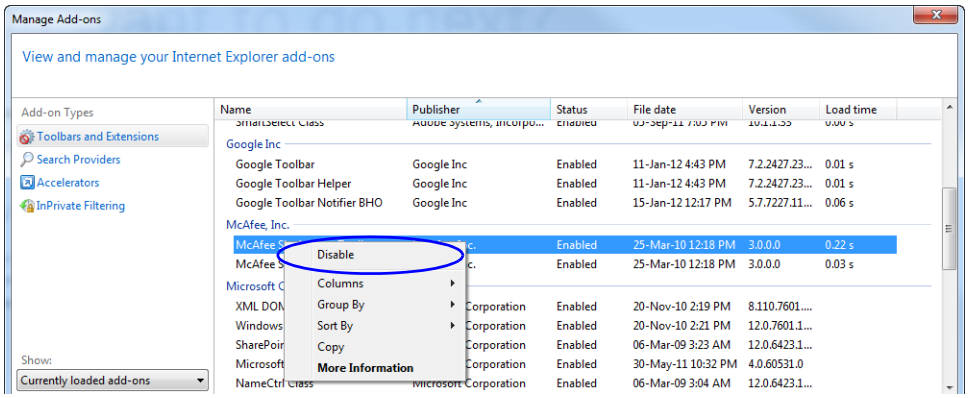
In some cases, previously installed add-ons, such as anti virus programs can create collisions between applications and prevent the installation of a new add on. Disabling these add-ons may be required in order to install the RMX Web Client.

To disable an add-on:

1 In the *Internet Explorer*, click **Tools > Manage Add-ons**.
The *Manage Add-ons - Toolbars and Extensions* dialog box opens.

2 Scroll to the add-on to disable (for example, the anti virus add-on), right-click it and then click **Disable**.

Alternatively, select the add-on and click the **Disable** button.



3 Click the **Close** button to close this dialog box.

4 Connect to the RMX.

If the problem persists, continue with the Procedure 4.

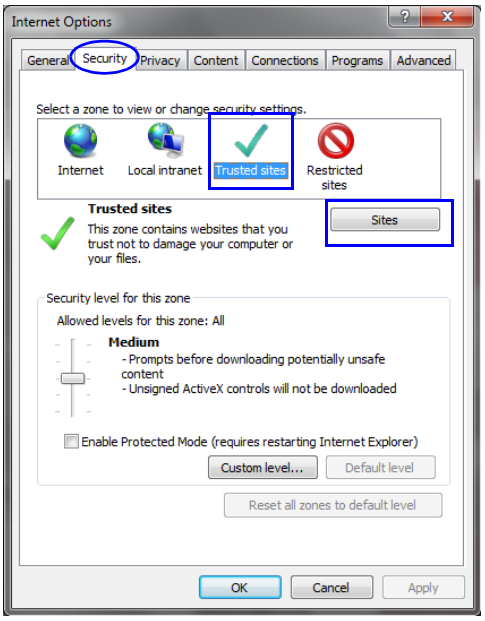
Procedure 4: Add the Collaboration Server to the Internet Explorer Trusted Sites List

In some cases, local security settings may prevent *Internet Explorer* from accessing the RMX.

To add the RMX to the *Internet Explorer* Trusted Sites list:

1 In the *Internet Options* dialog box, click the **Security** tab.

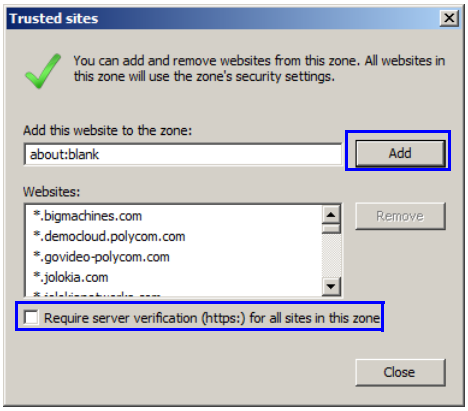
The **Security** tab is displayed.



2 Click the *Trusted Sites* tab.

3 Click the *Sites* button.

The *Trusted sites* dialog is displayed.



4 **If the RMX is using Secure Mode:**

- **a** In the *Add this website to the zone:* field, enter, "https://" followed by the IP address or the DNS name of the RMX.
- **b** Click the **Add** button.
- **c** Click the **Close** button.

5 **If the RMX is using Standard Security Mode:**

- **a** In the *Add this website to the zone:* field, enter, "https://" followed by the IP address or the DNS name of the RMX.
- **b** Click the **Add** button.
- **c** Clear the *Require server verification (https:) for all sites in this zone* checkbox.
- **d** Click the **Close** button.

Procedure 5: Browser Hosting Controls (Optional)

If the *RMX Web Client* does not load and run after *Procedures 1-4* have been performed, the reason may be that *.NET Framework 4* or higher is running on the workstation with *Managed Browser Hosting Controls* disabled.

Managed Browser Hosting Controls is an *Internet Explorer* operating mode required by the *RMX Web Client*. By default, *.NET Framework 4* and higher are not enabled to support *Managed Browser Hosting Controls*.

Perform *Procedure 5* to:

- Determine whether *.NET Framework 4* or higher is running on the workstation.
- Determine whether a *32-bit* or *64-bit* version of *Windows* is running on the workstation.
- Enable *Managed Browser Hosting Controls* if *.NET Framework 4* or higher is running on the workstation.

To enable Managed Browser Hosting Controls:

1. Determine whether *.NET Framework 4* or higher is running on the workstation.
   a. On the *Windows Desktop*, click **Start**.
   b. In the *Start Menu*, click **Control Panel**.
   c. In the *Control Panel*, click **Programs and Features**.
   d. Inspect the **Programs and Features** list for the version of *Microsoft .NET Framework Client Profile* that is installed.
2. Determine whether a *32-bit* or *64-bit* version of *Windows* is running on the workstation:
   a. On the *Windows Desktop*, click **Start**.
   b. In the *Start Menu*, click **Computer**.
   c. In the *Computer Menu*, **System properties** and inspect the value of the *System type* field in the *System* section
3. Enable *Managed Browser Hosting Controls* if *.NET Framework 4* or higher is running on the workstation.
   a. Open the *Registry*.
   b. Navigate to the *Subkey*:
      - **32-bit System:** HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\.NETFramework
      - **64-bit System:** HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
   c. Add the *Dword Value*: *EnableIEHosting*
   d. Set value of *EnableIEHosting* to **1**.
   e. Close the *Registry*.
   f. Close and re-open *Internet Explorer*.