



# Polycom<sup>®</sup> RMX<sup>®</sup> 1500/2000/4000

## Release Notes

#### Trademark Information

Polycom®, the Polycom “Triangles” logo, 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 is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.



This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 7.6.1 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

© 2012 Polycom, Inc. All rights reserved.

Polycom, Inc.  
4750 Willow Road  
Pleasanton, CA 94588-2708  
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

## Regulatory Notices

### United States Federal Communication Commission (FCC)

**Part 15: Class A Statement.** 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. Test 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 manuals, 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 or her own expense.

**Part 68: Network Registration Number.** This equipment is registered with the FCC in accordance with Part 68 of the FCC Rules. This equipment is identified by the FCC registration number.

If requested, the FCC registration Number and REN must be provided to the telephone company.

Any repairs to this equipment must be carried out by Polycom Inc. or our designated agent. This stipulation is required by the FCC and applies during and after the warranty period.

#### United States Safety Construction Details:

- All connections are indoor only.
- Unit is intended for RESTRICTED ACCESS LOCATION.
- Unit is to be installed in accordance with the National Electrical Code.
- The branch circuit overcurrent protection shall be rated 20 A for the AC system.
- This equipment has a maximum operating ambient of 40°C, the ambient temperature in the rack shall not exceed this temperature.

To eliminate the risk of battery explosion, the battery should not be replaced by an incorrect type. Dispose of used batteries according to their instructions.

### CE Mark R&TTE Directive

Polycom Inc., declares that the Polycom RMX™ 2000 is in conformity with the following relevant harmonized standards:

EN 60950-1:2001

EN 55022: 1998+A1:2000+A2:2003 class A

EN 300 386 V1.3.3: 2005

Following the provisions of the Council Directive 1999/CE on radio and telecommunication terminal equipment and the recognition of its conformity.

#### Canadian Department of Communications

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

**Notice:** The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunication network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment malfunctions, may give the telecommunications company causes to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

**Caution:** Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

### RMX 2000: Chinese Communication Certificate

#### 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。

Regulatory Notices
<p><b>Singapore Certificate</b></p> <p>RMX 2000 complies with IDA standards G0916-07</p>



# Table of Contents

<b>Version 7.6.1 - New Features</b>	<b>1</b>
<b>Version 7.6.1 - Changes to Existing Features</b>	<b>2</b>
<b>Version 7.6 - New Features</b>	<b>4</b>
<b>Version 7.6 - Changes to Existing Features</b>	<b>6</b>
<b>Version 7.6.1 - Interoperability Tables</b>	<b>9</b>
Devices	9
Polycom RMX and Avaya Interoperability	12
RMX Web Client	12
Windows 7™ Security Settings	13
Internet Explorer 8 Configuration	14
Polycom Solution Support	17
<b>Version 7.6.1 - Upgrade Package Contents</b>	<b>18</b>
Where to Get the Latest Product Information	18
<b>Upgrade Procedures</b>	<b>19</b>
Guidelines	19
Safe Upgrade Paths to Version 7.6.1	20
Upgrading from Version 7.0.1 / 7.0.2 / 7.0.3 / 7.1 / 7.2 / 7.2.1 / 7.2.2 / 7.5.0J/7.5.1J/ 7.6 to Version 7.6.1	21
Upgrading from Version 7.0 to Version 7.6.1	25
Upgrading from Version 7.0 to Version 7.0.3	25
Upgrade from Version 7.0.3 to Version 7.6.1	25
Upgrading from Version 6.0.2 to Version 7.6.1	26
Intermediate Upgrade from Version 6.0.2 to Version 7.0.3	26
Upgrade from Version 7.0.3 to Version 7.6.1	27
Upgrading from Versions 6.0/6.0.1 to Version 7.6.1	27
Intermediate Upgrade from Version 6.0/6.0.1 to Version 6.0.2	27
Intermediate Upgrade from Version 6.0.2 to Version 7.0.3	28
Upgrade from Version 7.0.3 to Version 7.6.1	28
Upgrading from Version 5.0.2 to Version 7.6.1	29
Intermediate Upgrade from Version 5.0.2 to Version 7.0.3	29
Upgrade from Version 7.0.3 to Version 7.6.1	30
Upgrading from Versions 5.0/5.0.1 to Version 7.6.1	30
Intermediate Upgrade from Version 5.0/5.0.1 to Version 5.0.2	30
Intermediate Upgrade from Version 5.0.2 to Version 7.0.3	31
Upgrade from Version 7.0.3 to Version 7.6.1	32
Upgrading from Version 4.x to Version 7.6.1	32
Intermediate Upgrade from Version 4.x to Version 5.0.2	32
Intermediate Upgrade from Version 5.0.2 to Version 7.0.3	33
Upgrade from Version 7.0.3 to Version 7.6.1	33
Upgrading from Versions 2.x/3.x to Version 7.6.1	33
Intermediate Upgrade From Version 2.x/3.x to Version 4.1.1	33
Intermediate Upgrade from Version 4.1.1 to Version 5.0.2	34

Intermediate Upgrade from Version 5.0.2 to Version 7.0.3 .....	34
Upgrade from Version 7.0.3 to Version 7.6.1 .....	34
Additional/Optional System Updates After Upgrading .....	35
IVR Services Update .....	35
Gathering Settings .....	36
SIP Registration .....	36
Media Encryption .....	38
Upgrading the RMX Manager Application .....	39
<b>Version 7.6.1 Detailed Description - New Features .....</b>	<b>41</b>
Inviting Participants using DTMF Code .....	41
Invite Call Flow .....	41
Entering Additional DTMF Codes .....	41
Error Handling .....	42
Guidelines .....	42
Enabling the Participants using DTMF Option .....	42
Disabling the Invite Participant Option .....	45
H.264 Content Updates .....	46
H.264 Cascade Optimized .....	46
Guidelines .....	47
Enabling H.264 Cascade Optimized Content Sharing .....	47
H.264 HD .....	51
Guidelines .....	51
Enabling H.264 HD Content Sharing for a Conference .....	52
Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD .....	53
Site Names .....	54
Guidelines .....	54
Site Names Display Position .....	55
Enabling, Disabling and Modifying Site Names Display .....	57
w448p Resolution .....	62
Guidelines .....	62
Content .....	63
Lost Packet Recovery .....	63
Enabling Support of the w448p Resolution .....	64
RMX System Flag Settings .....	64
RMX Profile Setting .....	64
Network Traffic Control .....	65
<b>Version 7.6.1 Changes to Existing Features .....</b>	<b>66</b>
Conference IVR Service - Invite Participant .....	66
Fields .....	66
Encryption Changes .....	67
Direct Connection to the Conference .....	68
Connection to the Entry Queue .....	69
Moving from the Entry Queue to Conferences or Between Conference .....	70
Recording Links .....	70
Upgrade Guidelines .....	71
Message Overlay .....	72

Enabling, Disabling and Modifying Message Overlay Display .....	72
Changes to the Message Overlay Properties during an ongoing conference ..	74
Sending Text Messages to Individual or Several Participants .....	75
Controlling Resource Allocations for Lync Clients Using RTV .....	76
Threshold HD Flag Settings using the RTV Video Protocol .....	78
New System Flag - SEND_SRTP_MKI .....	78
<b>Version 7.6 Detailed Description - New Features .....</b>	<b>79</b>
RMX and Cisco Telepresence Systems (CTS) Integration .....	79
Telepresence Interoperability Protocol (TIP) .....	79
Deployment Architectures .....	80
Single Company Model - Polycom and Cisco Infrastructure .....	80
Call Flows .....	82
Multipoint call with DMA .....	82
Multipoint call without DMA .....	83
Company to Company Models Using a Service Provider .....	84
Model 1 .....	85
Call Flow .....	86
Multipoint call via Service Provider - Model 1 .....	86
Model 2 .....	87
Call Flow .....	89
Multipoint call via Service Provider - Model 2 .....	89
Administration .....	90
Gatekeepers .....	90
Standalone Polycom CMA System as a Gatekeeper .....	90
Standalone Cisco IOS Gatekeeper .....	90
Neighbored Cisco IOS and Polycom CMA Gatekeepers .....	90
DMA .....	90
CUCM .....	90
Configuring the Cisco and Polycom Equipment .....	91
Cisco Equipment .....	92
Polycom Equipment .....	92
Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag ..	94
Procedure 2: Configuring RMX to statically route outbound SIP calls to DMA or CUCM .....	94
Procedure 3: Configuring the RMX's H.323 Network Service to register with CMA gatekeeper .....	95
Procedure 4: Configuring a TIP Enabled Profile on the RMX .....	96
Procedure 5: Configuring an Ad Hoc Entry Queue on the RMX if DMA is not used .....	98
Procedure 6: Configuring a Meeting Room on the RMX .....	99
Procedure 7: Configuring Participant Properties for dial out calls .....	99
Operations During Ongoing Conferences .....	100
Monitoring CTS Participants .....	100
SirenLPR .....	102
Guidelines .....	102
SIP Encryption .....	102
Auto Scan and Customized Polling in Video Layout .....	103
Guidelines .....	103

Enabling Auto Scan and Customized Polling .....	103
Auto Scan .....	103
Customized Polling .....	104
Participant Message Overlay .....	106
Guidelines .....	106
Enabling the Participant Message Overlay .....	106
Microsoft Call Admission Control (CAC) Support .....	110
Guidelines .....	110
RMX Configuration for CAC Implementation .....	110
Conferencing Behavior .....	110
Continuous Presence Conferences .....	110
Video Switching Conferences .....	110
Monitoring Participant Connections .....	112
SIP Proxy Failover With Polycom® Distributed Media Application™ (DMA™) 7000 .....	113
Safe Software Version Installation .....	114
Flag Settings .....	115
Safe Software Version Installation Flag Enabled .....	115
Safe Software Version Installation Flag Disabled .....	116
<b>Version 7.6 Detailed Description - New Security Features .....</b>	<b>117</b>
(PKI) Public Key Infrastructure .....	117
Unique Certificates for all Networked Entities .....	117
Offline Certificate Validation .....	118
Peer Certificates .....	118
Self Validation of Certificates .....	118
Certificate Revocation List .....	118
Installing and Using Certificates on the RMX .....	118
Default Management Network .....	119
Enabling Peer Certificate Requests .....	119
Default IP Network Service .....	120
Managing Certificates in the Certification Repository .....	121
Adding Trusted Certificates and CRLs to the Certification Repository .....	122
Trusted Certificates .....	122
Adding Trusted Certificates .....	122
Personal Certificates (Management and Signaling Certificates) .....	125
CRL (Certificate Revocation List) .....	125
Adding a CRL .....	126
Removing a CRL .....	127
Machine Account .....	128
Guidelines .....	128
MS Active Directory Integration .....	130
Directory and Database Options .....	130
Ultra Secure Mode .....	130
Standard Security Mode .....	130
Guidelines .....	131
Enabling Active Directory Integration .....	131
Intrusion Detection .....	133

Network Intrusion Detection System (NIDS) .....	133
Polycom RMX™ Serial Gateway S4GW .....	134
Guidelines .....	134
Configuring the RMX - Serial Gateway Connection .....	136
<b>Version 7.6 Detailed Description - Changes to Existing Features .....</b>	<b>137</b>
H.264 High Profile Support in Video Switched Conferences .....	137
Guidelines .....	137
Enabling H.264 High Profile in VSW Conferences .....	138
System Flags .....	138
IVR Tone Notifications .....	139
Using Tone Notifications .....	139
Play Tone Upon Cascading Link Connection .....	141
Adjust Reservations Start Time .....	142
CDR Additions .....	143
Login Page/Main Page Banners .....	144
Guidelines .....	144
Non-Modifiable Banner Text .....	144
Sample 1 Banner .....	144
Sample 2 Banner .....	145
Sample 3 Banner .....	145
Sample 4 Banner .....	145
User Management .....	146
User Name - Case Sensitivity .....	146
Strong Passwords .....	146
User Passwords .....	146
Maximum Repeating Characters .....	146
Conference and Chairperson Passwords .....	146
USB Restore Defaults .....	147
USB Ports on RMX 1500/2000/4000 .....	147
Restore to Factory Security Defaults .....	148
Comprehensive Restore to Factory Defaults .....	148
Comprehensive Restore to Factory Defaults Procedure .....	149
Procedure A: Backup Configuration Files .....	149
Procedure B: Restore to Factory Defaults .....	150
Procedure C: Restore the System Configuration From the Backup .....	150
Emergency CRL (Certificate Revocation List) Update .....	151
Emergency CRL Update Procedure .....	151
<b>Corrections and Known Limitations .....</b>	<b>155</b>
Corrections Between Version 7.6 and Version 7.6.1 .....	155
Corrections Between Version 7.2.2 and Version 7.6 .....	162
Version 7.6.1 System Limitations .....	178
<b>Troubleshooting Instructions .....</b>	<b>218</b>
Procedure 1: Ending all Internet Explorer Sessions .....	218
Procedure 2: Deleting the Temporary Internet Files, RMX Cookie and RMX Object .....	219
Procedure 3: Managing Add-ons Collisions .....	223



# Version 7.6.1 - New Features



Version 7.6.1 does not support MPM cards. Do not upgrade to Version 7.6.1 if MPM cards are installed in the RMX and contact Support.

The following table lists changes to existing features in Version 7.6.1.

**Table 1-1** Version 7.6.1 - New Features

	Category	Feature Name	Card Configuration Mode	Description
1	Conference	Invite Participant	MPM+/MPMx	A participant in a video or audio conference can invite another participant to the conference using the touch-tone DTMF numeric keypad on the participant's endpoint.
2	Conference	Content Enhancements	MPMx	Enables conference participants to receive higher quality <i>Content</i> in both single level and cascaded conferences.
3	Conference	Site Names	MPMx	The control over the display of <i>Site Names</i> during an ongoing <i>Continuous Presence</i> conference was moved to the <i>Conference Profile</i> level and can also be modified during the ongoing conference.
4	Video	w448 Resolution	MPMx	Improves interoperability with <i>Tandberg MXP 990/3000</i> endpoints providing these endpoints the resolution of <i>W448p</i> (768x448 pixels) at 25fps.
5	IP	Network Traffic Control	MPMx	A Network Traffic Control mechanism has been added to the RMX that controls the level of UDP packets generated by the system.

# Version 7.6.1 - Changes to Existing Features

The following table lists changes to existing features in Version 7.6.1.

**Table 1-2** Version 7.6.1- Changes to Existing Features

	Category	Feature Name	Card Configuration Mode	Description
1	Conference	Invite Participant	MPM+/MPMx	A new pane, <i>Invite Participant</i> , has been included in the <i>New Conference IVR Service</i> and <i>IVR Service Properties</i> dialog boxes.
2	Conference	Content Enhancements	MPMx	The <i>Content Protocol</i> selection, <i>Up to H.264</i> , has been renamed <i>H.263 &amp; H.264 Auto Selection</i> .
3	Conference	Encryption Changes	MPMx	The <code>ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF</code> <i>System Flag</i> is replaced by the <i>Encryption</i> option “ <i>Encrypt When Possible</i> ” in the <i>Conference Profile - Advance</i> dialog box and the <i>Encryption</i> check box has been replaced with a drop-down menu.
4	Conference	Message Overlay	MPMx	The Message Overlay options are added to the Conference Profile. In MPMx Card Configuration Mode, new options were added, providing additional control over the font size, the display position, text color and background color.
5	System Flag	Controlling Resource Allocations for Lync Clients Using RTV	MPM+/MPMx	The system flag <b>MAX_RTV_RESOLUTION</b> enables you to override the RMX resolution selection and limit it to a lower resolution.
6	System Flag	HD Frame Rate Flag Settings using the RTV Video Protocol	MPMx	The system flag <b>MAX_ALLOWED_RTV_HD_FRAME_RATE</b> defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions.
7	System Flag	Encryption	MPM+/MPMx	A new <i>System Flag</i> , <b>SEND_SRTP_MKI</b> , has been added in this version to enable or disable the inclusion of the <i>MKI</i> field in <i>SRTP</i> packets sent by the RMX.



**Table 1-2** Version 7.6.1- Changes to Existing Features (Continued)

	Category	Feature Name	Card Configuration Mode	Description
8	System Flag	Microsoft environment	MPM+/MPMx	<p>The System Flag <b>FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE</b> was added to the system configuration. It is used to force the use of a specific Audio algorithm when a Microsoft Office Communicator R2 or Lync Client is hosted on a workstation with a single core processor. The flag value overrides the default audio algorithm selection (G.722.1) that may cause audio quality problems when G.722.1 is used by Microsoft Clients running on single processor workstations.</p> <p>Possible values: AUTO, G711A, G711U, G722</p> <p>Default: G711A</p>

# Version 7.6 - New Features



Version 7.6 does not support MPM cards. Do not upgrade to Version 7.6 if MPM cards are installed in the RMX and contact Support.

The following table lists changes to existing features in Version 7.6.

**Table 1-3** Version 7.6 - New Features

	Category	Feature Name	Card Configuration Mode	Description
1	Conference	RMX and Cisco Telepresence Systems (CTS) Integration	MPMx	Polycom's solution to allow the RMX to natively inter-operate with Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls between: <ul style="list-style-type: none"> <li>• Polycom Immersive Telepresence Systems,</li> <li>• Polycom video conferencing endpoints</li> <li>• Cisco TelePresence® System (CTS)</li> </ul>
2	Audio	Siren 14 Stereo	MPM+, MPMx	Added support for Siren 14 Stereo. Siren 14 Stereo is supported at line rates between 256Kbps and 4096Kbps. Siren 14 Stereo is supported by HDX endpoints and VSX endpoint (with the exception of VSX 500).
3	Audio	SirenLPR	MPMx	Prevents audio degradation and maintains high audio (CD) quality if packet loss occurs.
4	Video	Auto scan	MPM+, MPMx	<i>Auto Scan</i> enables a user to define a single cell in the conference layout to cycle the display of participants that are not in the conference layout. <i>Customized Polling</i> allows the cyclic display to be set to a predefined order for a predefined time period. The cyclic display only occurs when the number of participants is larger than the number of cells in the layout.
5	Microsoft	Microsoft Call Admission Control (CAC) Support	MPM+, MPMx	A protocol that enables bandwidth management via the Policy Server in federated (ICE) environments.
6	General	Participant Message Overlay	MPM+, MPMx	Participant Message Overlay allows the operator or administrator to send messages to a single participant or a selected number of participants during a conference. <b>Note:</b> In version 7.6.1 this feature description apply only to MPM+ Card Configuration Mode. There are changes and additions to the feature in 7.6.1 MPMx Card Configuration Mode.
7	General	SIP Proxy Failover DMA™ 7000	MPM,MPM+	RMX's that are part of a DMA environment can benefit from DMA's SIP Proxy Failover functionality.

**Table 1-3** Version 7.6 - New Features (Continued)

	Category	Feature Name	Card Configuration Mode	Description
<b>8</b>	General	Safe Software Version Installation	MPM+, MPMx	Ensures that a viable and safe software path is selected during an RMX safe software version installation.
<b>Ultra Secure Mode</b>				
<b>9</b>	Security	PKI (Public Key Infrastructure)	MPM+, MPMx	A set of tools and policies deployed to enhance the security of data communications between networking entities. All networked entities are checked for the presence of unique certificates by implementing the a defined set of rules and procedures during the TLS negotiation.
<b>10</b>	Security	Machine Account	MPM+, MPMx	Allows User names to be associated with servers (machines) and applications such as CMA and DMA to ensure that all users are subject to the same account and password policies.
<b>11</b>	Security	MS Active Directory Integration	MPM+, MPMx	It is possible to configure direct interaction between the RMX and Microsoft Active Directory for Authentication and Authorization of Management Network users.
<b>12</b>	Security	Intrusion Detection (NIDS)	MPM+, MPMx	The RMX system uses iptables for access control. For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the RMX must pass the rules applicable to it.
<b>13</b>	Security	Polycom RMX™ Serial Gateway S4GW	MPM+, MPMx	The Serial Gateway S4GW is connected directly to the RMX effectively becoming an additional module of the RMX, with all web and H.323 traffic passing through the RMX.

# Version 7.6 - Changes to Existing Features

The following table lists changes to existing features in Version 7.6.

**Table 1-4** Version 7.6 - Changes to Existing Features

	Category	Feature Name	Card Configuration Mode	Description
<b>1</b>	Video	High Profile	MPMx	High Profile Video is supported in ISDN calls.
<b>2</b>	Video	H.264 High Profile Support in Video Switched Conferences	MPMx	H.264 High Profile video protocol, previously supported only in Continuous Presence conferences, is now also supported in Switched (VSW) conferences.
<b>3</b>	Video	Minimum frame rate threshold for SD system flag.	MPM+, MPMx	The MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD system flag has been added. It can be used to prevent low quality, low frame rate SD resolution video being sent to endpoints.
<b>4</b>	IVR	IVR Tone Notifications	MPM+, MPMx	Roll Call announcements played upon participants connection or disconnection from a conference (Entry and Exit announcements) can be replaced by tones. The system is shipped with two default tones: Entry Tone and Exit tone.  This option replaces the system flag IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE which was removed from the System Configuration list of flags.
<b>5</b>	General	Play Tone Upon Cascading Link Connection	MPM+, MPMx	The RMX can be configured to play a tone when a cascading link between conferences is established.
<b>6</b>	General	Adjust Reservations Time	MPM+, MPMx	The start time of all the reservations can be manually adjusted in one operation following a change in the MCU time (for example, daylight saving change).
<b>7</b>	General	CDR Additions	MPM+, MPMx	A new event was added (33) to indicate that a connected participant was designated as a Chairperson.

**Table 1-4** Version 7.6 - Changes to Existing Features (Continued)

	Category	Feature Name	Card Configuration Mode	Description
8	General	Site Names Location	MPM+, MPMx	<p>A new flag SITE_NAMES_LOCATION was added to the system configuration.</p> <p>This flag enables you to define the position of the site name on the endpoint screen.</p> <p>Possible flag values:</p> <ul style="list-style-type: none"> <li>• DOWN_CENTER (Default)</li> <li>• DOWN_LEFT</li> <li>• DOWN_RIGHT</li> <li>• UP_CENTER</li> <li>• UP_LEFT</li> <li>• UP_RIGHT</li> <li>• AUTO</li> </ul> <p>When set to AUTO, configuration is according to the default system behavior.</p> <p><b>Note:</b> In version 7.6.1 this flags apply only to MPM+ Card Configuration Mode.</p> <p>In MPMx Card Configuration Mode, this flag is replaced by options in the new Profile - Site Names dialog box.</p>
9	General	Hide Site Names	MPM+, MPMx	<p>The system flag HIDE_SITE_NAMES is replaced by the option Site Names in the Conference Properties - Video Settings dialog box. It allows you to enable or disable the display of site names in conferences per conference.</p> <p>This option is unavailable in VSW conferences.</p> <p><b>Note:</b> In version 7.6.1 this flags apply only to MPM+ Card Configuration Mode.</p> <p>In MPMx Card Configuration Mode, this flags is replaced by options in the new Profile - Message Overlay dialog box.</p>
10	General	Participant Connection Monitoring	MPM+, MPMx	<p>The Participants list header displays two numbers in the format (n/m):</p> <ul style="list-style-type: none"> <li>• Currently Connected participants (n) - both defined and undefined participants currently connected to the conference.</li> <li>• Total - Connected and Expected to Connect (m) - Total number of participants known to take part in the conference. It includes all participants currently connected and Defined participants that are expected to connect to the conference.</li> </ul>
11	General	Multiple Networks	MPM+, MPMx	<p>Up to eight media and signaling networks can be defined for RMX 4000, or four for RMX 2000 and two for RMX 1500. Multiple IP Network Services can be defined, up to two for each media and signaling network connected to the RMX. The networks can be connected to one or several Media cards in the RMX unit.</p>

**Table 1-4** Version 7.6 - Changes to Existing Features (Continued)

	Category	Feature Name	Card Configuration Mode	Description
12	General	BFCP Content	MPM+, MPMx	The default value of the <code>ENABLE_SIP_PPC_FOR_ALL_USER_AGENT</code> <i>system Flag</i> has been changed to YES.
13	General	SIP Server UPDATE message	MPM+, MPMx	The <code>MS_UPDATE_CONTACT_REMOVE</code> <i>System Flag</i> allows the <i>Contact Header</i> to be removed from or included with the <i>UPDATE</i> message that is sent periodically to <i>SIP</i> endpoints.
<b>Ultra Secure Mode</b>				
1	Security	System Flag name	MPM+, MPMx	The <code>JITC_MODE</code> flag has been renamed to <code>ULTRA_SECURE_MODE</code> .
2	Security	Security mode name	MPM+, MPMx	JITC Mode has been renamed Ultra Secure Mode.
3	Security	Login Page / Main Page Banners	MPM+, MPMx	The administrator can select a Login Banner from a drop-down menu containing four non-modifiable banners and one custom banner.
4	Security	Strong Passwords	MPM+, MPMx	Password management now includes definition of Maximum Repeating Characters for Conference and Chairperson Passwords. <b>Note:</b> Chairperson users are not supported in Ultra Secure Mode.
5	Security	USB Restore to Default	MPM+, MPMx	The USB port of an RMX in Ultra Secure Mode can be used to: <ul style="list-style-type: none"> <li>Restore the RMX to Factory Security Defaults mode (https -&gt; http).</li> <li>Perform a Comprehensive Restore to Factory Defaults</li> <li>Perform an Emergency CRL Update Procedure</li> </ul>

# Version 7.6.1 - Interoperability Tables

## Devices

The following table lists the devices with which Version 7.6.1 was tested..

**Table 1-5** Version 7.6.1 Device Interoperability Table

Device	Version
<b>Gatekeepers/Proxies</b>	
<i>Polycom Netgear WGR614 (VBP AP and H460)</i>	v10 1.0.2.26_51.0.59NA
<i>Polycom VBP5300 E/ST</i>	11.2.x
<i>Polycom CMA</i>	6.0.x
<i>Polycom PathNavigator</i>	7.0.14
<i>Polycom SE200</i>	3.0.7.
<i>Polycom RMX S4 Gateway</i>	5.5.7.83-00601(B10)
<i>Cisco 3241 Gateway</i>	2.1(1.43)p
<i>Cisco 3745 Gatekeeper</i>	12.4
<i>Cisco (Tandberg) VCS</i>	X6.1
<i>Cisco (Tandberg) gateway</i>	G3.2
<i>Cisco (Tandberg) gatekeeper</i>	N6.1
<i>Radvision ECS gatekeeper</i>	7.1.2.12
<i>Radvision Scopia P10 Gateway</i>	5.7.2.0.25
<i>Microsoft OCS Server</i>	2007 R2 3.5.6907
<i>Microsoft Lync Server</i>	4.0.7577.0
<i>Broadsoft Proxy</i>	BroadWorks release R17 SP2
<b>Recorder</b>	
<i>Polycom RSS 2000</i>	4.0
<i>Polycom RSS 4000</i>	7.0
<b>MCUs, Call Managers Network Devices and Add ins</b>	
<i>Polycom MGC 25/50/100 and MGC+50/100</i>	8.0.2 and 9.0.4
<i>Polycom RMX 1000</i>	2.1.x
<i>Polycom DMA 7000</i>	4.0.x

**Table 1-5** Version 7.6.1 Device Interoperability Table (Continued)

Device	Version
<i>Polycom RMX Conferencing Add in for Microsoft Outlook</i>	1.0.7
<i>Avaya Communication MGR</i>	6.0.1.: 00.1.510.1, with video service pack # 19543
<i>Avaya Aura Session Manager</i>	R6.1 SP6 (616009)
<i>Avaya Aura Communication Manager as Evolution Server</i>	R6.0.1
<i>Cisco Call Manager</i>	8.5.1
<i>Cisco (Tandberg) Codian 4505 MCU</i>	4.1(1.50)
<i>Polycom RMX Conferencing Add-in for IBM Sametime</i>	V2.0.4
<i>IBM Sametime Server</i>	8.5.2_20110517
<i>Siemens Server</i>	V5.00.01.ALL.11_PS0017.E04
<b>Endpoints</b>	
<i>Polycom HDX Family</i>	3.0.3.1
<i>Polycom Telepresence (ITP) Systems</i>	3.0.3.1
<i>Polycom VSX and V-Series Family</i>	9.0.6.2
<i>Polycom Viewstation Family</i>	7.5.4 or higher
<i>Polycom Viewstation FX/EX</i>	6.0.5 or higher
<i>Polycom CMA Desktop</i>	5.2.2
<i>Polycom CMA Desktop for MAC</i>	5.2.2 or higher
<i>Polycom QDX6000</i>	4.0.2
<i>Polycom m500</i>	1.1
<i>Polycom m100</i>	1.0
<i>Polycom VVX1500</i>	4.0.1
<i>SoundPointIP 650</i>	4.0.1
<i>Polycom PVX</i>	8.0.16
<i>Polycom iPower 9000</i>	6.2
<i>Polycom Soundstation IP4000 SIP</i>	3.1.4
<i>Polycom DST B5</i>	2.0
<i>Polycom DST K60</i>	2.0.1
<i>Polycom DST K80</i>	4.0.2
<i>Avaya IP Softphone</i>	R6.0.1
<i>Avaya one-X Communicator</i>	6.1 SP3 (6.1.3.06_35509)



**Table 1-5** Version 7.6.1 Device Interoperability Table (Continued)

Device	Version
<i>Avaya 1000 series endpoint</i>	4.8.3(21)
<i>Avaya Desktop Video endpoint</i>	1.1 (A175_1_1_0_012003)
<i>LifeSize 200</i>	4.7.19
<i>LifeSize Room and Express</i>	4.7.19
<i>LifeSize Desktop Client</i>	2.0.2
<i>LifeSize Express 220</i>	4.8.6
<i>LifeSize Team 220</i>	4.8.6
<i>LifeSize Passport</i>	4.8.6
<i>Cisco (Tandberg) 150 MXP</i>	L6.1
<i>Cisco (Tandberg) 6000 B</i>	B10.3
<i>Cisco (Tandberg) 6000 E</i>	E5.3
<i>Cisco (Tandberg) EX90</i>	4.2.1
<i>Cisco (Tandberg) C Family</i>	4.2.1
<i>Cisco (Tandberg) MXP F-Family</i>	F9.1
<i>Cisco E20</i>	4.2.1
<i>Cisco CTS3010 (Telepresence)</i>	1.7.0.2/1.7.4
<i>Cisco CTS1300 (Telepresence)</i>	1.7.0.2/1.7.4
<i>Radvision SCOPIA XT1000 endpoint</i>	2.0
<i>Microsoft OC client R2</i>	3.5.6907.244
<i>Microsoft Lync client</i>	v4.0.7577.0
<i>IBM Sametime Client</i>	ST8.5.2_20110516
<i>Siemens Client</i>	V6 R0.2.7 (60.0.2.0007)
<i>Siemens OpenStage Desktop Voice</i>	V2_R2_37_0
<i>Vidyo Desktop client</i>	2.0.4



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.

The Polycom RMX 2000/4000 series of MCUs running software version 7.0.1.16 register to current generally available versions of Avaya Aura Session Manager R6.0 to provide multipoint video calls.

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 1-6** Version 7.0 Environment Interoperability Table

Web Browser	Operating System
Internet Explorer 6	Windows XP™
Internet Explorer 7	Windows XP™
	Windows Vista™
	Windows 7
Internet Explorer 8	Windows 7



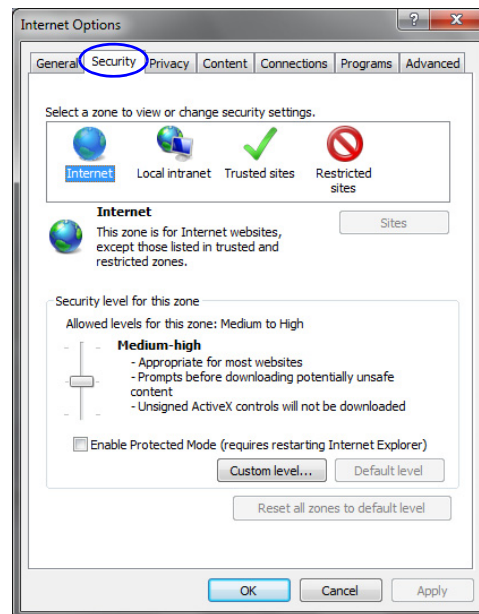
*It is not recommended to run RMX Web Client and Polycom CMAD applications simultaneously on the same workstation.*

## Windows 7™ Security Settings

If *Windows 7* is installed on the workstation, *Protected Mode* must be disabled before downloading the Version 7.6.x software to the workstation.

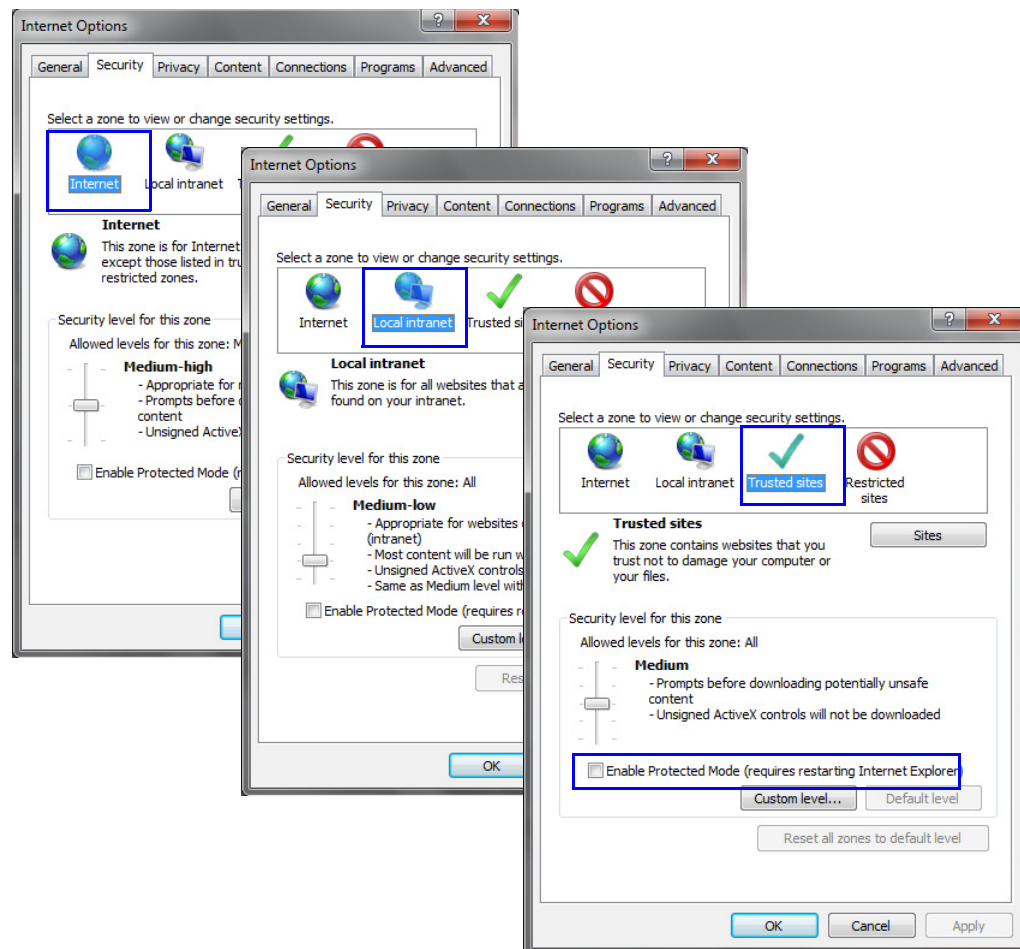
### To disable Protected Mode:

- 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*

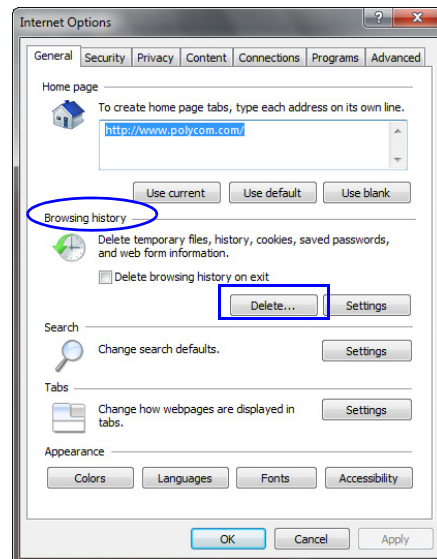
## Internet Explorer 8 Configuration

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

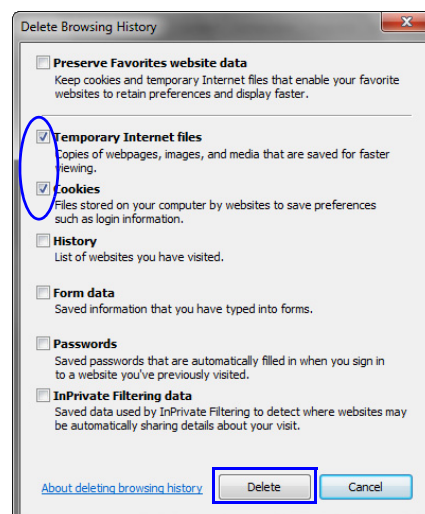
**To configure Internet Explorer 8:**

- 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 *RMX*.
- 4 In the *Internet Explorer* menu bar select **Tools >> Internet Options**.  
The *Internet Options* dialog box is displayed with *General* tab open.

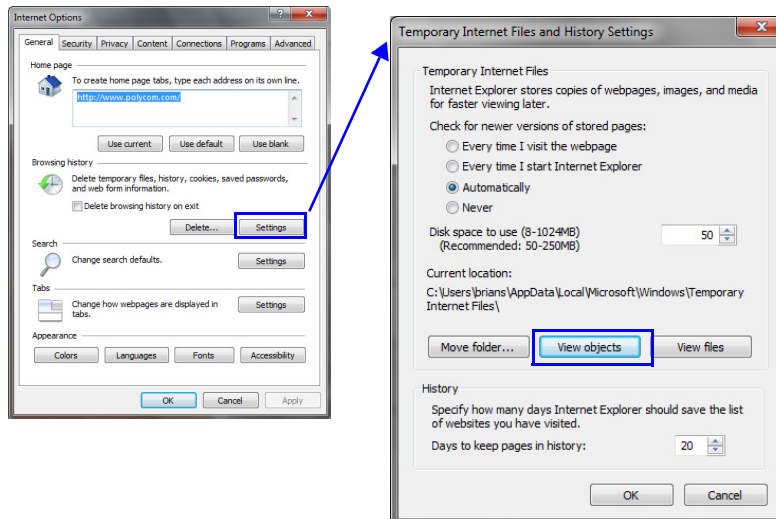


- 5 In the *Browsing history* section, click the **Delete** button.  
The *Delete Browsing History* dialog box is displayed.



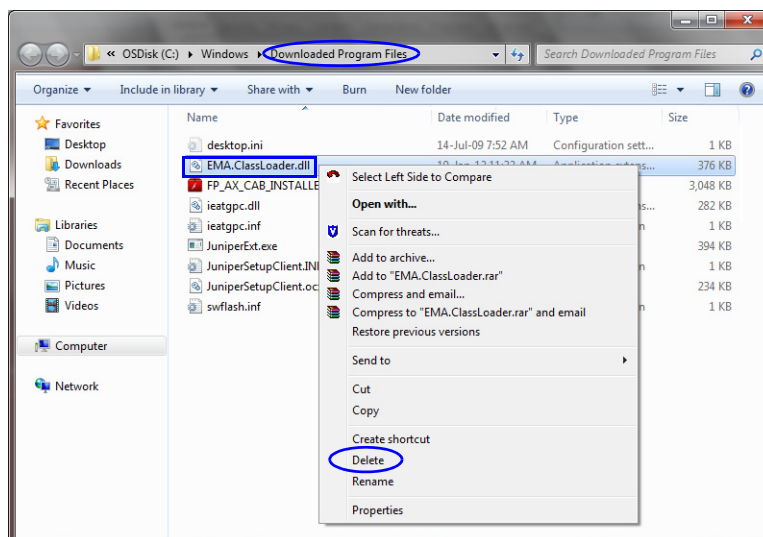
- 6 Select the **Temporary Internet** files and **Cookies** check boxes.
- 7 Click the **Delete** button.
- 8 The *Delete Browsing History* dialog box closes and the files are deleted.
- 9 In the *Internet Options* dialog box, click the **Settings** button.

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](http://www.polycom.com/services/professional_services/index.html) or contact your local Polycom representative.

# Version 7.6.1 - Upgrade Package Contents

The Version 7.6.1 upgrade package must be downloaded from the *Polycom Resource Center* and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Documentation
  - RMX 1500/2000/4000 Version 7.6.1 Release Notes
  - RMX 1500/2000/4000 Getting Started Guide
  - RMX 1500/2000/4000 Administrator's Guide
  - RMX 1500/2000/4000 Hardware Guide
  - RMX 1500/2000/4000 Quick Installation Booklet
  - 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 7.6.1
  - RMX 1500/2000/4000 XML API Version 7.6 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
- Translations of RMX 1500/2000/4000 Version 7.6 Documentation:
  - Getting Started Guide:  
French, German, Japanese, Russian, Simplified Chinese, Hebrew and Portuguese
  - Hardware Guide:  
French, German, Japanese, Korean, Russian, Simplified Chinese, Spanish

## 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

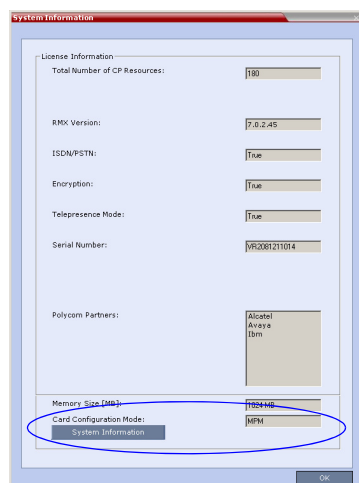


- **Version 7.6.1 does not support MPM cards. DO NOT** upgrade to Version 7.6.1 if *MPM* cards are installed in the RMX and contact *Polycom Support*.
- If the upgrade process includes upgrading the *Media* cards, refer to the *RMX 2000/4000 MPMx Migration Procedure* documentation.

## 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*.

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



- If *Windows 7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the RMX software to the workstation. For more information see "*Windows 7™ Security Settings*" on page **1-13**.
- 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.
- If an upgrade procedure fails contact *Polycom Support*.
- 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 **35**.
- To enable the *Gathering Phase* in the existing Profiles, you must modify the Profiles assigned to the conferencing entities. For more details, see "*Gathering Settings*" on page **36**.

- 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 entities. For more details, see “SIP Registration” on page 36.

## Safe Upgrade Paths to Version 7.6.1

A safety mechanism has been added to RMX to ensure that a viable and safe software version installation is selected on an RMX. It ensures that the current RMX software version and the new software installation are matched to an internal logic table, and enables or rejects the software installation. When an incorrect or non-viable version upgrade/downgrade path is attempted, an alarm and fault are activated on the RMX.

The following table shows a list of the software versions that are supported with the Safe Upgrade process for version 7.6.1.

**Table 1-7** RMX Version Software Version Upgrade/Downgrade Support for version 7.6.1

Software Version	1500X	1500Q	RMX 2000 MPM	RMX 2000 MPM+/MPMx	RMX 4000 MPM+/MPMx
2.x	-	-	-	-	-
3.x	-	-	-	-	-
4.x	-	-	-	-	-
4.7.2	✓	-	-	✓	✓
5.x	-	-	-	-	-
6.x	-	-	-	-	-
7.0	-	-	-	-	-
7.0.x/7.0.2C	✓	-	-	✓	✓
7.1	✓	✓	-	✓	✓
7.2/7.2.x	✓	✓	-	✓	✓
7.5.0J/7.5.1J	✓	-	-	✓	✓
7.6/7.6.1	✓	✓	-	✓	✓

To disable this mechanism change the default setting of the ENFORCE\_SAFE\_UPGRADE system flag to NO.

If your RMX version is not listed in Table 1-7, refer to Table 1-8 for intermediate and safe upgrade paths to version 7.6.1.

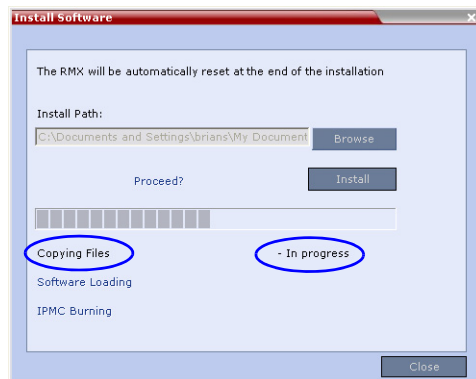
**Table 1-8** Upgrade Paths to Version 7.6.1

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		Third Intermediate Upgrade		New Version	
	Version	Key	Version	Key	Version	Key	Version	Key
7.6	N/A		N/A		N/A		<b>7.6.1</b>	No
7.5.0J/7.5.1J	N/A		N/A		N/A		<b>7.6.1</b>	Yes
7.2 / 7.2.1 / 7.2.2	N/A		N/A		N/A		<b>7.6.1</b>	Yes
7.0.1 / 7.0.2 / 7.0.3 / 7.1	N/A		N/A		N/A		<b>7.6.1</b>	Yes
7.0	7.0.3	No	N/A		N/A		<b>7.6.1</b>	Yes
6.0.2	7.0.3	Yes	N/A		N/A		<b>7.6.1</b>	Yes
6.0 / 6.0.1	6.0.2	No	7.0.3	Yes	N/A		<b>7.6.1</b>	Yes
5.0.2	7.0.3	Yes	N/A		N/A		<b>7.6.1</b>	Yes
5.0 / 5.0.1	5.0.2	No	7.0.3	Yes	N/A		<b>7.6.1</b>	Yes
4.x	5.0.2	Yes	7.0.3	Yes	N/A		<b>7.6.1</b>	Yes
2.x / 3.x	4.1.1	Yes	5.0.2	Yes	7.0.3	Yes	<b>7.6.1</b>	Yes

## Upgrading from Version 7.0.1 / 7.0.2 / 7.0.3 / 7.1 / 7.2 / 7.2.1 / 7.2.2 / 7.5.0J/7.5.1J/7.6 to Version 7.6.1

- 1 Download the Version 7.6.1 software from the *Polycom Resource Center* web site.
- 2 Obtain the Version 7.6.1 *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the RMX Getting Started Guide, "Obtaining the Activation Key" on page 2-25.
- 3 Backup the configuration file. For more information, see the RMX 1500/2000/4000 *Administrator's Guide*, "Software Management" on page 20-48.
- 4 Install MCU Software Version 7.6.1.  
On the RMX menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 7.6.1.x.x.bin** file in the folder where Version 7.6.1 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.

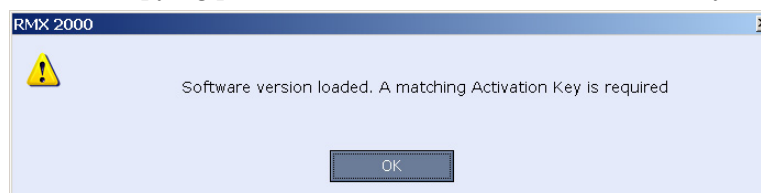


Click **OK**. The RMX software installation procedure is aborted and a system alert activates in the Faults List as shown below.

Faults List (126)							
ID	Time	GMT	Category	Level	Code	Process Name	Description
126	11	01	Assert	Major	Software assert failure	Installer	File:ManagerTask ASSERT:Upgrade_rejected_Updating_from_7.6.0.138_to_7.0.0.164_is_not_supported
125	11	01	General	Major	Invalid conference setting	ConfParty	ISDN protocol cannot be selected for dial-out in the gateway Profile because ISDN Network Service is no
124	11	01	General	Major	SSH is enabled	McuMgr	SSH is enabled
123	11	01	General	Startu	System is starting	McuMgr	RMX Version : 7.6.0.138, MCU Build Version : RMX_7.6.0.138
122	11	01	General	Syste	Invalid System Configurat	McuMgr	Flag does not exist: CHECK_ARPING
121	11	01	Assert	Major	Software assert failure	McuMgr	File:SysConfigBase.cpp, Line:575, Code:1.; ASSERT:Flag_does_not_exist:_IPV4_RESPONSE_ECHO
120	11	01	Assert	Major	Software assert failure	McuMgr	File:SysConfigBase.cpp, Line:575, Code:1.; ASSERT:Flag_does_not_exist:_IVR_ROLL_CALL_USE_TONE

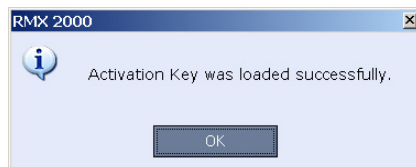
- During any upgrade or downgrade software version installation when the *Safe Software Version Installation* warning has been activated your current browser session will block any new installation attempt. This applies to all software versions, except for version 7.6 which will still enable version downgrades. 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.



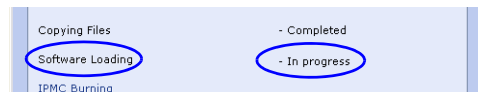
- Click the **OK** button.  
The *Product Activation* dialog box is displayed with the serial number field completed.
- In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

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.

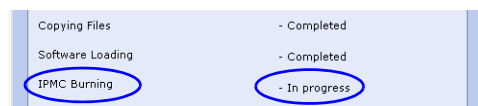
The *Install Software* information box indicates that *Software Loading* is in progress.



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

Active Alarms (6)								
ID	Time	GMT Tim	Category	Level	Code	Process Name	Description	
8	Wed	Wednes	General	System	IPMC software upgrade	Installer	IPMC upgrade 95%	
7	Wed	Wednes	General	System	IPMC software upgrade	Cards	RTM IP IPMC upgrade 84% board Id:5	
6	Wed	Wednes	General	System	IPMC software upgrade	Cards	Media card IPMC software upgrade 80% board	
3	Wed	Wednes	General	System	Warning: Upgrade start	Installer	Warning: Upgrade started and SAFE Upgrade	

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.

Active Alarms (6)								
ID	Time	GMT Tim	Category	Level	Code	Process Name	Description	
7	Wed	Wednes	General	System	IPMC software upgrade	Cards	RTM IP IPMC upgrade 0% board Id:5	
6	Wed	Wednes	General	System	IPMC software upgrade	Cards	Media card IPMC software upgrade 0% board	
3	Wed	Wednes	General	System	IPMC software upgrade	Cards	Media card IPMC software upgrade 0% board	

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

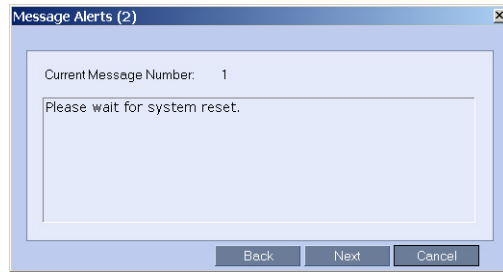


Sometimes, when updating the *Version 7.6.1* license key, the system displays the following active alarm:

Active Alarms (1)								
MCU	ID	Time	Category	Level	Code	Process Name	Description	
172.22.185.145	2	11:57:15 2010	General	Major	Insufficient resources	Resource	Insufficient resources	

Ignore this Active Alarm and complete this installation procedure.

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



Connection to the RMX 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 RMX.  
If the browser displays a message indicating that it cannot display the requested page, close and reopen the browser and connect to the RMX.  
The version number in the *Welcome* screen has changed to 7.6.1.
- 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 RMX. If the error message appears again, either run the automatic troubleshooter utility or manually preform the suggested troubleshooting procedures. For more details, see “*Troubleshooting Instructions*” on page 218.

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

**Starting up (15:25)** showing the time remaining until the system start-up is complete.

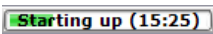
To use the new features such as *Operator Assistance* and *Gateway Sessions* the IVR Services must be updated. For more details, see “*Additional/Optional System Updates After Upgrading*” on page 35.

The upgrade to Version 7.6.1 is complete.

## Upgrading from Version 7.0 to Version 7.6.1

This upgrade requires an intermediate upgrade from *Version 7.0* to *Version 7.0.3*.

### Upgrading from Version 7.0 to Version 7.0.3

- 1 Download the *Version 7.0.3* software from the *Polycom Resource Center* web site
- 2 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page **20-48**.
- 3 Install MCU Software *Version 7.0.3*.  
On the RMX menu, click **Administration > Software Management > Software Download**.
- 4 Browse to the *Install Path*, selecting the **Version 7.0.3.x.bin** file in the folder where *Version 7.0.3* is saved and click **Install**.  
The *Install Software* information box indicates that *Copying Files* is *In progress*.  
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.  
Connection to the RMX is terminated and you are prompted to reopen the browser.
- 5 Approximately 5 minutes after receiving this message, close and reopen the browser.
- 6 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to RMX.  
If the browser displays a message indicating that it cannot display the requested page close and re-open the browser and connect to the RMX.  
The version number in the *Welcome* screen has changed to 7.0.3.
- 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.

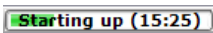
### Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

## Upgrading from Version 6.0.2 to Version 7.6.1

This upgrade requires an intermediate upgrade from *Version 6.0.2* to *Version 7.0.3*.

### Intermediate Upgrade from Version 6.0.2 to Version 7.0.3

- 1 Download the *Version 7.0.3* software from the *Polycom Resource Center* web site.
- 2 Obtain the *Version 7.0.3 Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Started Guide*, "Modifying the Factory Default Management Network Settings on the USB Key" on page 2-7.
- 3 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page 20-48.
- 4 Install MCU Software Version 7.0.3.  
On the RMX menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 7.0.3.x.bin** file in the folder where *Version 7.0.3* is saved and click **Install**.  
  
The *Install Software* information box that *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.  
  
After about 30 minutes, **close and reopen the browser** and connect to the RMX.  
If the browser was not closed and reopened, the following error message is displayed: *Browser environment error. Please reopen the browser*. If this occurs, close and re-open the browser and connect to the RMX.  
  
The version number in the *Welcome* screen has changed to 7.0.3.
- 10 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.



## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

## Upgrading from Versions 6.0/6.0.1 to Version 7.6.1

This upgrade requires the following intermediate upgrade procedures:

- 1 Upgrade from *Version 6.0./6.0.1* to *Version 6.0.2*.
- 2 Upgrade from *Version 6.0.2* to *Version 7.0.3*.

### Intermediate Upgrade from Version 6.0/6.0.1 to Version 6.0.2

- 1 Download the Version 6.0.2 software from the *Polycom Resource Center* web site
- 2 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page **20-48**.
- 3 Install MCU Software Version 6.0.2.  
On the RMX menu, click **Administration > Software Management > Software Download**.
- 4 Browse to the *Install Path*, selecting the Version 6.0.2.x.bin file in the folder where Version 6.0.2 is saved and click **Install**.

The *Install Software* information box that *Copying Files* is *In progress*.

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.

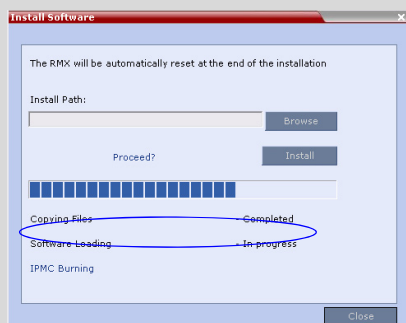
The *Install Software* information box indicates that *IPMC Burning* is *In progress*.

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

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



When upgrading from version 6.0.1, if after 20 minutes the system remains in the *Loading Software* stage:



and sometimes the following Active Alarm is displayed:

Faults Full List (1000)						
ID	Time	Category	Level	Code	Process	Description
1627	26-10-2010 17:37:49	Assert	Major	Softwar	Installer	File:InstallerManager.cpp,Line:996,Code:1.; ASSERT:Timeout_reached_during_installation_flow
1626	26-10-2010 17:14:56	Assert	Major	Softwar	McuMng	File:McuMngManager.cpp,Line:947,Code:1.; ASSERT:CMcuMngManager::OnAuthenticationInd_
1625	26-10-2010 17:14:56	General	Major	Socket r	MplApi	Socket reconnect (board id: 5)

Close the Install Software window, access the **Hardware Monitor** and **Reset** the RMX.

After reset, the upgrade process continues as described below.

Connection to the RMX is terminated and you are prompted to reopen the browser.

- 5 After approximately 5 minutes close and reopen the browser.
- 6 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to RMX.

If the browser displays a message indicating that it cannot display the requested page close and re-open the browser and connect to the RMX.

The *Login* screen is displayed. The version number has changed to 6.0.2.

- 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

**Starting up (15:25)**

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

## Intermediate Upgrade from Version 6.0.2 to Version 7.0.3

- >> Continue with the upgrade from *Version 6.0.2* to *Version 7.0.3* as described starting on page 26.

## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

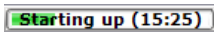
# Upgrading from Version 5.0.2 to Version 7.6.1

This upgrade requires an intermediate upgrade from *Version 5.0.2* to *Version 7.0.3*.

## Intermediate Upgrade from Version 5.0.2 to Version 7.0.3

- 1 Download the software Version 7.0.3 software from the *Polycom Resource Center* web site.
- 2 Obtain the Version 7.0.3 *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Started Guide*, "Procedure 1: First-time Power-up" on page 2-24.
- 3 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page 20-48.
- 4 Install MCU Software Version 7.0.3.  
On the RMX menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 7.0.3.x.bin** file in the folder where **Version 7.0.3** 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 2000/4000 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 RMX, click **Yes** to reset the RMX.
- 9 When prompted to wait while the RMX resets, click **OK**.  
  
The upgrade procedure takes approximately 30 minutes.  
Connection to the RMX 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 RMX.  
  
If the browser displays a message indicating that it cannot display the requested page, refresh the browser periodically until connection to the RMX is established and the *Login* screen is displayed.  
  
You may receive a message stating *Browser environment error. Please reopen the browser*. If this occurs, close and re-open the browser and connect to the RMX.
- 12 **Optional.** Close and reopen the browser.
- 13 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to RMX.  
  
The *Login* screen is displayed. The version number has changed to 7.0.3.
- 14 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.

## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

## Upgrading from Versions 5.0/5.0.1 to Version 7.6.1

This upgrade requires the following intermediate upgrade procedures:

- 1 Upgrade from *Version 5.0./5.0.1* to *Version 5.0.2*.
- 2 Upgrade from *Version 5.0.2* to *Version 7.0.3*.

### Intermediate Upgrade from Version 5.0/5.0.1 to Version 5.0.2

- 1 Download the required software *Version 5.0.2* from the *Polycom Resource Center* web site
- 2 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page **20-48**.
- 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 5.0.2.x.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.

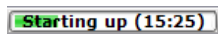
The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP*.

- 7 After about **30** minutes, **close and reopen the browser** and connect to the RMX.  
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 7.0.3

- 1 Download the software Version 7.0.3 software from the *Polycom Resource Center* web site.
- 2 Obtain the Version 7.03 *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Started Guide*, "Obtaining the Activation Key" on page 2-25.
- 3 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page 20-48.
- 4 Install *MCU Software* Version 7.0.3.  
On the *RMX* menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 7.0.3.x.bin** file in the folder where **Version 7.0.3** 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 2000/4000* 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 *RMX*, click **Yes** to reset the *RMX*.



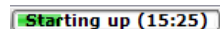
Sometimes when upgrading from version 5.0.2 to version 7.0.x the reset process fails. In such a case, you can try to connect to the *MCU* via the Shelf Management and reset the *MCU* from the Hardware Monitor or you can "hard" reset the *MCU* by turning the Power off and on again.

- 9 When prompted to wait while the *RMX* resets, click **OK**.  
The upgrade procedure takes approximately 30 minutes.  
Connection to the *RMX* 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 *RMX*.  
The browser displays a message indicating that it cannot display the requested page.
- 12 Refresh the browser periodically until connection to the *RMX* 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 *RMX*.

The *Login* screen is displayed. The version number has changed to 7.0.3.

- 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

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

## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

## Upgrading from Version 4.x to Version 7.6.1

This upgrade requires the following intermediate upgrade procedures:

- 1 Upgrade from *Version 4.x* to *Version 5.0.2*.
- 2 Upgrade from *Version 5.0.2* to *Version 7.0.3*.

## Intermediate Upgrade from Version 4.x to Version 5.0.2

- 1 Download the *Version 5.0.2* software from the *Polycom Resource Center* web site.
- 2 Obtain the *Version 5.0.2 Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Stated Guide*, "Obtaining the Activation Key" on page 2-25.
- 3 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page 20-48.
- 4 Install *MCU Software Version 5.0.2*  
On the *RMX* menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 5.0.2.x.bin** file in the folder where the downloaded version 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.
- 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 Click the **OK** button.
- 9 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 RMX 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*.



Sometimes when upgrading from version 4.x to version 5.0.2 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.

After about **30 minutes**, **close and reopen the browser** and connect to the RMX. If the browser was not closed and reopened, the following error message is displayed: *Browser environment error. Please reopen the browser.* If this occurs, close and re-open the browser and connect to the RMX.

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

- 10** 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

**Starting up (15:25)** showing the time remaining until the system start-up is complete

## Intermediate Upgrade from Version 5.0.2 to Version 7.0.3

- >> Continue with the upgrade from *Version 5.0.2* to *Version 7.0.3* as described starting on page 29.

## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.

## Upgrading from Versions 2.x/3.x to Version 7.6.1

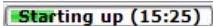
From *Versions 2.x/3.x*, the upgrade to *Version 7.6.1* requires three intermediate upgrades:

- 1** Intermediate upgrade to *Version 4.1.1*.
- 2** Intermediate upgrade from *Version 4.1.1* to *Version 5.0.2*.
- 3** Intermediate upgrade from *Version 5.0.2* to *Version 7.0.3*.

## Intermediate Upgrade From Version 2.x/3.x to Version 4.1.1

- 1** Download the *Version 4.1.1* software from the *Polycom Resource Center* web site.
- 2** Obtain the *Version 4.1.1 Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Stated Guide*, “*Obtaining the Activation Key*” on page **2-25**.
- 3** Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator’s Guide*, “*Software Management*” on page **20-48**.
- 4** Install *MCU Software Version 4.1.1*  
On the *RMX* menu, click **Administration > Software Management > Software Download**.



- 5 Browse to the *Install Path*, selecting the **Version 4.1.1.x.bin** file in the folder where *Version 4.1.1* 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.
- 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 Click the **OK** button.
- 9 When prompted whether to reset the *MCU*, click **Yes** to reset the *MCU*.  
The upgrade procedure may take up to 30 minutes during which time an *Active Alarm - System Upgrade* is displayed.  
The RMX 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*.
- 10 After 30 minutes, close and re-open the browser and connect to the RMX.  
The version number in the *Welcome* screen has changed to 4.1.1
- 11 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 4.1.1 to Version 5.0.2

- >> Continue with the upgrade from *Version 4.x* to *Version 5.0.2* as described starting on page 32.

## Intermediate Upgrade from Version 5.0.2 to Version 7.0.3

- >> Continue with the upgrade from *Version 5.0.2* to *Version 7.0.3* as described starting on page 29.

## Upgrade from Version 7.0.3 to Version 7.6.1

- >> Continue with the upgrade from 7.0.1 / 7.0.2 / 7.0.3 / 7.1/7.2 / 7.2.1 / 7.2.2 to Version 7.6 as described on page 21.



# Additional/Optional System Updates After Upgrading

## IVR Services Update

When upgrading from version 4.0 and earlier, *Operator Assistance* and the *Gateway calls* options require that the IVR Services include specific (new) DTMF Codes and voice messages. These additions are not automatically added to existing IVR Services in order to avoid conflicts with existing DTMF codes. Therefore, to use these options, new Conference and Entry Queue IVR Services must be created.

In **Version 6.0**, recording can be controlled from the HDX remote control using the designated recording buttons. This is enabled by changing the existing definitions of the DTMF codes of the Roll Call and Recording actions in the Conference IVR Services already defined in the RMX.

In **Version 7.x**, PCM for ISDN participants is enabled by a DTMF code. The code must be added to the *DTMF Codes* tab to enable the PCM for ISDN participants. Default value is 1.

In **Version 7.6.1**, a participant can invite another participant to the conference using a DTMF code. This code must be added manually to the existing Conference IVR Services. In addition, the *Invite Participant* voice message requesting the participant to enter the destination number must be selected in the *General* tab.

### 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 1-9** DTMF Code Changes

Action	Existing DTMF Code	New DTMF Code
<i>Enable Roll Call</i>	*32	*42
<i>Disable Roll Call</i>	#32	#42
<i>Roll Call Review Names</i>	*33	*43
<i>Roll Call Stop Review</i>	#33	#43
<i>Start/Resume Recording</i>	*73	*3
<i>Stop Recording</i>	*74	*2
<i>Pause Recording</i>	*75	*1
<i>Request Private Assistance</i>		*0
<i>Request Assistance for the conference</i>		00
<i>PCM (for ISDN participants only)</i>		##
<i>Invite Participant</i>		*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 *RMX 2000 Administrator's Guide*, "Defining a New Conference IVR Service" on page 16-7.

## Gathering Settings

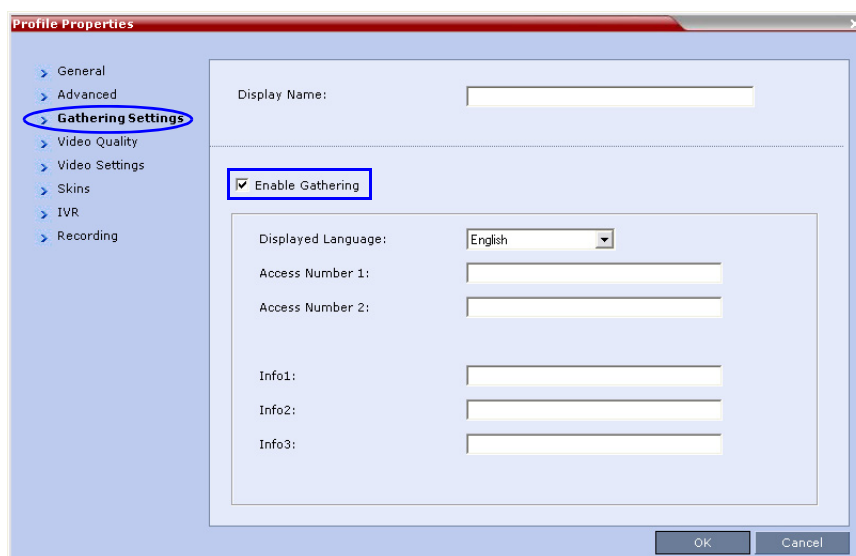
When upgrading from earlier versions, the *Enable Gathering* check box in the *Profile Properties - Gathering Settings* dialog box is not selected by default for existing *Profiles*.

**To set Enable Gathering as default:**

- 1 In the *RMX Management* pane, click *Conference Profiles*.
- 2 In the *Conference Profiles* pane, double-click the **Profile** or right-click the *Profile*, and then click **Profile Properties**.

The *Profile Properties - General* dialog box opens.

- 3 Click **Gathering Settings**.



- 4 Select the **Enable Gathering** check box.
- 5 Click the **OK** Button.

For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Gathering Phase" on page 3-23.

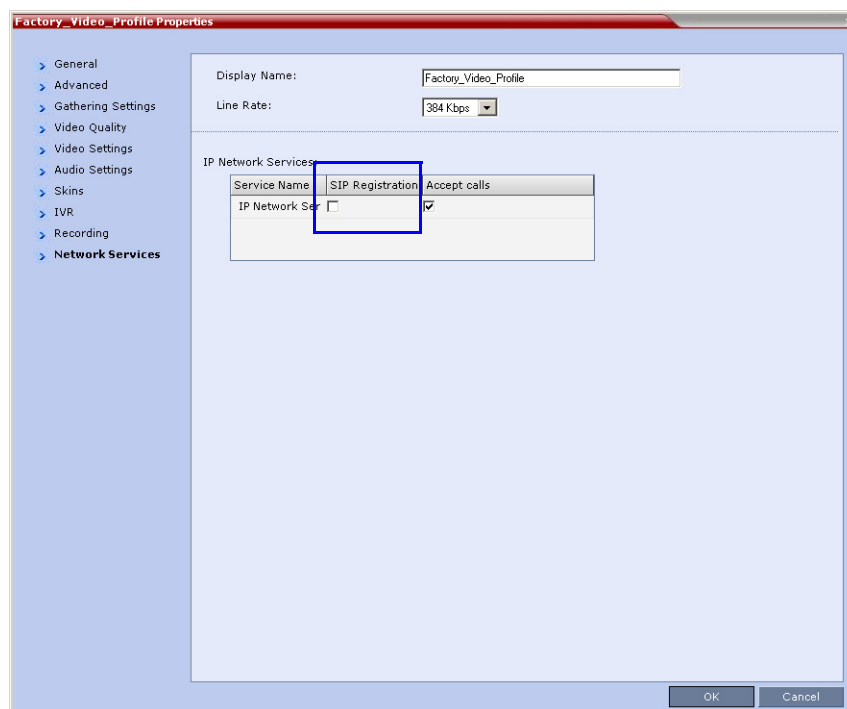
## SIP Registration

Starting with Version 7.1, enabling the registration of the conferencing entities with the SIP proxy is moved from the *IP Network Service* to the *Conference Profile - Network Services*. To ensure that conferencing entities that were registered with the SIP Server remain registered after upgrading to Version 7.6.1, the appropriate conference *Profile* must be updated accordingly.

**To enable the registration with the SIP Server:**

- 1** Verify which Profile is used by conferencing entities you wish to register with the SIP Server.
- 2** List the **Conference Profiles**.
- 3** Display the *Profile Properties* by double-clicking it or right-clicking the Profile and then selecting **Properties**.  
The Profile Properties - General dialog box opens.
- 4** Click the **Network Services** tab.

The *Profile - Network Services* dialog box is displayed.



The system lists the *IP Network Services* currently defined in the RMX system depending on the system configuration (single Network or Multiple Networks).

- 5** In the *SIP Registration* column, click the check box of the *Network Service* to enable the registration of the conferencing entity to which this profile is assigned with the SIP Server defined in that Network Service.
- 6** To prevent dial in participants from connecting to a conferencing entity when connecting via a certain Network Service, clear the *Accept Calls* check box of that Network Service.
- 7** Click OK.

## 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 the encryption requirements through the new encryption options according to Table 2.

**Table 2** 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	<b>YES</b>	Profile Encryption Setting	<b>Encrypt All</b>
Profile Encryption Setting	<b>NO</b>	Profile Encryption Setting	<b>No Encryption</b>
System Flag	<b>ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF=YES</b>	Profile Encryption Setting	<b>Encrypt when possible</b>

## Upgrading the RMX Manager Application

The RMX Manager application can be downloaded from one of the RMX systems installed in your site or from Polycom web site at <http://www.polycom.com/support>.

**To install RMX Manager (downloading the application from the RMX):**



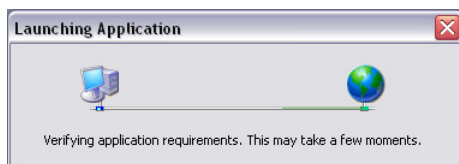
- When upgrading the RMX Manager application, it is recommended to backup the MCU list using the **Export RMX Manager Configuration** option. For more details, see *RMX 1500/2000/4000 Administrator's Guide*, "Software Management" on page **20-48**.
- When upgrading the RMX Manager from a major version (for example, version 7.0) to a maintenance version of that version (for example, 7.x), the installation must be performed from the same MCU (IP address) from which the major version (for example, version 7.0) was installed.  
If you are upgrading from another MCU (different IP address), you must first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs**.

- 1 Start Internet Explorer and connect to the RMX unit from which the current version was installed.

The *Login* screen is displayed.

- 2 Click the **Install RMX Manager** link on the upper right corner of the *Login* screen.

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



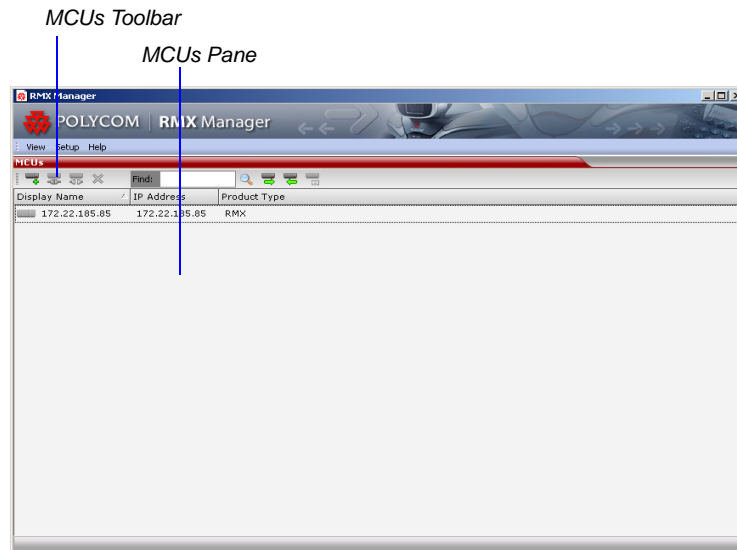
If the following error message is displayed, you are upgrading from an MCU that other than the one used for the installed version (different IP address). In such a case, first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs**.



The *Install* dialog box is displayed.

- 3 Click the **Install** button.  
The installation proceeds.

The installation completes, the application loads and the *RMX Manager - MCUs* screen is displayed.



The list includes the previously defined MCUs.



If the MCUs list is empty, import the backed up list using the **Import RMX Manager Configuration** option. For more details, see *RMX 1500/2000/4000 Administrator's Guide "Import/Export RMX Manager Configuration"* on page [19-23](#).

# Version 7.6.1 Detailed Description - New Features

## Inviting Participants using DTMF Code

A participant in a video or audio conference can invite another participant to the conference using the touch-tone DTMF numeric keypad on the participant's endpoint. You can invite a participant using various communication devices, such as a mobile phone, an IP phone, PSTN phones, laptops, or connect to another conference running on another PBX or MCU.

### Invite Call Flow

The following flow describes how a participant is invited to the conference using the DTMF codes:

- 1 During the conference, the participant enters the DTMF code (default is \*72) on the numeric keypad to invite another participant.
- 2 The participant is prompted to enter the invited participant's destination number (a number or IP address) including the prefix (if required) and the DTMF delimiter digit ('\*' or '#') at the end. The asterisk (\*) is used to denote the dot in the IP address.

For example: To enter an IP address such as 10.245.22.19, on the DTMF keypad press 10\*245\*22\*19 and then the DTMF delimiter.



Digits that are entered after the DTMF delimiter and before the participant is connected are ignored.

- 3 The system automatically dials to the destination according to the protocol order as defined in the *IVR Services Properties - Video Services* tab.

When the call cannot be completed by the current protocol, the system attempts to connect to the destination using the next protocol according to the protocol order.

The RMX connects the participant when the call is answered.

### Entering Additional DTMF Codes

In some environments, the call is answered by an IVR system (for example when connecting to another conference or PBX), requesting a password or a destination number to complete the connection process. In such a case, additional DTMF digits must be entered before the **DTMF forward duration** time has expired and are forwarded to the invited destination. When the additional DTMF codes are entered, they are heard by all the conference participants.

If the DTMF code is not entered on time or if the wrong DTMF code is entered, the participant is prompted for a new input. After the defined number of retries have elapsed, the call is ended.

## Error Handling

- If the destination endpoint is busy or the participant did not answer, the system ends the call.
- When an incorrect number is entered, the call fails and an error message is displayed.
- If the destination number is not entered in a specific amount of time (defined in **Timeout for user input** in the *IVR Services - Global* tab), the participant is prompted to enter a destination number again. Depending on the **Number of user input retries** as defined in the *IVR Services - Global* tab, the system will attempt to receive the required input. When all the retries have failed, the call to the invited participant is cancelled.

## Guidelines

- Participants can be invited to CP and VSW conferences.
- All network protocols are supported (H.323, SIP, ISDN, and PSTN). It is recommended to select PSTN and not ISDN if PSTN is the only destination protocol. If both PSTN and ISDN are enabled, it is recommended to select the PSTN before ISDN as the connection process for PSTN endpoints will be quicker.
- In an Multiple IP Networks environment, the system will try to connect the participant using each of the IP Network Services listed in the *Conference Profile - Network Services* dialog box. Network services that are excluded from this list are skipped during the dialing sequence.
- In CP conferences, the participant initiating the invitation to another participant is able to view the dialing information and connection status. During the dialing process, the dialing string is displayed as the participant name which is replaced by the site name when connected to the conference.
- By default, all participants (Everyone) are granted permission to invite a participant to join a conference. To change the permission to the Chairperson, modify the *Permission* column in the *IVR Service - DTMF Codes* tab.

## Enabling the Participants using DTMF Option

The option to invite participants to a conference using the DTMF keypad is enabled in the following *Conference IVR Services* dialog boxes:

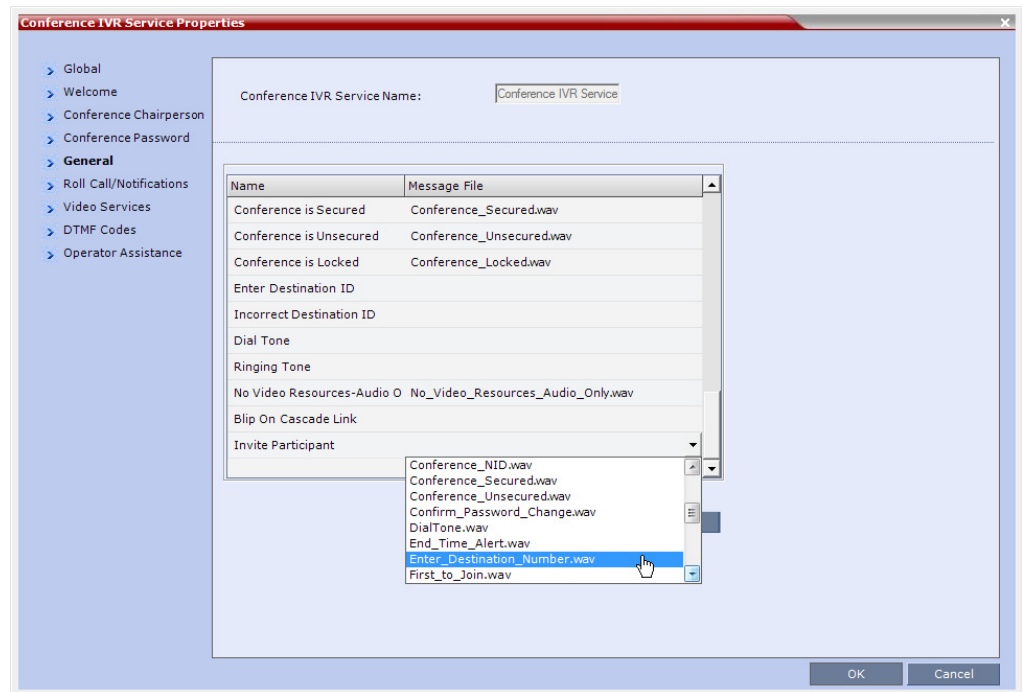
- *General*
- *Video Services*
- *DTMF Codes*

**To enable the Invite Participant using DTMF on the RMX:**

- 1 Open an existing or define a new *Conference IVR Service*.  
*Conference IVR Service - Global* dialog box opens.
- 2 Click the **General** tab.

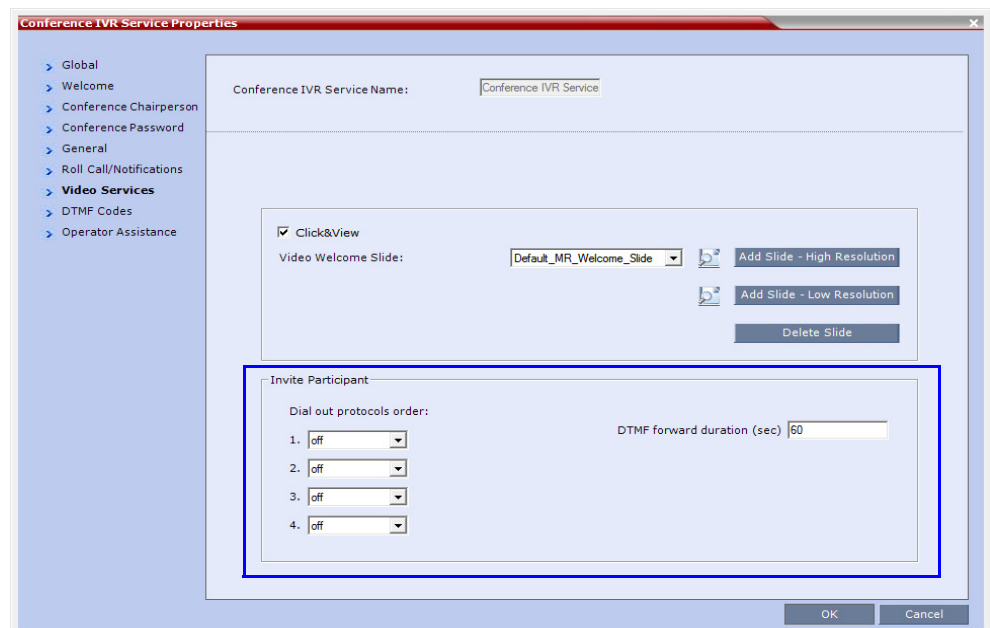


The *Conference IVR Services - General* tab is displayed.



- 3 In the Message File column of the **Invite Participant** entry, click the drop-down arrow and select the required voice message. The file **Enter\_Destination\_Number.wav** that is shipped with the system can be used for this message. To upload a new file, click the **Add Message File**. For more details, see the *RMX 1500/2000/4000 Administrator's Guide*, "Creating Audio Prompts and Video Slides" on page 16-29.
- 4 Click the **Video Services** tab.

The *IVR Services - Video Services* tab is displayed.



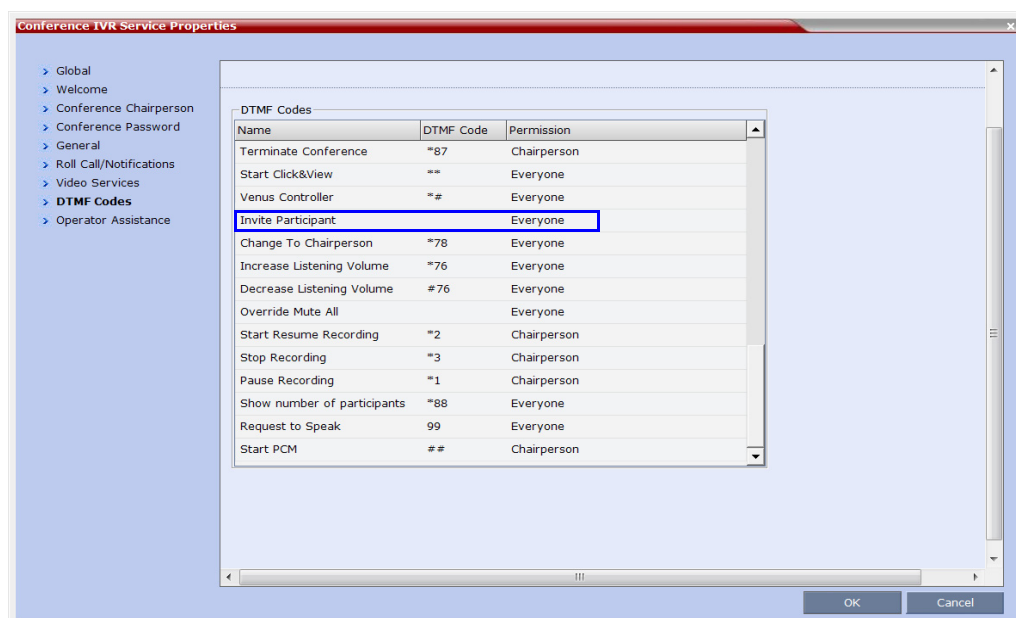
- 5 Define the following parameters:

**Table 1-1** IVR Services Properties - Video Services Parameters - Invite Participants

Video Services	Description
<i>Dial out protocols order</i>	<p>Select the order of the network protocols that will be used by the system to dial the destination number. The system will start dialing using the first protocol, and if the call is not answered it will continue with the second, third and fourth protocols (if they are enabled) until the call is answered. By default, H.323 is set as the first protocol and SIP as the second while the remaining protocols are disabled (set to Off).</p> <p>For PSTN calls, select the PSTN protocol and not ISDN.</p> <p>Set PSTN before ISDN if both PSTN and ISDN protocols are required.</p>
<i>DTMF forward duration</i>	<p>Use this field when connecting to another conferencing entity with an IVR, requiring the input of a password, destination number or ID. Enter the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number. The range can be from 10 seconds to 600 seconds. Default is 60 seconds.</p>

- 6 Click the **DTMF Codes** tab.

The *IVR Services - DTMF Codes* tab is displayed.



- 7 Ensure that *Invite Participant* has DTMF Code **\*72** assigned to it. Although **\*72** is the default and recommended DTMF Code for *Invite Participant*, it may still have to be assigned if the system was upgraded from a previous version.
- 8 If required, determine who can invite other participants to the conference using DTMF codes by changing the permissions to either **Chairperson** or **Everyone**.
- 9 Click **OK**.

## Disabling the Invite Participant Option

**To disable the Invite Participant option:**

- 1** From the *IVR Services - DTMF Codes* tab, delete the DTMF digits from the **DTMF Code** column.
- 2** Click **OK**.

## H.264 Content Updates

Additional options for sharing *Content Protocols* have been included in this version, enabling conference participants to share higher quality *Content* in both standard and cascaded conferences.

The following *Content Protocols* options are supported:

- **H.263**
  - *Content* is shared using the *H.263* protocol.
  - This option is used when most of the endpoints support *H.263* and some endpoints support *H.264*.
- **H.263 & H.264 Auto Selection** (in version 7.6 and earlier, it was named *Up to H.264* )
  - The default selection
  - *Content* is shared using *H.263* if a mix of *H.263*-supporting and *H.264*-supporting endpoints are connected.
  - *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
  - If the first endpoint to connect to the conference only supports *H.263*, the *H.263* protocol is used for *Content* for all conference participants.
  - If *Content* is already being shared using the *H.264* protocol when a *H.263* endpoint connects, *Content* sharing is stopped and must be manually restarted using *H.263*, for all participants. If the *H.263* endpoint disconnects, *Content* sharing must be manually stopped and restarted and will automatically upgrade to the *H.264* protocol.
  - Endpoints that do not have at least *H.263* capability can connect to the conference but cannot share *Content*.
- **H.264 Cascade Optimized** (new in Version 7.6.1)
  - When this option is selected, all content is shared using the *H.264* content protocol and is optimized for use in cascaded conferences.
- **H.264 HD** (new in Version 7.6.1)
  - This option ensures high quality content when most endpoints support *H.264* and *HD Resolutions*.

## H.264 Cascade Optimized

In versions prior to *Version 7.6.1*, *Content* could be sent over the cascading link only in *H.263* protocol. From *Version 7.6.1* *Content* can be sent over a cascading link using *H.264*.

However, to maintain the content quality and minimize the amount of *Content* refreshes that occur in large cascading conferences when participants connect or disconnect from the conference, the *H.264 Cascade Optimized* option uses fixed *Line Rates*, *Content Settings* and *Content Resolutions*.

Endpoints that do not support the required *Content* parameters (*Content* line rate, *H.264* protocol and *Content Resolution*), along with *ISDN* endpoints, can be connected as *Legacy Endpoints* and receive content through their video channel. This ensures that *Content* settings are not changed following the participants connection or disconnection from the conference. If the *Send Content to Legacy Endpoints* option is disabled, these endpoints will not receive content.

## Guidelines

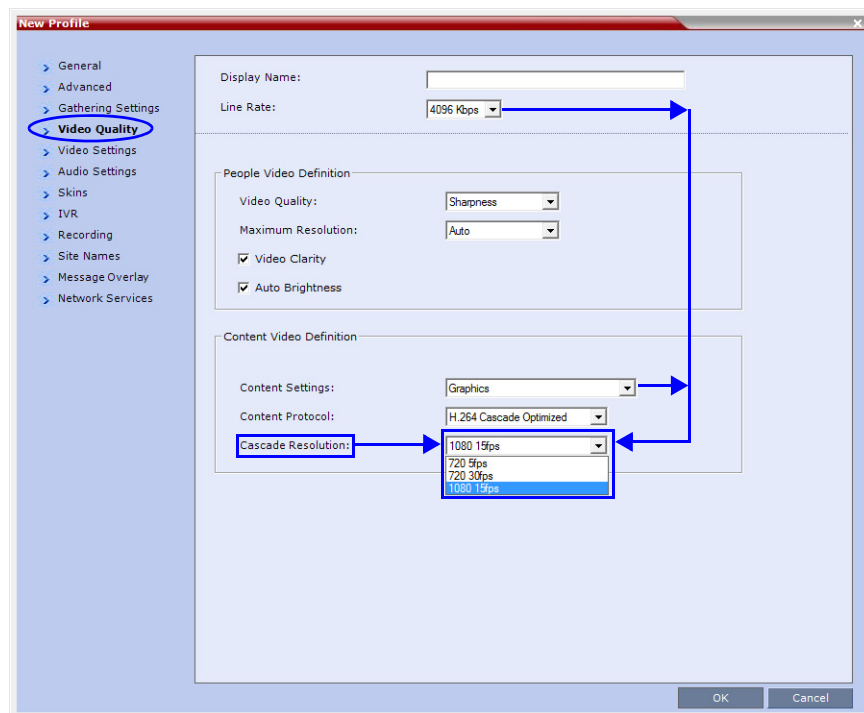
- The cascade link must be *H.323*.
- *H.323*, *SIP* and *ISDN* participants are supported.
- *H.264 High Profile* is not supported.
- In *MPM+ Card Configuration Mode*, maximum supported content resolution is HD 720p.
- When *H.264 Cascade Optimized* is selected, the *Send Content to Legacy Endpoints* selection is enabled by default in the *Conference Profile – Video Settings* dialog box.
- Endpoints that cannot connect at a line rate required to support the conference Content Rate are considered *Legacy Endpoints* and will receive Content in the video channel.

## Enabling H.264 Cascade Optimized Content Sharing

*H.264 Cascade Optimized* content sharing is selected in the *New Profile – Video Quality* dialog box.

When *H.264 Cascade Optimized* is selected as the *Content Protocol*, an additional field is displayed in the *Content Video Definition* pane enabling the user to select the *Cascade Resolution*.

The *Cascade Resolution* is a fixed resolution and frame rate for *Content* sharing in a Cascaded Conference. The *Cascade Resolutions* that are available for selection are dependent on the *Line Rate* and *Content Settings* that have been selected for the conference.



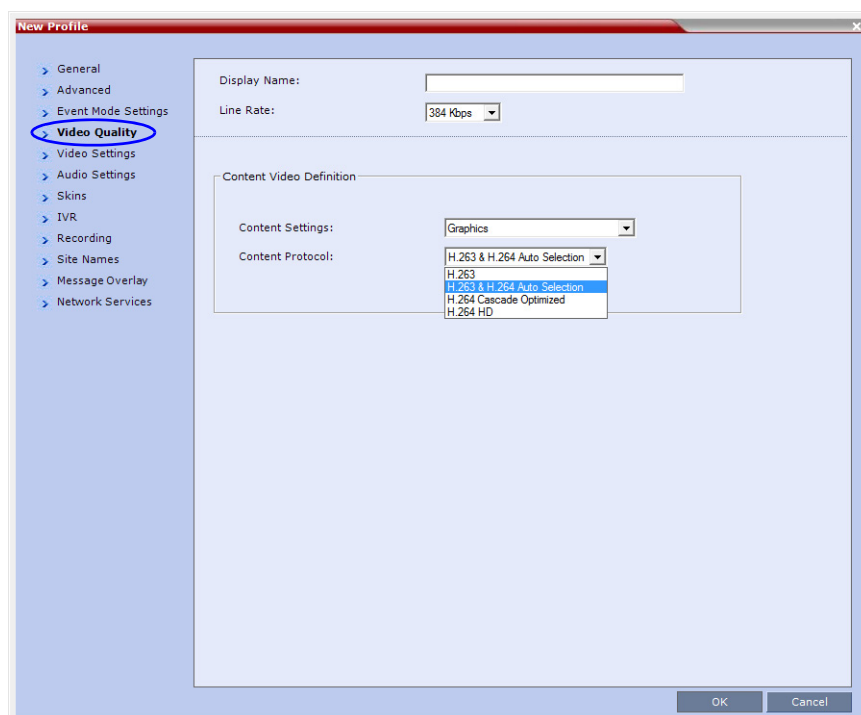


Table 1-2

summarizes the interaction of these parameters.

**Table 1-2** Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Cascade Resolution

Content Settings	Cascade Resolution/fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Graphics	HD720/5		64	128	128	256	256	256	512	512
	HD720/30							512	512	512
	HD1080/15						768	768	1152	1152
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The selection of the appropriate *Content Resolution* option, when several options are available, should be based on the line rate and capabilities that can be used by most or all endpoints connecting to the conference.

**Examples:**

- If the conference *Line Rate* is **1024 kbps**.  
and
- If the *Content Settings* selection is **Graphics**.
  - **Cascade Resolutions of HD720/5 and HD1080/15** are selectable with **256Kbps** and **768Kbps** allocated as the *Conference Content Rate* respectively.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Graphics	HD720/5		64	128	128	256	256	256	512	512
	HD720/30							512	512	512
	HD1080/15						768	768	1152	1152

The higher *Cascade Resolution*, **HD1080/15** should be selected only if most of the endpoints connecting to the conference can support a *Content Rate* of 768Kbps, which requires the participant to connect to the conference at a *Line Rate* of 1024kbps.

When the lower *Cascade Resolution* **HD720/5** is selected, the conference *Content Rate* is set to 256Kbps. This will enable the endpoints that connect to the conference at a *Line Rate* of at least 768Kbps to receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 768Kbps, will receive content in the video channel.

- If the *Content Settings* selection is **Hi Resolution Graphics**.
  - Only **HD720/5** can be selected as the *Cascade Resolution* with **384kbps** allocated as the conference *Content Rate*.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152

Only endpoints that connect at a *Line Rate* of 1024Kbps that is required to support a *Content Rate* of 384Kbps will receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 1024Kbps, will receive content in the video channel.

- If the *Content Settings* selection is **Live Video**.
  - **HD720/5, HD720/30 or HD1080/15** can be selected as the *Cascade Resolution* with **768Kbps** allocated the as the *Conference Content Rate*.

Content Settings	Cascade Resolution/fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The higher *Cascade Resolution* should be selected according to the resolution capabilities of the majority of the endpoints connecting to the conference. Endpoints that cannot support the selected *Cascade Resolution* are considered *Legacy Endpoints* and will receive *Content* in the video channel.



## H.264 HD

Bit rate allocation to the *Content* channel by the RMX is dynamic according to the conference line rate and Content Settings. Endpoints must however connect at *Content* rates above a minimum as specified by specific *System Flags* to ensure high quality *Content* for all participants. For more information about *System Flags* see “*Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD*” on page 53.

Endpoints that do not support *H.264*, along with *ISDN* endpoints, are connected as *Legacy Endpoints* and receive content through their video channel. If the *Send Content to Legacy Endpoints* selection is disabled these endpoints will not receive content.

Select this option only if most of the endpoints support the *H.264* protocol.

### Guidelines

- Only endpoints that support *H.264* capability at a resolutions of *HD720p5* or higher will be able to receive and send *Content*.
- In *MPM+ Card Configuration Mode*, maximum supported content resolution is HD 720p.
- When *H.264 HD* is selected, the *Send Content to Legacy Endpoints* selection is enabled by default in the *Conference Profile – Video Settings* tab.
- Once an endpoint is categorized as a *Legacy Endpoint* and receives the content over the video channel, it remains in this mode without the ability to upgrade to *H.264 HD* content and receive content over the *Content* channel.

Content Bit rate is allocated by the RMX according to the conference line rate and Content Settings shown in *Table 1-3* decision matrix:

**Table 1-3** 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 1728	1920	2048	4096	6144
Graphics		64	64	128	128	256	256	256	256	512	1152	1536
Hi Resolution Graphics		64	128	192	256	384	384	512	768	768	1536	1536
Live Video		64	128	256	384	512	768	768	1152	1152	1536	1536

Table 1-4 summarizes the *Maximum Resolution of Content* and *Frames per Second (fps)* for *Bit Rate Allocations* to the *Content Channel* as set out in Table 1-3.

**Table 1-4** Content - Maximum Resolution, Frames/Second per Bit Rate Allocation

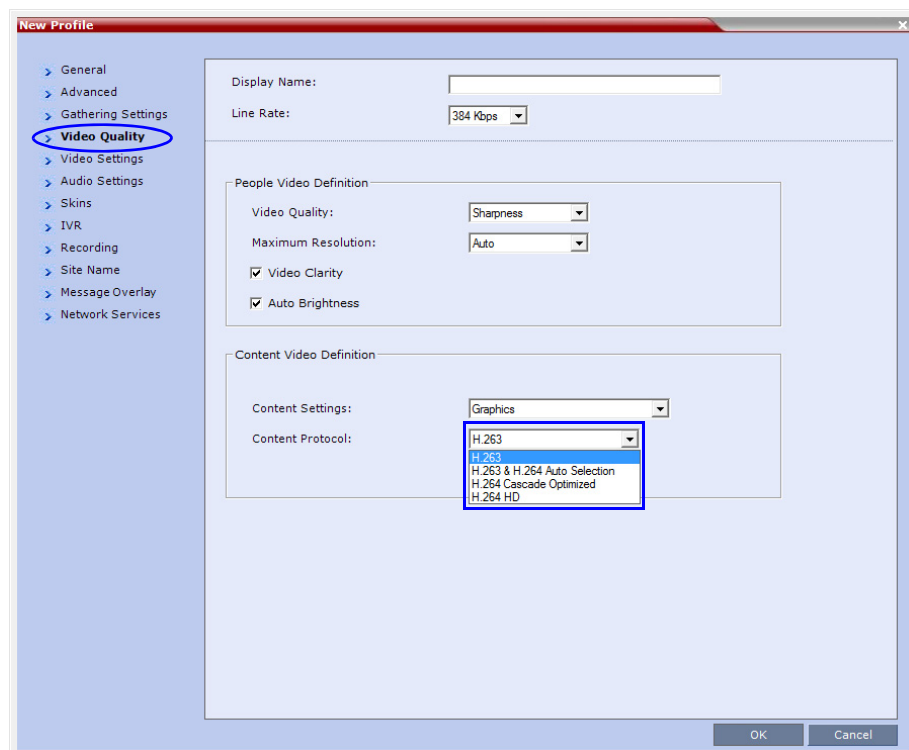
Bit Rate Allocated to Content Channel (kbps)	Content	
	Maximum Resolution	Frames/Second
From <b>64</b> and less than <b>512</b>	H.264 HD720p	5
From <b>512</b> and less than <b>768</b>	H.264 HD720p	30
From <b>768</b> and up to <b>1536</b>	H.264 HD1080p	15

- The minimum *Content Rate* required for allowing a participant to share *Content* is the lower valued parameter when comparing the *System Flag* setting and the *content bit rate allocation* derived from the conference line rate (Table 1-3).

When the flag settings enable an endpoint to share Content at a content rate that is lower than the conference content rate (Table 1-3), the content rate of the entire conference is reduced to the content rate supported by that endpoint.

## Enabling H.264 HD Content Sharing for a Conference

H.264 HD content sharing is selected in the *New Profile – Video Quality* tab.



## Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD

The following *System Flags* determine the minimum content rate required for endpoints to share H.264 high quality content via the *Content* channel. A *System Flag* determines the minimum line rate for each *Content Setting*: *Graphics*, *Hi Resolution Graphics*, *Live Video*.

In order to change the *System Flag* values, the flags must be manually added to the *System Configuration*. For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying System Flags" on page 21-1.

Content Settings	Flag Name	Range	Default
<b>Graphics</b>	<i>H264_HD_GRAPHICS_MIN_CONTENT_RATE</i>	0-1536	128
<b>Hi Resolution Graphics</b>	<i>H264_HD_HIGHRES_MIN_CONTENT_RATE</i>	0-1536	256
<b>Live Video</b>	<i>H264_HD_LIVEVIDEO_MIN_CONTENT_RATE</i>	0-1536	384

### Example

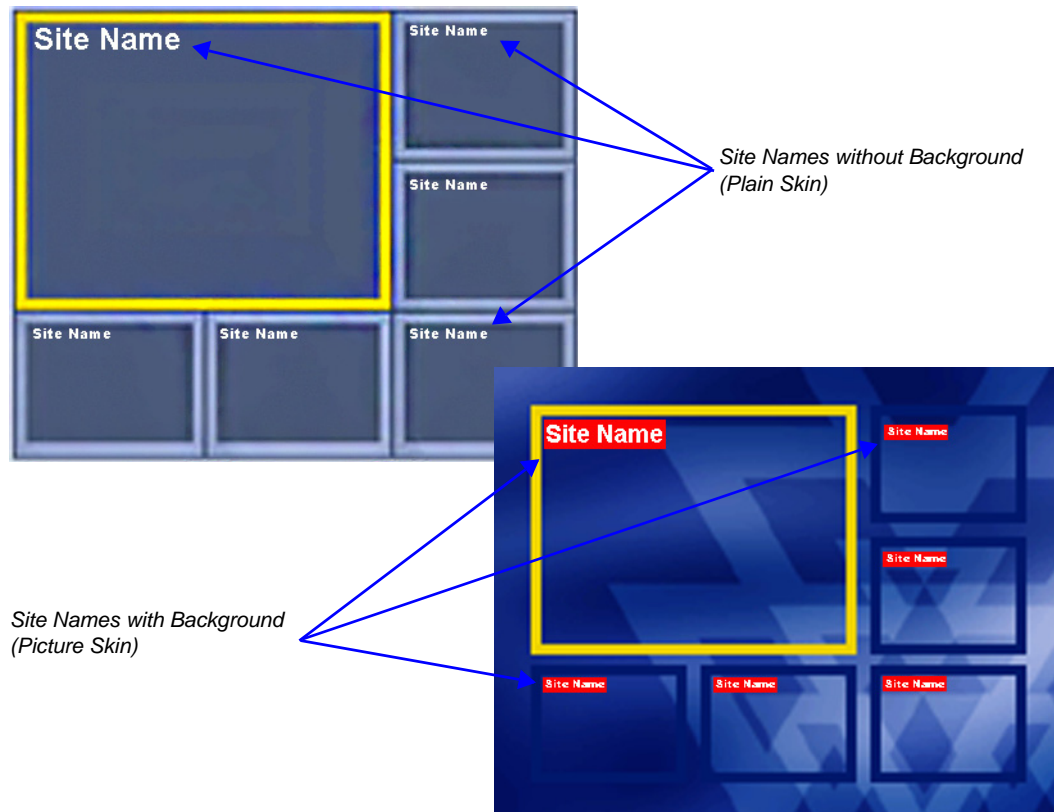
Table 1-5, summarizes an example of two participants trying to share content when connected to a conference set to a *Line Rate* of 1024Kbps and *Content Quality* is set to **Hi Resolution Graphics** with different *H264\_HD\_HIGHRES\_MIN\_CONTENT\_RATE* *System Flag* different line rate values

**Table 1-5** Participant Content Sharing Based on cOnnection Line Rate and System Flag Setting

	Participant		Conference		Flag Value	Result
	Line Rate	Bit Rate Allocation to Content Channel (Table 1-3)	Line Rate	Bit Rate Allocation to Content Channel (Table 1-3)		
<i>Participant 1</i>	384	192	1024	384	128	Participant and conference share content at 192Kbps
					512	Participant receives content in the video channel (Legacy)
<i>Participant 2</i>	1024	384			128	Participant and conference share content at 384Kbps
					512	Participant and conference share content at 384Kbps

## Site Names

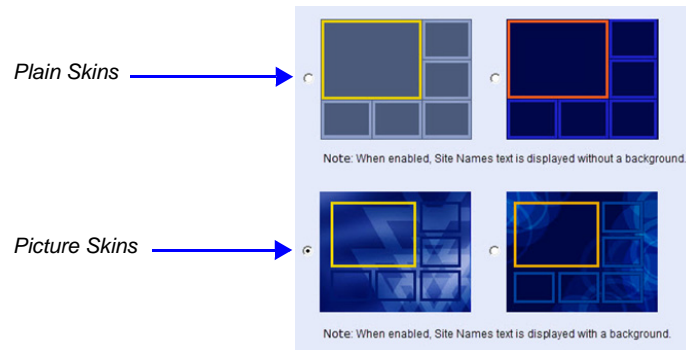
The control over the display of *Site Names* during an ongoing *Continuous Presence* conference was moved to the *Conference Profile* level. Using the *Site Name* dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the *Video Window*.



### Guidelines

- Only *MPMx* cards are supported.
- *Site Names* display is **Off** by default in a new profile.
- *Site Names* can be enabled to function in one of two modes:
  - **Auto** – Site names are displayed for 10 seconds whenever the conference layout changes.
  - **On** – Site names are displayed for the duration of the conference.
- *Site Names* display is not available for *Video Switching (VSW)* conferences.
- *Site Names* display characteristics (position, size, color) can be modified during an ongoing conference using the *Conference Properties - Site Names* dialog box. Changes are immediately visible to all participants.
- *Site Names* display text and background color is dependent on the *Skin* selected for the conference:
  - **Plain Skins** - *Site Names* text is displayed without a background.

- **Picture Skins** - *Site Names* text is displayed with a background.



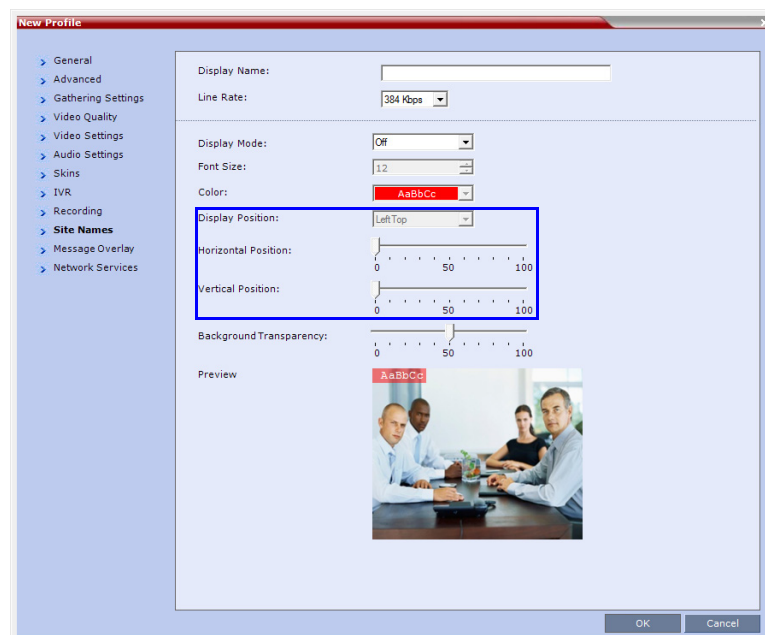
- In *MPMx Card Configuration Mode*, the *Site Names* tab options replace the functionality of the *System Flags* that were used in versions 7.6 and earlier.
- In *MPM+ Card Configuration Mode*, *Site Names* display is controlled by the following *System Flags*, as in previous versions:
  - SITE\_NAME\_TRANSPARENCY
  - SITE\_NAMES\_ALWAYS\_ON
  - SITE\_NAMES\_LOCATION

For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying *System Flags*" on page [21-1](#).

## Site Names Display Position

The *Site Names* display position is controlled using three fields in the *Site Names* tab:

- *Display Position* drop-down menu
- *Horizontal Position* slider
- *Vertical Position* slider



Using these three fields, the position at which the *Site Names* are displayed in the *Video Windows* can be set by:

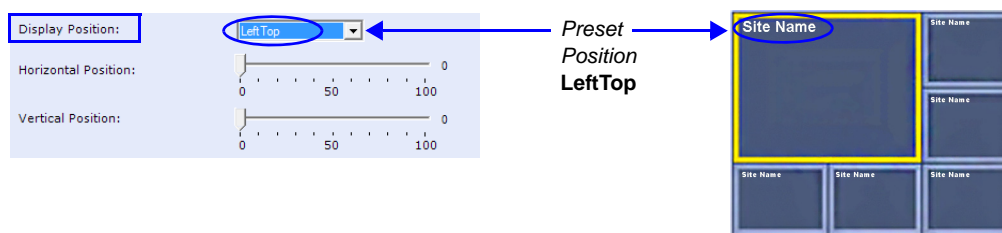
- Selecting a preset position from the drop-down menu in the *Display Position* field.
- Moving the *Horizontal* and *Vertical Position* sliders.
- Selecting **Custom** and moving the *Horizontal* and *Vertical Position* sliders.

#### Selecting a preset position from the drop-down menu in the *Display Position* field

>> In the *Display Position* drop-down menu select a preset position for *Site Names* display. Preset positions include:

*LeftTop*      *Top*      *RightTop*  
*LeftMiddle*      *RightMiddle*  
*LeftBottom*      *Bottom*      *RightBottom*  
*Custom*

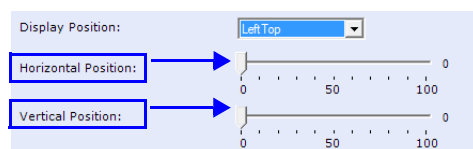
When *Custom* is selected, the current position becomes the initial position for *Site Names* position adjustments using the *Horizontal* and *Vertical Position* sliders.



The *Horizontal* and *Vertical Position* sliders are automatically adjusted to match the *Display Position* drop-down menu preset selection.

#### Moving the *Horizontal* and *Vertical Position* sliders

>> Drag the *Horizontal* and *Vertical Position* sliders to adjust the position of the *Site Names* display.



The *Site Names* display moves from its current position according to the slider movement.

Dragging the sliders causes the *Display Position* drop-down menu field to be set **Custom**.

#### Selecting **Custom** and moving the *Horizontal* and *Vertical Position* sliders

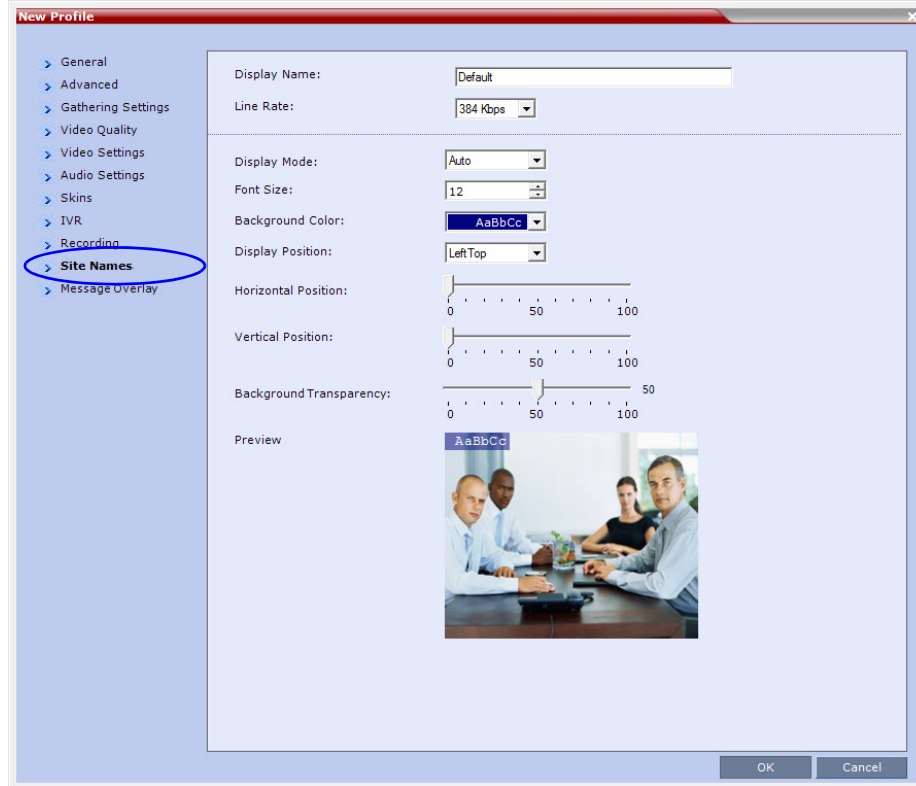
1 In the *Display Position* drop-down menu select **Custom**.

The current *Site Names* position becomes the initial position for *Site Names* position. Dragging the *Horizontal* and *Vertical Position* sliders moves the *Site Names* from this position.

2 Drag the *Horizontal* and *Vertical Position* sliders to adjust the position of the *Site Names* display.

## Enabling, Disabling and Modifying Site Names Display

*Site Names* display is enabled, disabled and modified using the *New Profile - Site Names* tab, or the *Profile Properties - Site Names* tab.



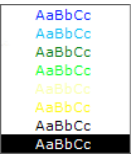
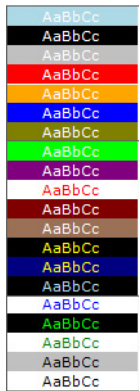
**To enable, disable or modify the Site Names display:**

>> Modify the following fields:

**Table 1-6** *New Profile / Profile Properties - Site Names Tab*

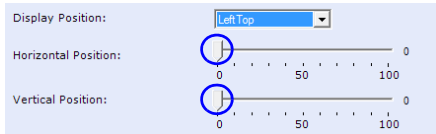

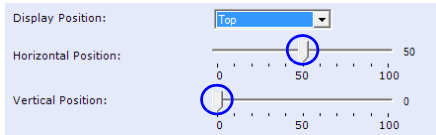

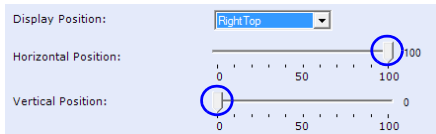
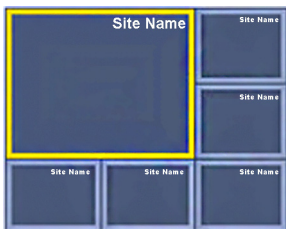
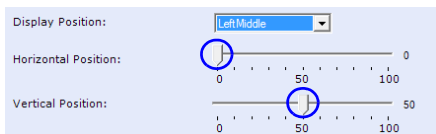

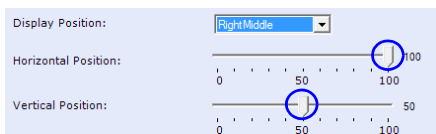
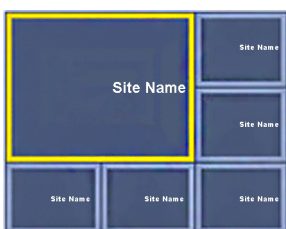
Field	Description
<i>Display Mode</i>	<p>Select the display mode for the site names:</p> <ul style="list-style-type: none"> <li><b>Auto</b> - Display the <i>Site Names</i> for 10 seconds whenever the <i>Video Layout</i> changes.</li> <li><b>On</b> - Display the <i>Site Names</i> for the duration of the conference.</li> <li><b>Off</b> (default) - Do not display the <i>Site Names</i>.</li> </ul> <p><b>Note:</b>  The <i>Display Mode</i> field is grayed and disabled if <i>Video Switching</i> mode is selected in the <i>Profile - General</i> tab.  If <i>Display Mode</i> is <b>Off</b>, all other fields in this tab are grayed and disabled.  Selecting <b>Off</b> enables <i>Video Switching</i> for selection in the <i>Profile - General</i> tab (if the conference is not already ongoing).</p>

**Table 1-6** New Profile / Profile Properties - Site Names Tab (Continued)

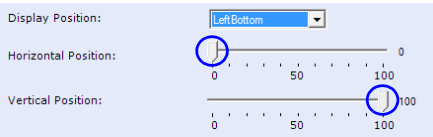
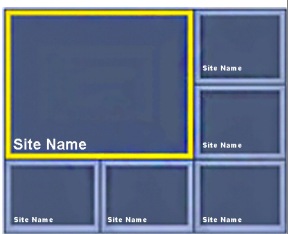
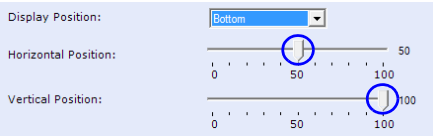

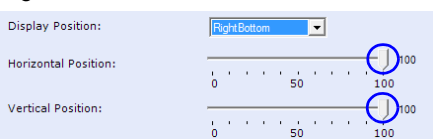
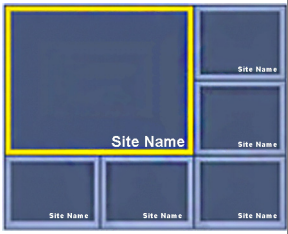
Field	Description
Font Size	<p>Click the arrows to adjust the font size (in points) for the <i>Site Names</i> display.</p> <p><b>Range:</b> 9 - 32 points</p> <p><b>Default:</b> 12</p> <p><b>Note:</b> Choose a <i>Font Size</i> that is suitable for viewing at the conference's video resolution. For example, if the resolution is <i>CIF</i>, a larger <i>Font Size</i> should be selected for easier viewing.</p>
Background Color	<p>Select the color of the <i>Site Names</i> display text.</p> <p>The color and background for <i>Site Names</i> display text is dependent on whether a <i>Plain Skin</i> or a <i>Picture Skin</i> was selected for the conference in the <i>Profile - Skins</i> tab.</p> <p>The choices are:</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: left;"> <p><b>Plain Skin</b></p>  <p><b>Default:</b> White Text No Background</p> <p>(For contrast, no background is shown as black when the text is white.)</p> </div> <div style="text-align: left;"> <p><b>Picture Skin</b></p>  <p><b>Default:</b> White Text Red Background</p> </div> </div> <p><b>Note:</b> Choose a <i>Background Color</i> combination that is suitable for viewing at the conference's video resolution. At low resolutions, it is recommended to select brighter colors as dark colors may not provide for optimal viewing.</p>



**Table 1-6** New Profile / Profile Properties - Site Names Tab (Continued)

Field	Description
<i>Display Position</i>	<p>Select the pre-set position for the display of the <i>Site Names</i>.</p> <p><b>Selection</b></p> <p><b>LeftTop (Default)</b></p>   <p><b>Top</b></p>   <p><b>RightTop</b></p>   <p><b>LeftMiddle</b></p>   <p><b>RightMiddle</b></p>  

**Table 1-6** New Profile / Profile Properties - Site Names Tab (Continued)

Field	Description
<i>Display Position</i> (cont.)	<div> <p><b>LeftBottom</b></p>   </div> <div> <p><b>Bottom</b></p>   </div> <div> <p><b>RightBottom</b></p>   </div> <div> <p><b>Custom</b></p> <p>The current <i>Site Names</i> display position becomes the initial position for <i>Site Names</i> position adjustments using the <i>Horizontal</i> and <i>Vertical Position</i> sliders.</p> </div>
<i>Horizontal Position</i>	<p>Move the slider to the <b>left</b> to move the horizontal position of the <i>Site Names</i> to the <b>left</b> within the <i>Video Windows</i>. Move the slider to the <b>right</b> to adjust the horizontal position of the <i>Site Names</i> to the <b>right</b> within the <i>Video Windows</i>.</p>
<i>Vertical Position</i>	<p>Move the slider to the <b>left</b> to move the vertical position of the <i>Site Names</i> <b>upward</b> within the <i>Video Windows</i>. Move the slider to the <b>right</b> to move the vertical position of the <i>Site Names</i> <b>downward</b> within the <i>Video Windows</i>.</p>
<p><b>Note:</b> Use of these sliders will set the <i>Display Position</i> selection to <b>Custom</b>.</p>	

**Table 1-6** *New Profile / Profile Properties - Site Names Tab (Continued)*

Field	Description
<i>Background Transparency</i>	<p>Move the slider to the left to decrease the transparency of the background of the <i>Site Names</i> text. 0 = No transparency (solid background color). Move the slider to the right to increase the transparency of the background of the <i>Site Names</i> text. 100 = Full transparency (no background color)</p> <p><b>Default:</b> 50</p> <p><b>Note:</b> This slider is only displayed if a <i>Picture Skin</i> is selected.</p>

## w448p Resolution

For improved interoperability with *Tandberg MXP 990/3000* endpoints, this version, with the appropriate *System Flag* settings, will force the RMX to send *w448p* (768x448 pixels) at 25fps as a replacement resolution for *WSD15* (848x480) and *SD15* (720x576 pixels).

### Guidelines

- The *w448p* resolution is supported:
  - In *MPMx* card configuration mode.
  - In *CP* mode.
  - At conference line rates of 384kbps and 512kbps.
  - With *H.323*, *SIP* and *ISDN* endpoints.  
*H.323* endpoints must identify themselves as **Tandberg MXP** during capabilities exchange.
  - In all *Video Layouts*.
  - In *1x1 Layout*:
    - When *Video Clarity* is **Off**, the RMX transmits the same resolution as it receives.
    - When *Video Clarity* is **On**, the RMX changes the transmitted resolution to *w448p*.
- For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "*Video Clarity™*" on page **1-18**.
- Resource consumption for the *w448p* resolution is the same as for *SD* and *WSD* resolutions, with each *MPMx-D* card supporting up to 60 *w448p* participants.

Table 2 lists the video outputs from the RMX to the *Tandberg Endpoints* for both 16:9 *Aspect Ratio* when the *w448p* resolution is enabled.

**Table 2** Video Output to Tandberg Endpoints- Aspect Ratio 16:9

Network Environment	Video Quality		Line Rate Kbps	Resolution	Frame Rate fps	Resolution	Frame Rate fps
	Tandberg	RMX		Tandberg to RMX		RMX to Tandberg	
<i>H.323</i> <i>SIP</i> <i>ISDN</i>	Motion	Sharpness	384	512x288	30	<b>768x448</b>	<b>25</b>
			512	768x448	30	<b>768x448</b>	<b>25</b>
<i>H.323</i> <i>SIP</i> <i>ISDN</i>	Sharpness*	Sharpness	384	1024x576	15	<b>768x448</b>	<b>25</b>
			512	1024x576	15	<b>768x448</b>	<b>25</b>

\* It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the RMX.

Table 3 list the video outputs from the RMX to the Tandberg Endpoints for 4:3 Aspect Ratio when the w448p resolution is enabled.

**Table 3** Video Output to Tandberg Endpoints - Aspect Ratio 4:3

Network Environment	Video Quality		Line Rate Kbps	Resolution	Frame Rate fps	Resolution	Frame Rate fps
	Tandberg	RMX		Tandberg to RMX		RMX to Tandberg	
H.323 SIP ISDN	Motion	Sharpness	384	576x448 ‡	25	768x448	25
			512	576x448 ‡	25	768x448	25
H.323 SIP ISDN	Sharpness*	Sharpness	384	4CIF	15	768x448	25
			512	4CIF	15	768x448	25

\* It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the RMX.

‡ MXP 990/3000 endpoints transmit 576x448 pixels. Other MXP endpoints may transmit other resolutions eg. CIF.

## Content

Sharing and receiving *Content* is supported.

Bandwidth allocated to the *Content* channel during *Content* sharing may cause the video resolution to be decreased as from w448p to w288p.

When *Content* sharing stops and the full bandwidth becomes available, video resumes at the previous w448p resolution.

For more information see the RMX 1500/2000/4000 Administrator's Guide, "H.239 / People+Content" on page 3-2.

## Lost Packet Recovery

If there is *Packet Loss* in the network and *Dynamic Bandwidth Allocation (DBA)* is activated, allocating bandwidth for *Lost Packet Recovery*, video resolution decreases from w448p to w288p.

When *Packet Loss* ceases and *DBA* no longer needs to allocate bandwidth for *Lost Packet Recovery*, the full bandwidth becomes available and video resumes at the previous w448p resolution.

For more information see the RMX 1500/2000/4000 Administrator's Guide, "LPR – Lost Packet Recovery" on page 3-41.

## Enabling Support of the w448p Resolution

*w448p* resolution support for *Tandberg* endpoints requires setting of the following entities:

- *Tandberg* endpoint
- RMX flags
- RMX Conference Profile

### RMX System Flag Settings

- The *System Flag* **USE\_INTERMEDIATE\_SD\_RESOLUTION** must be manually added to *system.cfg* with its value set to **YES**.
- The value of the **PAL\_NTSC\_VIDEO\_OUTPUT** *System Flag* must be set to **PAL**.  
If the *System Flag* is not defined as **PAL**, and if the current speaker is sending **NTSC** video stream, the *frame rate* will decrease to 15fps. Setting the flag to **PAL** will ensure that a *frame rate* of 25fps is maintained.

For more information about modifying *System Flags*, see the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying *System Flags*" on page **21-1**.

### SIP and ISDN endpoints

The *System Flag* only affects endpoints that support *SD* resolution and for which the RMX would have selected a transmission frame rate of 15 fps. Higher resolution endpoints are not affected by this flag.

All *SIP* and *ISDN* endpoints (not only *Tandberg MXP*) are connected as if they are *Tandberg MXP* causing RMX to select *w448p*, because endpoint-type information from these endpoints is not guaranteed during capabilities exchange.



For flag changes (including deletion) to take effect, the RMX must be reset. For more information, see "Resetting the RMX" on page **20-67**.

### RMX Profile Setting

- On the RMX, the *Video Quality* field in the *New Profile - Video Quality* dialog box must be set to **Sharpness**.  
For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Defining *Profiles*" on page **1-10**.

## Network Traffic Control

A Network Traffic Control mechanism has been added to the RMX that controls the level of UDP packets generated by the system. Network Traffic Control regulates a set of queuing



Only supported in the MPMx Card Configuration mode.

systems and mechanisms by which UDP packets are received and “transmitted” to the network router. During a conference, MPMx cards occasionally blast-out UDP packets which can cause overloads on the network. RMX bandwidth usage can increase to above the designated conference participant line rate settings, causing network bandwidth issues such as latency and packet loss.

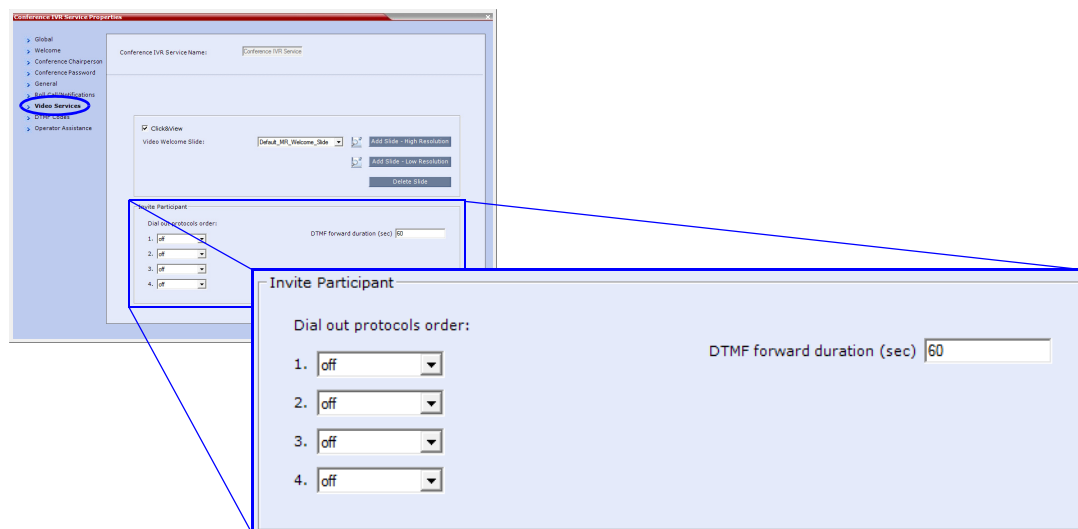
Three Network Traffic Control Flags are added:

- `ENABLE_TC_PACKAGE` - default = NO. When the flag is set to NO, Network Traffic Control is disabled on the RMX. Set the flag to YES to enable Network Traffic Control.
- `TC_BURST_SIZE` - default = 10, flag range: 1-30. This flag regulates the Traffic Control buffer or maxburst size as a percentage of the participant line rate. In general, higher traffic rates require a larger buffer. For example, if the flag is set to 10 and the participants line rate is 2MB, then the burst size is 200Kbps.
- `TC_LATENCY_SIZE` - default = 500, flag range: 1-1000 (in milliseconds). This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue.

# Version 7.6.1 Changes to Existing Features

## Conference IVR Service - Invite Participant

A new pane, *Invite Participant*, has been included in the *New Conference IVR Service* and *IVR Service Properties - Video Services* dialog boxes.



### Fields

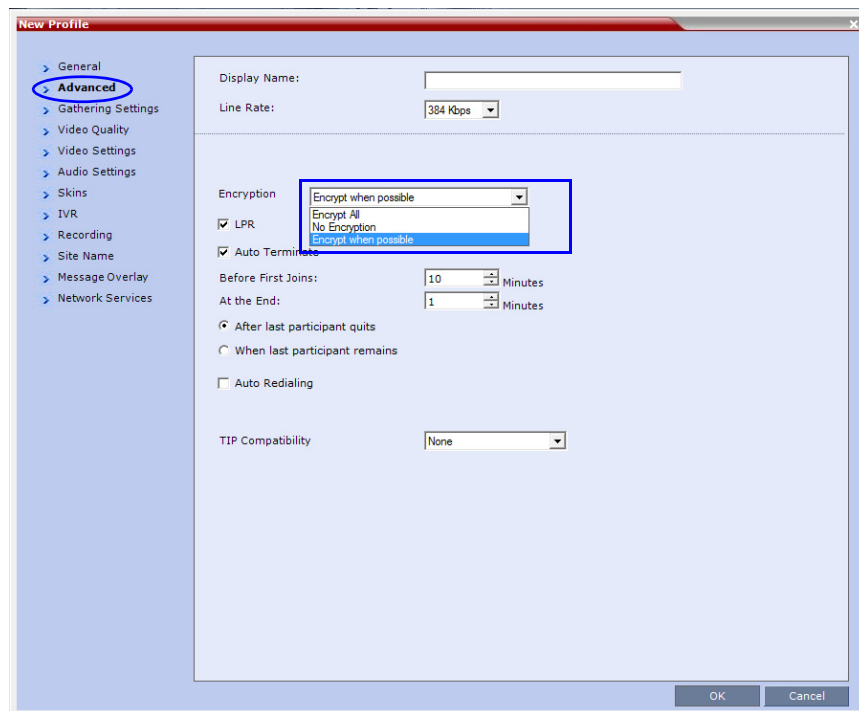
- *Dial out protocol order*  
Selects the order of the network protocols that will be used by the system to dial the destination number.
- *DTMF forward duration (sec)*  
Sets the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number.

For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Defining a New Conference IVR Service" on page **16-7**.



## Encryption Changes

From version 7.6.1, the `ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF` System Flag is replaced by the *Encryption* option “*Encrypt When Possible*” in the *Conference Profile - Advance* dialog box and the *Encryption* check box has been replaced with a drop-down menu.



The *Encryption* option - “*Encrypt When Possible*” enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. Defined participants that cannot connect encrypted are connected non-encrypted, with the exception of dial-out SIP participants.



- When the conference encryption is set to “*Encrypt when possible*”, dial out SIP participants whose encryption is set to AUTO can only connect with encryption, otherwise they are disconnected from the conference.
- In CISCO SIP environments, dial in endpoints that are registered to CUCM can only connect as non-encrypted when the conference encryption is set to “*Encrypt when possible*” as the CUCM server sends the Invite command without SDP.

The same system behavior can be applied to undefined participants, depending on the setting of the System Flag

`FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE`:

- When set to **NO** and the conference encryption in the Profile is set to “*Encrypt When Possible*”, both *Encrypted* and *Non-encrypted undefined participants* can connect to the same conferences, where encryption is the preferred setting.
- When set to **YES** (default), *Undefined participants* must connect encrypted, otherwise they are disconnected.

For *defined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile*, the *Defined Participant's* encryption settings.

For *undefined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile*, the System Flag setting and the connecting endpoint's *Media Encryption* capabilities.

## Direct Connection to the Conference

Table 1-1, summarizes the connection status of participants, based on the encryption settings in the conference *Profile*, the *Defined Participant's* encryption settings or the System Flag setting for undefined participants and the connecting endpoint's *Media Encryption* capabilities.

**Table 1-1** Connection of Defined and Undefined H.323 and SIP Participants to the Conference Based on the Encryption Settings

Conference Encryption Setting	Defined Participant		Undefined Participant	
	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES
No Encryption	Auto	Connected, non-encrypted	Connected non-encrypted (Encryption is not declared by the RMX, therefore the endpoint does not use encryption)	Connected non-encrypted (Encryption is not declared by the RMX, therefore the endpoint does not use encryption)
	No	Connected, non-encrypted		
	Yes	Connected only if encrypted. Non-encrypted endpoints are disconnected as encryption is forced for the participant.		
Encrypt All	Auto	Connected, encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected
	No	Disconnected (cannot be added to the conference)		
	Yes	Connected, encrypted		

**Table 1-1** Connection of Defined and Undefined H.323 and SIP Participants to the Conference Based on the Encryption Settings (Continued)

Conference Encryption Setting	Defined Participant		Undefined Participant	
	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES
Encrypt When Possible	Auto	<p><i>All defined participants except dial-out SIP participants:</i> Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities.</p> <p><i>Defined dial-out SIP participant:</i> Connect only if encrypted. Non-encrypted endpoints are disconnected.</p>	Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities	Connect only if encrypted. Non-encrypted endpoints are disconnected.
	No	Connected, non-encrypted		
	Yes	Connected, encrypted		

\* System Flag = FORCE\_ENCRYPTION\_FOR\_UNDEFINED\_PARTICIPANT\_IN\_WHEN\_AVAILABLE\_MODE

For more information, see the *RMX 1500/2000/4000 Administrator's Guide, "Media Encryption"*.

## Connection to the Entry Queue

An undefined participant connecting to an *Entry Queue* inherits the encryption characteristics of the *Entry Queue* as defined in the *Entry Queue's* profile.

Table 1-2 summarizes the connection possibilities for a participant that is to be moved from an *Entry Queue* to a destination conference for each of the conference *Profile* and *Entry Queue* encryption options.

**Table 1-2** Connection of Undefined Participants to the Entry Queue Based on the Encryption Settings

Entry Queue Encryption Setting	Undefined Participant Connection to the Entry Queue	
	*Flag = No	*Flag = YES
No Encryption	Connected, non-encrypted (Encryption is not declared by the RMX, therefore endpoint does not use encryption)	Connected, non-encrypted (Encryption is not declared by the RMX, therefore endpoint does not use encryption)
Encrypt All	Connected only if encrypted. Non-encrypted endpoints are disconnected	Connected only if encrypted. Non-encrypted endpoints are disconnected

**Table 1-2** Connection of Undefined Participants to the Entry Queue Based on the Encryption Settings (Continued)

Entry Queue Encryption Setting	Undefined Participant Connection to the Entry Queue	
	*Flag = No	*Flag = YES
<b>Encrypt When Possible</b>	Connected encrypted - Endpoints with encryption capabilities. Connected non-encrypted - endpoints without encryption capabilities	Connected only if encrypted. Non-encrypted endpoints are disconnected.

\* System Flag = FORCE\_ENCRYPTION\_FOR\_UNDEFINED\_PARTICIPANT\_IN\_WHEN\_AVAILABLE\_MODE

## Moving from the Entry Queue to Conferences or Between Conference

When moving from the Entry Queue to the destination conference, or when the RMX user moves participants from one conference to another, the connection rules are similar and they are summarized in Table 1-3:

**Table 1-3** Moving Participants from the Entry Queue to the Destination conference or between conferences Based on the Encryption Settings

Destination Conference Encryption Setting	Current Participant Encryption Status			
	Encrypted		Non-Encrypted	
	*Flag = NO	*Flag = YES	*Flag = NO	*Flag = YES
<b>No Encryption</b>	Move succeeds, connected encrypted		Move succeeds, connected non-encrypted	
<b>Encrypt All</b>	Move succeeds, connected encrypted.		Move fails, disconnected.	
<b>Encrypt When Possible</b>	Move succeeds, connected encrypted	Move succeeds, connected encrypted	Move succeeds, connected non-encrypted	Connected only if endpoint was a defined participant in the source conference. Otherwise, move fails.

\* System Flag = FORCE\_ENCRYPTION\_FOR\_UNDEFINED\_PARTICIPANT\_IN\_WHEN\_AVAILABLE\_MODE

## Recording Links

*Recording Links* are treated as regular participants, however the ALLOW\_NON\_ENCRYPT\_RECORDING\_LINK\_IN\_ENCRYPT\_CONF *System Flag* must be set to YES if a non-encrypted *Recording Link* is to be allowed to connect to an encrypted conference.

Table 1-4 summarizes the connection possibilities for a *Recording Link* that is to be connected to a conference for each of the conference *profile* and *Entry Queue* encryption options.

**Table 1-4** Connections by Recording Link and Conference Encryption Settings

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	
	YES	NO
<b>Encrypt All</b>	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected
<b>No Encryption</b>	Connected non-encrypted	Connected non-encrypted
<b>Encrypt when possible</b>	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

## Upgrade Guidelines

- 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 the encryption requirements through the new encryption options according to Table 1-5.

**Table 1-5** 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	<b>YES</b>	Profile Encryption Setting	<b>Encrypt All</b>
Profile Encryption Setting	<b>NO</b>	Profile Encryption Setting	<b>No Encryption</b>
System Flag	<b>ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF =YES</b>	Profile Encryption Setting	<b>Encrypt when possible</b>

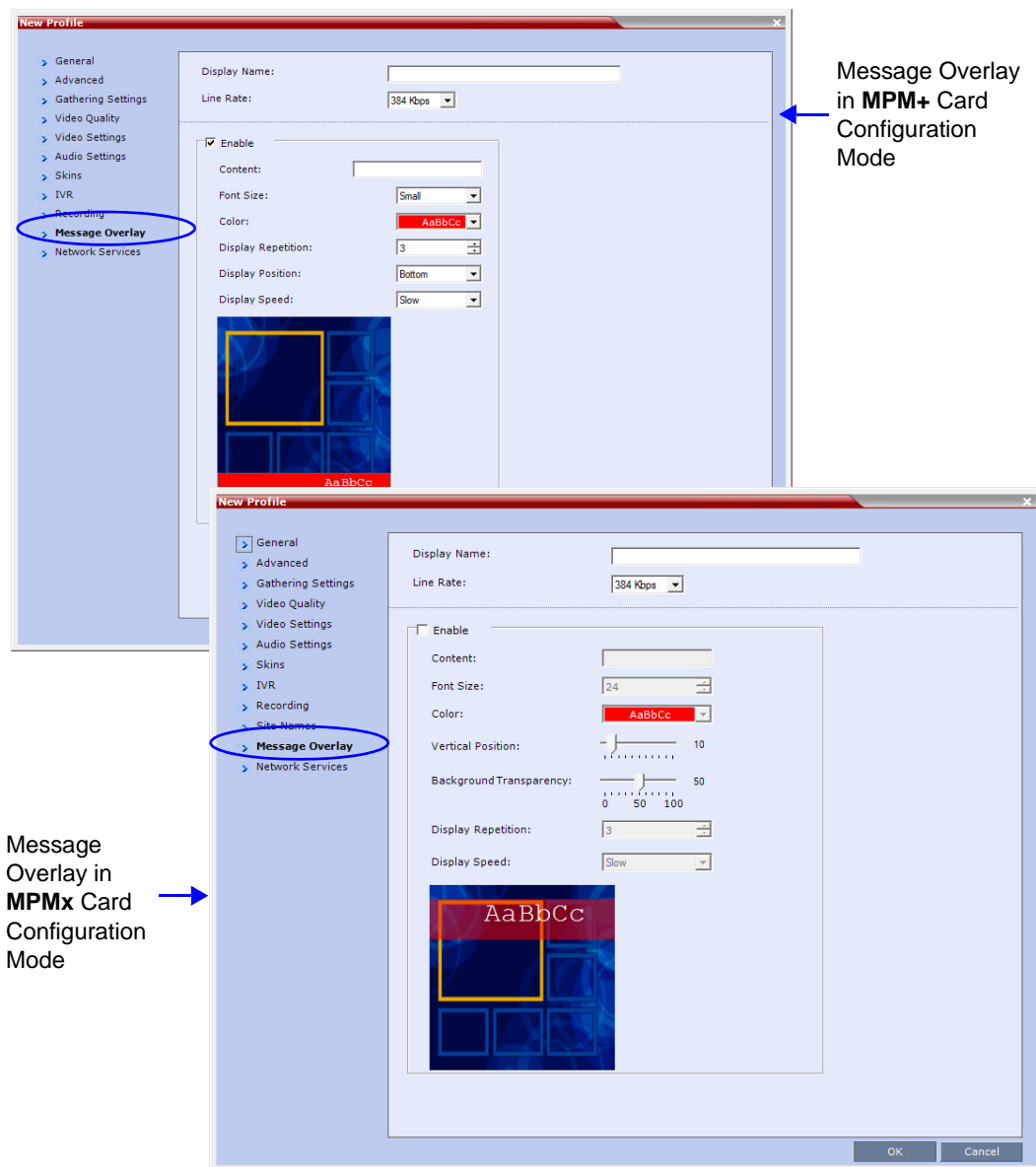
## Message Overlay

In version 7.6.1, the *Message Overlay* options are added to the *Conference Profile* in addition to their definition during the ongoing conference (in the conference *Properties - Message Overlay* dialog box).

In *MPMx Card Configuration Mode*, new options were added to the message overlay, providing additional control over the font size, the display position, text color and background color.

## Enabling, Disabling and Modifying Message Overlay Display


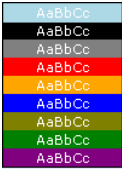
*Message Overlay* display is enabled, disabled and modified either in the *New Profile - Message Overlay* dialog box or in the *Profile Properties - Message Overlay* dialog box.



**To enable, disable or modify the Message Overlay display:**

>> Modify the following fields:

**Table 1-6** *New Profile / Profile Properties - Message Overlay Tab*

Field	Description
<i>Enable</i>	<p>Select this check box to enable <i>Message Overlay</i>. Clear this check box to disable <i>Message Overlay</i>.</p> <p><b>Default:</b> Cleared.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>The <i>Message Overlay</i> field is shaded and disabled when <i>Video Switching</i> mode is selected in the <i>New Profile - General</i> tab. All other fields in this tab are also disabled.</li> <li>Clearing the <i>Enable</i> check box enables <i>Video Switching</i> for selection in the <i>New Profile - General</i> tab.</li> <li>If <i>Message Overlay</i> is selected, the <i>Video Switching</i> check box in the <i>New Profile - General</i> tab is disabled and cannot be selected.</li> </ul>
<i>Content</i>	<p>Enter the message text. The message text can be up to 50 Chinese characters.</p>
<i>Font Size</i>	<p><b>In MPMx Card Configuration Mode:</b></p> <p>Click the arrows to adjust the font size (points) for the <i>Message Overlay</i> display.</p> <p><b>Range:</b> 9 - 32</p> <p><b>Default:</b> 24</p> <p><b>In MPM+ Card Configuration Mode:</b></p> <p>Select the size of the text font from the list: Small, Medium or Large.</p> <p><b>Default:</b> Small</p> <p><b>Note:</b> In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.</p>
<i>Color</i>	<p>From the drop-down menu select the color and background of the <i>Message Overlay</i> display text.</p> <p>The choices are:</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  <p><b>MPMx Mode</b> Color Options</p> </div> <div>  <p><b>MPM+ Mode</b> Color Options</p> </div> </div> <p><b>Default:</b> White Text on Red Background.</p>

**Table 1-6** New Profile / Profile Properties - Message Overlay Tab (Continued)

Field	Description
<i>Vertical Position</i> (MPMx Card Configuration Mode Only)	Move the slider to the <b>right</b> to move the vertical position of the <i>Message Overlay</i> <b>downward</b> within the <i>Video Layout</i> . Move the slider to the <b>left</b> to move the vertical position of the <i>Message Overlay</i> <b>upward</b> within the <i>Video Layout</i> . <b>Default:</b> Top Left (10)
<i>Background Transparency</i> (MPMx Card Configuration Mode Only)	Move the slider to the <b>left</b> to <b>decrease</b> the transparency of the background of the <i>Message Overlay</i> text. 0 = No transparency (solid background color). Move the slider to the <b>right</b> to <b>increase</b> the transparency of the background of the <i>Message Overlay</i> text. 100 = Full transparency (no background color). <b>Default:</b> 50
<i>Display Repetition</i>	Click the arrows to increase or decrease the number of times that the text message display is to be repeated. <b>Default:</b> 3
<i>Display Position</i> (MPM+ Card Configuration Mode Only)	Select the position for the display of the Message Overlay on the endpoint screen: <ul style="list-style-type: none"> <li>• Top</li> <li>• Middle</li> <li>• Bottom</li> </ul> <b>Default:</b> Bottom
<i>Display Speed</i>	Select whether the text message display is static or moving across the screen, the speed in which the text message moves: <ul style="list-style-type: none"> <li>• Static</li> <li>• Slow</li> <li>• Fast</li> </ul> <b>Default:</b> Slow

## Changes to the Message Overlay Properties during an ongoing conference

Changes to the display characteristics (position, size, color and speed) during an on going conference are immediately visible to all participants.

Changes to the *Content* are immediately visible to all participants. When there is a current *Message Overlay*:

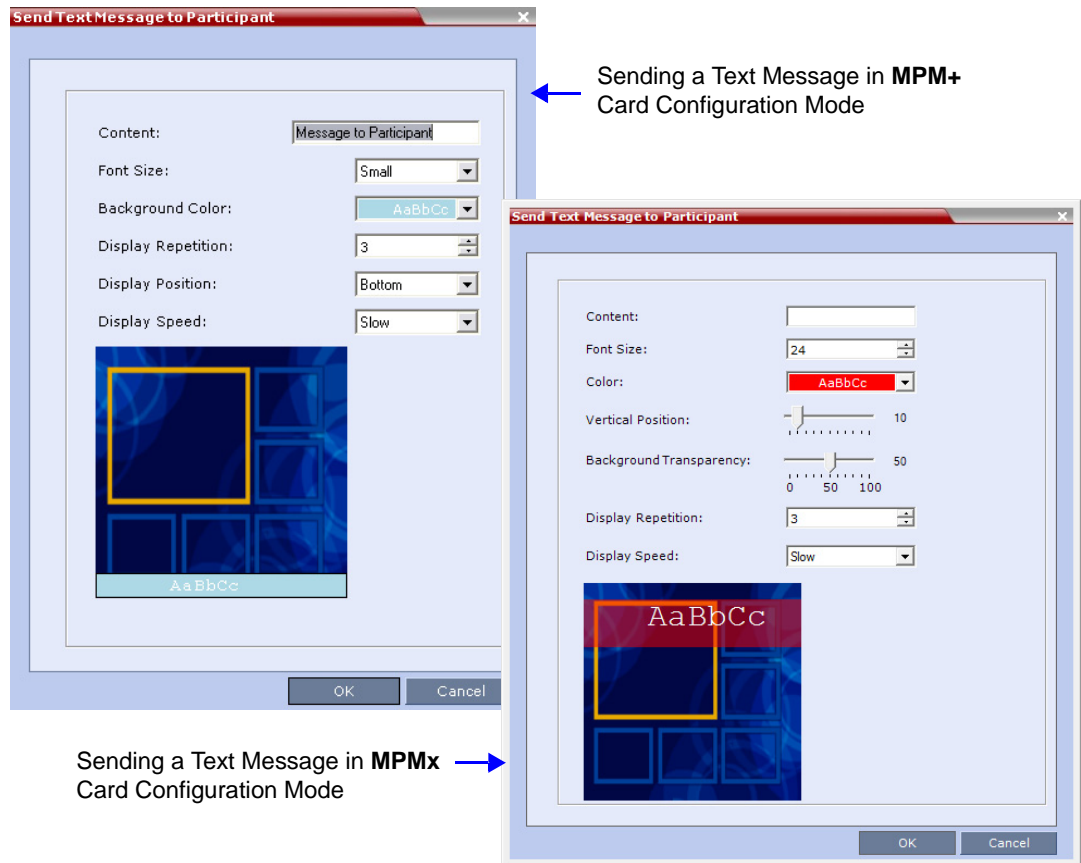
- The current message is stopped immediately.
- The *Display Repetition* count is reset to 1.

The new message *Content* is displayed <*Display Repetition*> times or until it is stopped and replaced by another *Content* change.



## Sending Text Messages to Individual or Several Participants

The same changes that were implemented to the Message Overlay parameters in MPMx card configuration mode, are also reflected in the *Send Text Message to Participant* dialog box.



## Controlling Resource Allocations for Lync Clients Using RTV

The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the Maximum video resolution set in the *Conference Profile*.

In versions 7.6 and earlier, when conferences are set to line rates above 600 kbps, the RMX could allocate up to three video resources to Lync clients connecting using the RTV video protocol.

From version 7.6.1, the system flag **MAX\_RTV\_RESOLUTION** enables you to override the RMX resolution selection and limit it to a lower resolution. Resource usage can then be minimized the 1 or 1.5 video resources per call instead of 3 resources, depending on the selected resolution.

Possible flag values are: **AUTO** (default), **QCIF**, **CIF**, **VGA** or **HD720**.

For example, if the flag is set to VGA, conference line rate is 1024Kbps, and the Profile Maximum Resolution is set to Auto, the system will limit the Lync RTV client to a resolution of VGA instead of HD720p and will consume only 1.5 video resources instead of 3 resources.

When set to **AUTO** (default), the system uses the default resolution matrix based on the conference line rate.

To change the default flag setting, add the **MAX\_RTV\_RESOLUTION** flag to the *System Configuration* flags and set its value. For information, see the RMX 1500/2000/4000 Administrator's Guide, "Manually Adding and Deleting System Flags" on page [21-16](#).

The following table summarizes the RMX resources allocated to a Lync Client based on the **MAX\_RTV\_RESOLUTION** flag setting, the connection line rate and the video resolution.

**Table 1-7** Selected video resolution based on flag setting and conference line rate and core processor

Maximum Resolution Value	Line Rate	Selected Video Resolution Per Core Processor		
		Quad	Dual	Single
<i>AUTO</i>	> 600 kbps	HD720p 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
<i>HD720p</i>	> 600 kbps	HD720p 30fps	HD720p 13fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
<i>VGA</i>	> 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF

**Table 1-7** Selected video resolution based on flag setting and conference line rate and core processor (Continued)

Maximum Resolution Value	Line Rate	Selected Video Resolution Per Core Processor		
		Quad	Dual	Single
CIF	> 600 kbps	CIF	CIF	CIF
	250 kbps - 600 kbps	CIF	CIF	CIF
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
QCIF	> 600 kbps	QCIF	QCIF	QCIF
	250 kbps - 600 kbps	QCIF	QCIF	QCIF
	180 kbps - 249 kbps	QCIF	QCIF	QCIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF



When the MAX\_ALLOWED\_RTV\_HD\_FRAME\_RATE flag equals 0 (default value), Table 1-1 for the MAX\_RTV\_RESOLUTION flag applies. When the MAX\_ALLOWED\_RTV\_HD\_FRAME\_RATE flag does not equal 0, see the RMX Administrators Guide, "Threshold HD Flag Settings using the RTV Video Protocol" on page 2-28 for more information.

Table 1-2 describes the number of allocated video resources for each video resolution when using the RTV protocol.

**Table 1-8** Allocated video resolutions per video resolution

Selected Video Resolution	Number of Allocated Video Resources
HD720p	3
VGA	1.5
CIF	1
QCIF	1

## Threshold HD Flag Settings using the RTV Video Protocol

The system flag **MAX\_ALLOWED\_RTV\_HD\_FRAME\_RATE** defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions.

Flag values are as follows:

- Default: 0 (fps) - Implements any Frame Rate based on Lync RTV Client capabilities



If the **MAX\_RTV\_RESOLUTION** flag is set to AUTO dual core systems always view VGA. For more information on Lync RTV Client capabilities, see the RMX Administrators Guide, "Controlling Resource Allocations for Lync Clients Using RTV Video Protocol" on page 2-26 for more information.

- Range: 0-30 (fps)

For example, when the flag is set to 15 and the Lync RTV Client declares HD 720P at 10fps, because the endpoint's frame rate (fps) of 10 is less than flag setting of 15, then the endpoint's video will open VGA and not HD.

In another example, when the flag is set to a frame rate of 10 and the Lync RTV Client declares HD 720P at 13fps, because the endpoint's frame rate (fps) of 13 is greater than flag setting of 10, then the endpoint's video will open HD and not VGA.



- Single core PC's cannot view HD and always connect in VGA.
- Dual Core Processor - The threshold for flag settings on Dual Core systems is 13 (fps) and less for viewing HD. When system flag is set to 14 (fps) or higher, the RTV Video Protocol shall connect in VGA.
- Quad Core PC systems always view HD, even when flag settings are set anywhere from 0-30.
- The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the maximum video resolution set in the Conference Profile. For more information, see the RMX Administrators Guide, Microsoft RTV Video Protocol.

To change the **MAX\_ALLOWED\_RTV\_HD\_FRAME\_RATE** threshold default flag setting, add the flag to the *System Configuration* flags and set its value. For information, see the RMX 1500/2000/4000 Administrator's Guide, "Manually Adding and Deleting System Flags" on page 19-18.

## New System Flag - SEND\_SRTP\_MKI

Certain endpoints (eg. CounterPath Bria 3.2 softphone) cannot decrypt SRTP-based audio and video streams if the MKI (Master Key Identifier) field is included in SRTP packets sent by the RMX.

A new *System Flag*, **SEND\_SRTP\_MKI**, has been added in this version to enable or disable the inclusion of the MKI field in SRTP packets sent by the RMX.

The default flag value is **YES**.

To disable the inclusion of the MKI field in SRTP packets sent by the RMX, the flag must be added to *system.cfg* and its value set to **NO**.

The **SEND\_SRTP\_MKI** *System Flag* should not be set to **NO** when HDX endpoints, Microsoft Office Communicator and Lync Clients are used as they all support SRTP with MKI.

# Version 7.6 Detailed Description - New Features

## RMX and Cisco Telepresence Systems (CTS) Integration

### Telepresence Interoperability Protocol (TIP)

*TIP* is a proprietary protocol created by *Cisco* for deployment in *Cisco TelePresence systems (CTS)*. Since *TIP* is not compatible with standard video communication systems, interoperability between *Cisco* and other vendors' telepresence systems was initially impossible.

Gateways were developed to provide interoperability but were subject to the inherent problems of additional latency (delay) in connections and low video quality resulting from the reformatting of video and audio content.

*Polycom's* solution is to allow the RMX to natively inter-operate with *Cisco TelePresence Systems*, ensuring optimum quality multi-screen, multipoint calls between:

- *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 Version 3.0.3*
  - 7000 HD Rev C
  - 8000 HD Rev B
  - 9006
  - 4500
- *Cisco TelePresence® System (CTS) Version 1.7*
  - CTS 1000
  - CTS 3000

*TIP* is supported by RMX 1500/2000/4000 systems with MPMx cards.

Conferences hosted on the RMX can include a mix of existing end points (that do not support *TIP*) and *CTS* endpoints.

*TIP*-enabled endpoints must support *TIP Version 7* or higher. Calls from endpoints supporting older versions of *TIP* will be rejected.

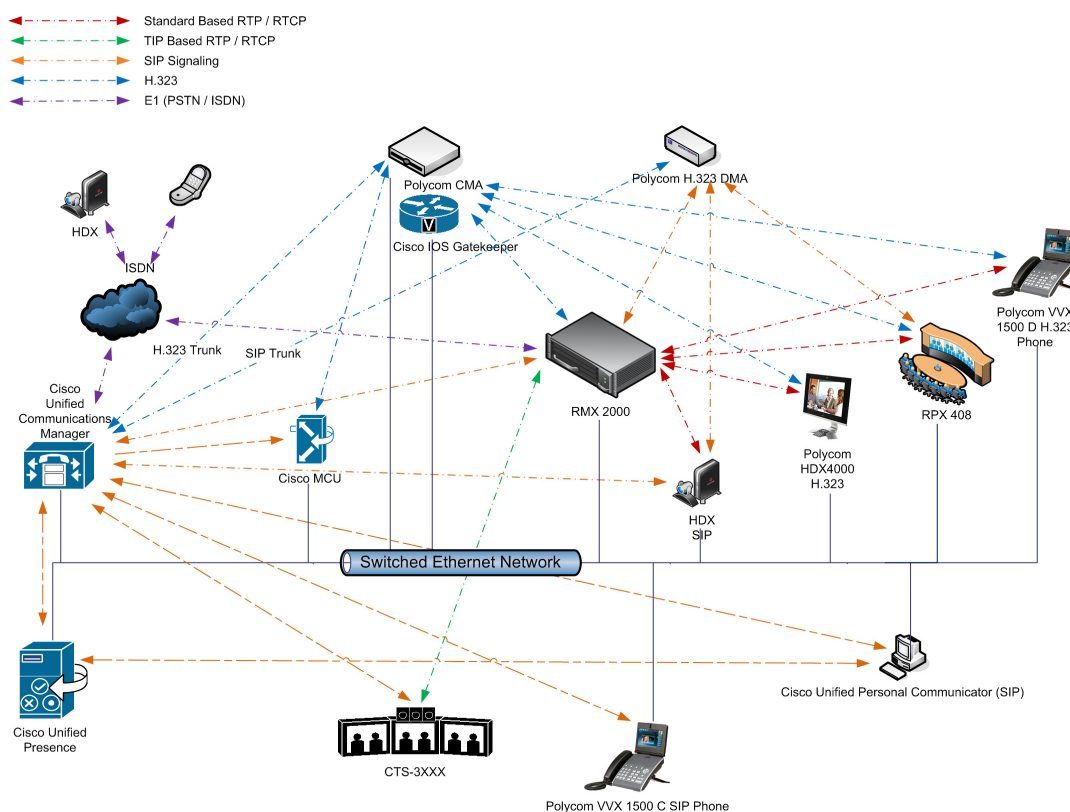
## Deployment Architectures

The following multipoint topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

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

### Single Company Model - Polycom and Cisco Infrastructure

The deployment architecture in *Figure 1-1* shows a company that has a mixture of *Polycom* and *Cisco* endpoints, room systems and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the *RMX* as the conference bridge.



**Figure 1-1** Single company with Polycom and Cisco Infrastructure

Table 1-9 lists components and versions of the *RMX and Cisco Telepresence Systems (CTS) Integration Solution Architecture*.

**Table 1-9** Solution Architecture Components

Component	Version	Description
<b>CISCO Equipment</b>		
<i>CUCM</i>	8.5	Cisco Unified Communication Manager: CUCM must be configured to: <ul style="list-style-type: none"> <li>Route calls to DMA (if present).</li> <li>Route all H.323 calls to the gatekeeper, which can be either CMA or IOS.</li> </ul>
<i>IOS</i>	15.x	Cisco Internetwork Operating System - Gatekeeper
<i>Endpoints (CTS)</i>	1.7	Telephony, desktop and room systems. <ul style="list-style-type: none"> <li>CTS endpoints must register to <i>CUCM</i>.</li> </ul>
<b>Polycom Equipment</b>		
<i>DMA 7000</i>	4.0	Polycom Distributed Media Application <ul style="list-style-type: none"> <li><i>DMA</i> is an optional component but is essential if <i>Content</i> sharing is to be enabled.</li> <li>All <i>SIP</i> endpoints register to <i>DMA</i> as a <i>SIP Proxy</i>.</li> <li><i>DMA</i> should be configured to route <i>SIP</i> calls (with CTS destination) to <i>CUCM</i>. If <i>DMA</i> is not present in the solution architecture, <i>SIP</i> endpoints must register to <i>CUCM</i> as gatekeeper.</li> <li><i>DMA</i> must be configured with a <i>VMR (Virtual Meeting Room)</i>. Incoming calls are then routed to the <i>RMX</i>.</li> </ul>
<i>RMX</i>	7.6.x	MCU: <ul style="list-style-type: none"> <li>Functions as the network bridge for multipoint calls between <i>H.323</i>, <i>SIP</i> and <i>TIP</i> endpoints.</li> <li>The <i>RMX</i> can be interfaced to <i>CUCM</i> using a <i>SIP</i> trunk, enabling CTS to join multipoint calls on <i>RMX</i>. Signaling goes through the <i>CUCM</i> while the media in <i>TIP</i> format goes directly between the CTS and <i>RMX</i>.</li> <li>The <i>RMX</i> must be configured to route outbound <i>SIP</i> calls to <i>DMA</i>.</li> <li>The H.323 Network Service of the <i>RMX</i> should register its dial prefix with the <i>CMA</i> gatekeeper.</li> <li>When <i>DMA</i> is not used an <i>Ad-hoc Entry Queue</i>, designated as <i>Transit Entry Queue</i>, must be pre-defined on the <i>RMX</i>.</li> </ul>
<i>MLA</i>	3.0.3	Multipoint Layout Application Required for managing multi-screen endpoint layouts for <i>Cisco CTS 3XXX</i> , <i>Polycom TPX</i> , <i>RPX</i> or <i>OTX</i> systems.
<i>CMA</i>	5.5	Polycom Converged Management Application - Gatekeeper <ul style="list-style-type: none"> <li>The gatekeeper must route calls to <i>RMX</i> based on the <i>RMX</i> prefix registration on the gatekeeper.</li> </ul>

**Table 1-9** Solution Architecture Components

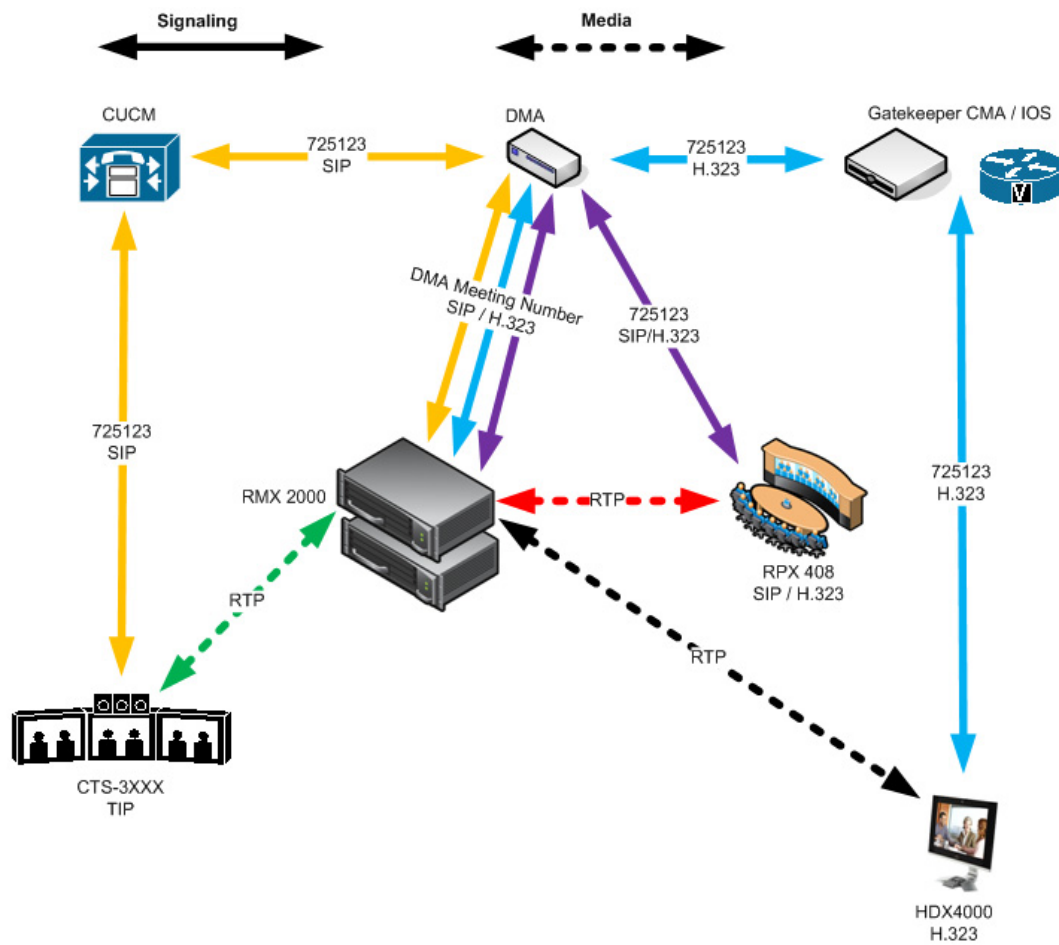
Component	Version	Description
Endpoints		Telephony, desktop and room systems. <ul style="list-style-type: none"> <li>H.323 endpoints must register to the CMA or IOS gatekeeper.</li> <li>Polycom SIP endpoints must register to DMA as SIP Proxy when DMA is used.</li> <li>H.323 endpoints must register to the CMA or IOS gatekeeper.</li> </ul>

## Call Flows

### Multipoint call with DMA

In this example:

- RMX prefix in the gatekeeper 72
- Virtual Meeting Room in DMA 725123
- DMA Meeting Number Generated by DMA

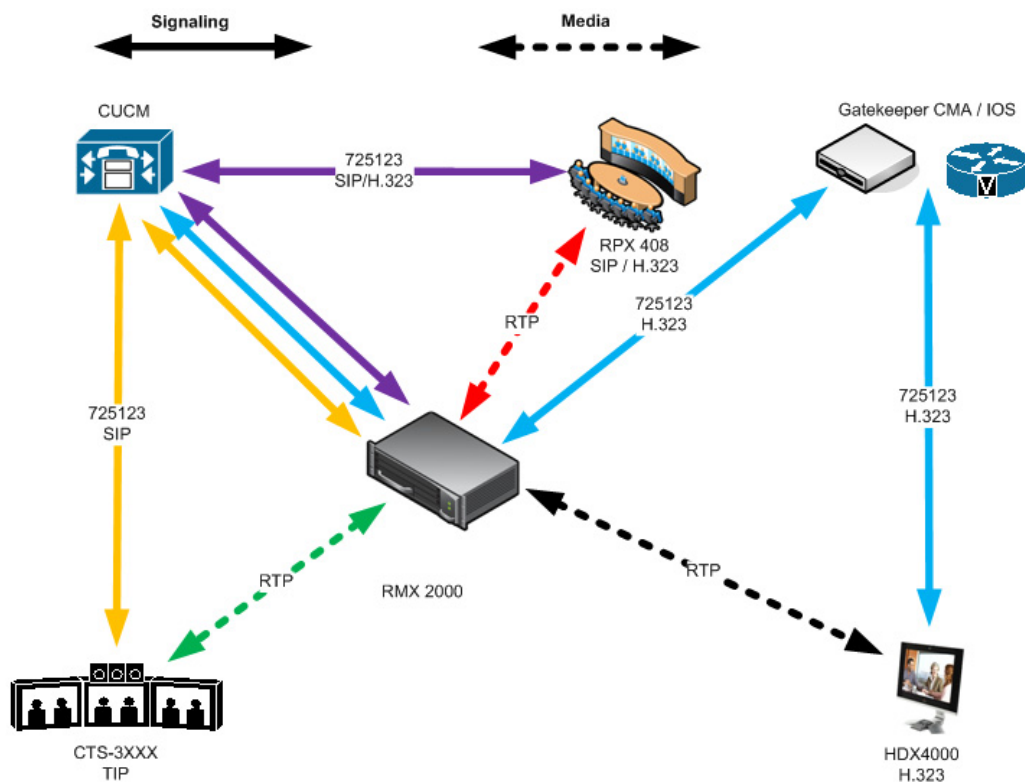




## Multipoint call without DMA

In this example:

- RMX prefix in the gatekeeper 72
  - CUCM
- According to its *Dial Plan* forwards calls with prefix 72 to the RMX



## Company to Company Models Using a Service Provider

Using this topology, both companies connect to a *Service Provider* via a *Cisco Session Border Controller (SBC)*. The *Service Provider* functions as a *B2B Telepresence Exchange*, enabling multipoint calls between the two companies and their respective video and audio endpoints using the *RMX* as the conference bridge.

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

Two topology models are discussed:

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

## Model 1

The deployment architecture in *Figure 1-2* shows two companies: *Company A* and *Company B*.

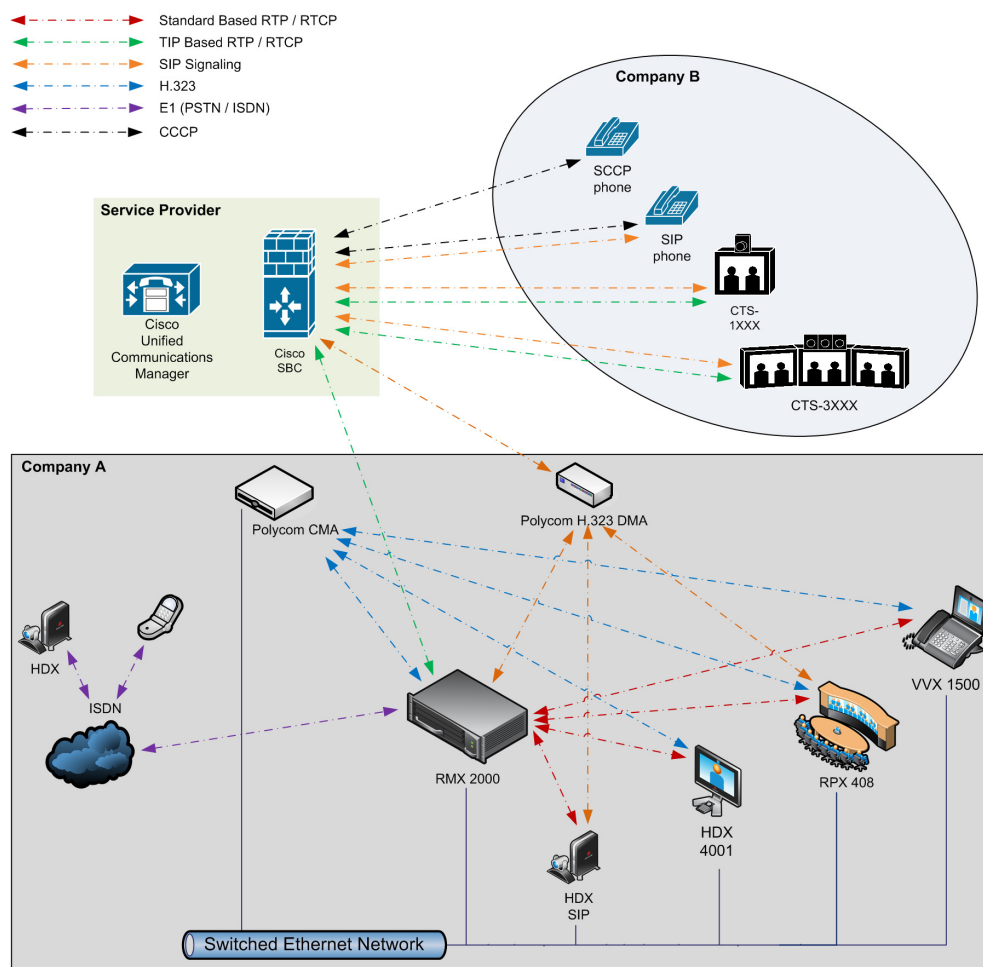
**Company A** - has deployed a *Polycom* solution including:

- DMA
- RMX
- MLA
- CMA Gatekeeper
- *Polycom* telephony and desktop endpoints.

The roles of the *Polycom* components are described in the *Polycom Equipment* section of Table 1-9 on page 81.

**Company B** - has deployed a *Cisco* solution including:

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



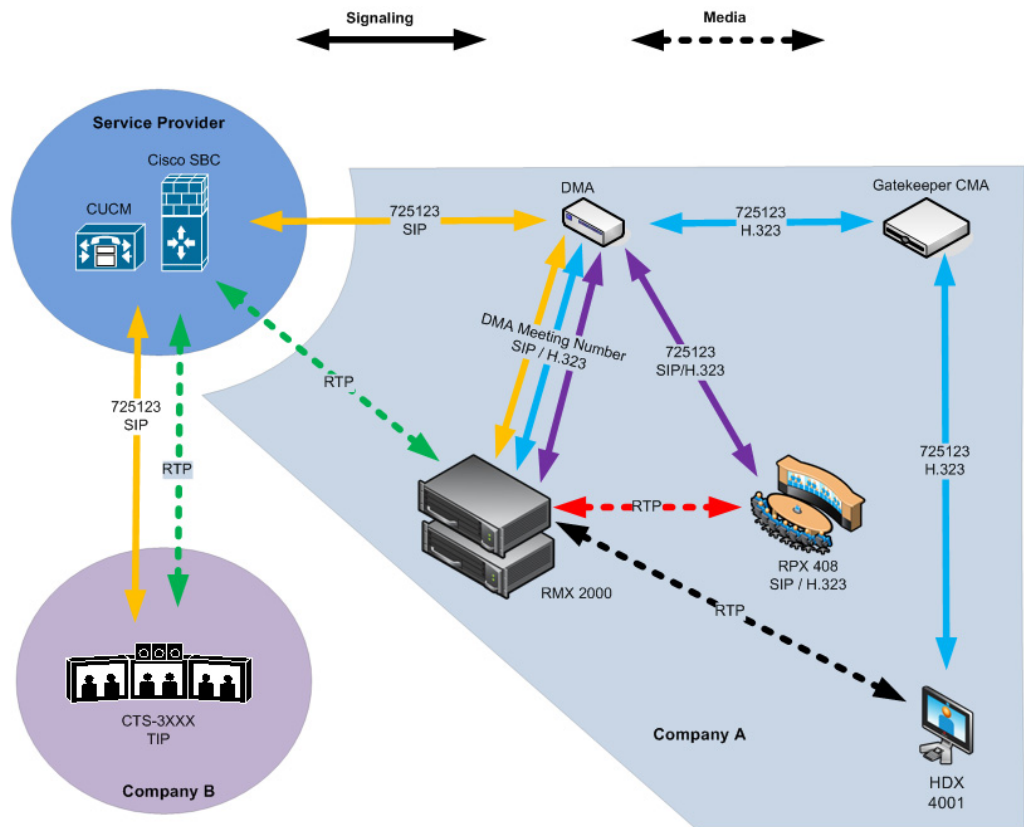
**Figure 1-2** Company to Company via Service Provider - Model 1

## Call Flow

### Multipoint call via Service Provider - Model 1

In this example:

- *RMX* prefix in the gatekeeper 72
- *Virtual Meeting Room* in DMA 725123
- *DMA Meeting Number* Generated by DMA



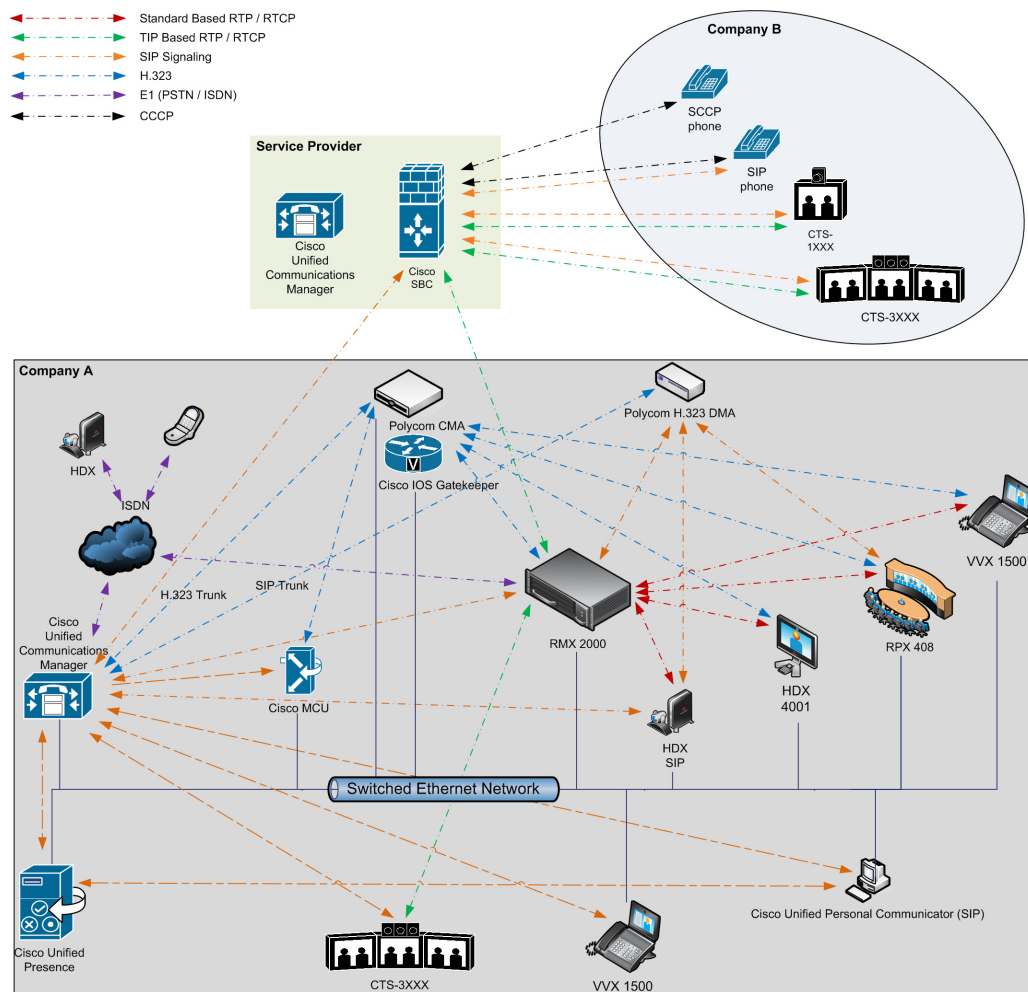
## Model 2

The deployment architecture in *Figure 1-3* shows two companies: *Company A* and *Company B*.

**Company A** - has the same deployment architecture as shown in “*Single Company Model - Polycom and Cisco Infrastructure*” on page 80.

**Company B** - has deployed a *Cisco* solution including:

- CTS 1000
- CTS 3000
- *Cisco* telephony endpoints.



**Figure 1-3** Company to Company via Service Provider - Model 2

The deployment architecture includes:

### Company A

For a full description of *Company A's* deployment, see “*Single Company Model - Polycom and Cisco Infrastructure*” on page 80.

Differing or additional configuration requirements for each element of this deployment model are listed below:

**Table 1-10** *Solution Architecture Components*

Component	Version	Description
<b>CISCO Equipment</b>		
<i>CUCM</i>	8.5	Cisco Unified Communication Manager: CUCM must be configured with a SIP trunk to the Service Provider's SBC.
<b>Polycom Equipment</b>		
<i>RMX</i>	7.6.x	MCU: RMX must be configured to send and receive RTP streams to and from the Service Provider's SBC.

### Company B

**Table 1-11** *Solution Architecture Components*

Component	Version	Description
<b>CISCO Equipment</b>		
<i>Endpoints</i>		Endpoints should register with the <i>Service Provider's CUCM</i> (or the local CUCM, if present).

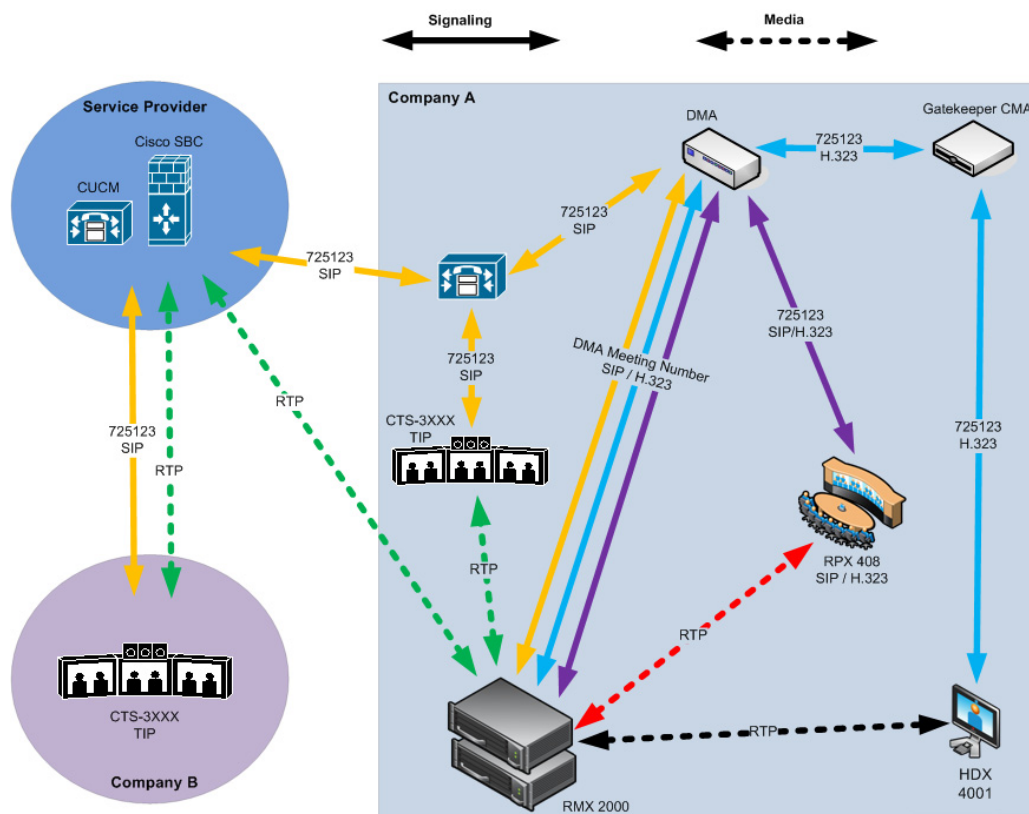
## Call Flow

## Multipoint call via Service Provider - Model 2

In this example:

- *RMX* prefix in the gatekeeper 72
- *Virtual Meeting Room* in DMA 725123
- *CUCM* Accord

According to its *Dial Plan* forwards calls with prefix 72 to the RMX



## Administration

The various deployment combinations and settings within the various *Deployment Architectures* affects the administration of the system.

## Gatekeepers

### Standalone Polycom CMA System as a Gatekeeper

The *Polycom CMA* system can be used as the only gatekeeper for the network. Bandwidth and call admission control of endpoints registered with the *CMA* system is split between the *CMA* system and the *CUCM*.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, “Using a Polycom CMA System as a Gatekeeper”.

### Standalone Cisco IOS Gatekeeper

The *Cisco IOS Gatekeeper* can be used as the only gatekeeper for the network if the management capabilities of the *Polycom CMA* system are not required.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, “Using a Standalone Cisco IOS Gatekeeper”.

### Neighbored Cisco IOS and Polycom CMA Gatekeepers

Neighbored gatekeepers make it easier to create a common dial plan and should be considered when integrating an existing *Cisco* telephony environment with an existing *Polycom* network. *Neighbored Gatekeepers* allow number translation while maintaining the existing environments.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, “Neighbored Cisco IOS and Polycom CMA Gatekeepers”.

## DMA

The *Polycom DMA* system can be configured as a *SIP* proxy and registrar for the environment. When used as a *SIP* peer, the *DMA* system can host video calls between *Cisco* endpoints that are registered with the *CUCM* and *Polycom SIP* endpoints that are registered with the *DMA* system.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, “Using a Polycom DMA System as SIP Peer”.

## CUCM

When *Polycom SIP* endpoints (voice and video) are registered directly with *CUCM* you can take advantage of supported telephone functions. *CUCM* may not support the full range of codecs and features available on the *Polycom* equipment. *CUCM* supported codecs and features will be used in such cases.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, “Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants”.



## Configuring the Cisco and Polycom Equipment

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

*Call Detail Records (CDR)* are generated on both the *CMA Gatekeeper* and the *CUCM* for reporting and billing purposes.

### Content

*Polycom* and *Cisco* endpoints can share *Content* within a *Cisco TelePresence* environment. The content sharing experience depends on whether the endpoints are registered with the *DMA* or *CUCM*.

**Table 2** Endpoint Registration Options - Content Sharing Experience

Multipoint Calls on RMX	Content Sharing	People + Content
<b>Endpoints Registered to DMA</b>		
<i>HDX/ITP to HDX/ITP</i>	Yes	Yes
<i>HDX/ITP to Cisco CTS</i>	Yes	No
<i>Cisco CTS to HDX/ITP</i>	Yes	Yes
<b>Endpoints Registered to CUCM</b>		
<i>HDX/ITP to HDX/ITP</i>	Yes	No
<i>HDX/ITP to Cisco CTS</i>	Yes	No,
<i>Cisco CTS to HDX/ITP</i>	No	No

- *H.239*
  - A variety of resolutions and frame rates are supported.  
For more information see "*H.239 / People+Content*" on page 3-2.
  - Can be used with *SIP* and *H.323* endpoints, desktop (*CMAD*), room systems (*HDX*) and *ITP* (*OTX, RPX*).
  - Not supported by *Lync* clients, *IBM* clients and *Cisco CTS* endpoints.
  - Cannot be used when *HDX* endpoints are registered to *CUCM*.
- *TIP*
  - The resolution is fixed at XGA at 5fps.
  - Supported on *HDX*, *Polycom ITP* and *Cisco CTS* systems.
- The following content compatibility options are available:
  - **Tip not enabled** – *CTS* cannot join the conference, all other endpoints can share *H.239* content.
  - **TIP video compatibility** – *CTS* receives people video, all other endpoints can share *H.239* content.
  - **TIP video and content compatibility** – *CTS* and *HDX* can share *TIP* content, all other endpoints receive only the people video.

For more information see "Procedure 4: Configuring a TIP Enabled Profile on the RMX" on page 1-96.

## Cisco Equipment

To configure the various *Cisco* entities the following procedures are required.

### CUCM

**3** Configure the *CUCM* to send and receive calls from the *H.323* network.

**a With Neighbored IOS and CMA Gatekeepers**

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "Configuring Cisco Unified Communications Manager for H.323".

**b With CMA Gatekeeper**

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "Configuring Cisco Unified Communications Manager for H.323".

**c With IOS Gatekeeper**

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "Configuring Cisco Unified Communications Manager for H.323".

### IOS Gatekeeper

>> Set up zones and gateway type prefixes to enable dialing to DMA and RMX systems.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "Configuring the Cisco IOS Gatekeeper".

### IOS and CMA Gatekeepers (Neighbored)

>> Configure the *Cisco IOS Gatekeeper* for two separate zones.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "Configure the Cisco IOS Gatekeeper for use with a CMA System".

## Polycom Equipment

Table 3 lists the Polycom products supported within the various Deployment Architecture. Only RMX configurations are described in detail in this document.

Configuration procedures for all other solution components are described in the *Polycom Unified Communications Deployment Guide for Cisco Environments*. .

**Table 3** supported current Polycom products

Polycom TIP and SIP	Version(s)
Polycom DMA 7000 system	V4.0
Polycom RMX 2000 and 4000 systems	V7.6.x MPMx card are required.
Immersive Telepresence Systems: <ul style="list-style-type: none"> <li>RPX 200 and 400 systems</li> <li>OTX 300 system</li> <li>TPX HD 306 system</li> <li>ATX HD 300 system</li> </ul>	V3.0.3 Requires TIP option key. Requires Polycom Touch Control.

**Table 3** supported current Polycom products

HDX Systems: <ul style="list-style-type: none"> <li>7000 HD Rev C</li> <li>8000 HD Rev B</li> <li>9006</li> <li>4500</li> </ul>	V3.0.3 Requires TIP option key.
The following Polycom peripheral: <ul style="list-style-type: none"> <li>Polycom Touch Control</li> </ul>	1.3.0
<b>SIP ONLY (no TIP support)</b>	<b>Version(s)</b>
Spectralink wireless phones 8020/8030	
Polycom VVX 1500	V4.0
Polycom VVX 1500 C	V3.3.1
KIRK Wireless Server 300/600v3/6000	

The following procedures **1 - 16** are a summary of the configuration procedures. The detailed procedures **1 - 16** begin with “*Procedure 1: Set the MIN\_TIP\_COMPATIBILITY\_LINE\_RATE System Flag*” on page [94](#).

#### RMX

- 1 Set the **MIN\_TIP\_COMPATIBILITY\_LINE\_RATE** *System Flag*
- 2 Configuring the RMX to statically route outbound SIP calls to DMA or CUCM
- 3 Configuring the RMX’s H.323 Network Service to register with CMA gatekeeper
- 4 Configuring a TIP enabled Profile on the RMX
- 5 Configuring an Ad Hoc Entry Queue on the RMX if DMA is not used
- 6 Configuring a Meeting Room on the RMX
- 7 Configuring Participant Properties for dial out calls

#### DMA

If DMA is present in the configuration perform procedures **8** and **9**, otherwise skip to procedure **10**.

- 8 Configuring DMA to route SIP calls to CUCM
- 9 Configuring a Virtual Meeting Room (VMR)  
The procedures for configuring DMA are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

#### CMA

- 10 Configuring CMA to route H.323 calls to RMX
- 11 Configuring CMA for use with Cisco IOS Gatekeeper (Neighbored)
- 12 Configuring CMA to route H.323 calls to CUCM
- 13 Configuring CMA to route non-H.323 calls to CUCM

The procedures for configuring CMA are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

## Endpoints

### 14 Configuring H.323 endpoints to register to the CMA or IOS gatekeeper

The procedures for configuring H.323 endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

### 15 Configuring SIP endpoints to register to:

- a DMA as SIP Proxy
- b CUCM as SIP Proxy

The procedures for configuring SIP endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

### 16 Configuring TIP endpoints to register to:

- a DMA
- b CUCM

The procedures for configuring TIP-enabled endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

## Procedure 1: Set the MIN\_TIP\_COMPATIBILITY\_LINE\_RATE System Flag

The **MIN\_TIP\_COMPATIBILITY\_LINE\_RATE** System Flag determines the minimum line rate at which an *Entry Queue* or *Meeting Room* can be TIP enabled.

CTS version 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 *RMX1500/2000/4000 Administrator's Guide*, "Modifying System Flags" on page [21-1](#).

## Procedure 2: Configuring RMX to statically route outbound SIP calls to DMA or CUCM

- 1 In the *IP Network Services Properties* dialog box, click the **SIP Servers** tab.
- 2 In the *SIP Server* field, select **Specify**.
- 3 In the *SIP Server Type* field, select **Generic**.
- 4 Set *Refresh Registration every* **3600** seconds.
- 5 If not selected by default, change the *Transport Type* to **TCP**.
- 6 In the *SIP Servers* table:
  - a Enter the IP address of the DMA or CUCM in both the *Server IP Address or Name* and *Server Domain Name* fields.
  - b The *Port* field must be set to its default value: **5060**. DMA and CUCM use this port number by default.
- 7 In the *Outbound Proxy Servers* table:
  - a Enter the IP address in the *Server IP Address or Name* field. (The same value as entered in Step 6a.)

- b The *Port* field must be set to its default value: **5060**.  
(By default, the *Outbound Proxy Server* is the same as the *SIP Server*.)

**IP Network Service Properties**

Network Service Name: IP Network Service

IP Network Type: H.323 & SIP

SIP Server: Specify

SIP Server Type: Generic

Refresh Registration every: 3600 seconds

Transport Type: TCP Create Certificate

Certificate Method: CSR Send Certificate

SIP Servers:

Parameter	Primary Server	Alternate Server
Server 1	10.226.24.10	
Port	5060	

Outbound Proxy Servers:

Parameter	Primary Server
Server 1	10.226.24.10
Port	5060

OK Cancel

When configuring *RMX* to statically route *SIP* calls to *DMA* or *CUCM*, it is important to also configure the *RMX*'s *H.323 Network Service* to register with *CMA* gatekeeper. For more information see "Procedure 3: Configuring the *RMX*'s *H.323 Network Service* to register with *CMA* gatekeeper" on page 1-95.

### Procedure 3: Configuring the *RMX*'s *H.323 Network Service* to register with *CMA* gatekeeper

- 1 In the *IP Network Services Properties* dialog box, click the **Gatekeeper** tab.
- 2 In the *MCU Prefix in Gatekeeper* field, enter the prefix that the *RMX* uses to register with the gatekeeper.

**IP Network Service Properties**

Network Service Name: IP Network Service

IP Network Type: H.323 & SIP

Gatekeeper: Specify

Primary Gatekeeper

IP Address or Name: 172.22.185.157

Backup Gatekeeper

IP Address or Name:

MCU Prefix in Gatekeeper: 1562

☐ Register as Gateway

Service Mode: board\_hunting

Refresh Registration every: 120 seconds

Aliases:

Alias	Type
	None
	None
	None
	None
	None

## Procedure 4: Configuring a TIP Enabled Profile on the RMX

*TIP* enabled profiles must be used for the *Entry Queues* and *Meeting Rooms* defined on the RMX. (Different *Profiles* can be assigned to *Entry Queues* and *Meeting Rooms*, however they must be *TIP* enabled.)

- 1 Create a *New Profile* for the *Meeting Room*. For more information see the *RMX1500/2000/4000 Administrator's Guide*, "Defining Profiles" on page 1-10.
- 2 In the *New Profile - General* tab, set the *Line Rate* to a value of at least that specified for the **MIN\_TIP\_COMPATIBILITY\_LINE\_RATE** *System Flag* in *Procedure 1*.

The screenshot shows the 'New Profile' window with the 'General' tab selected. The 'Display Name' field contains 'TIPCon'. The 'Line Rate' dropdown menu is open, showing '1024 Kbps' selected. The 'Routing Name' field is empty. In the 'Video Switching' section, the 'H.264 720p30' option is selected. The 'Operator Conference' checkbox is unchecked.

- 3 Click the *Advanced* tab.

The screenshot shows the 'New Profile' window with the 'Advanced' tab selected. The 'Display Name' field is empty. The 'Line Rate' dropdown menu is open, showing '384 Kbps' selected. The 'Encryption', 'LPR', and 'Auto Terminate' checkboxes are checked. The 'Before First Joins' field is set to '10' and 'At the End' is set to '1', both with 'Minutes' as the unit. The 'After last participant quits' radio button is selected. The 'Auto Redialing' checkbox is unchecked. The 'TIP Compatibility' dropdown menu is open, showing 'video\_and\_content' selected.

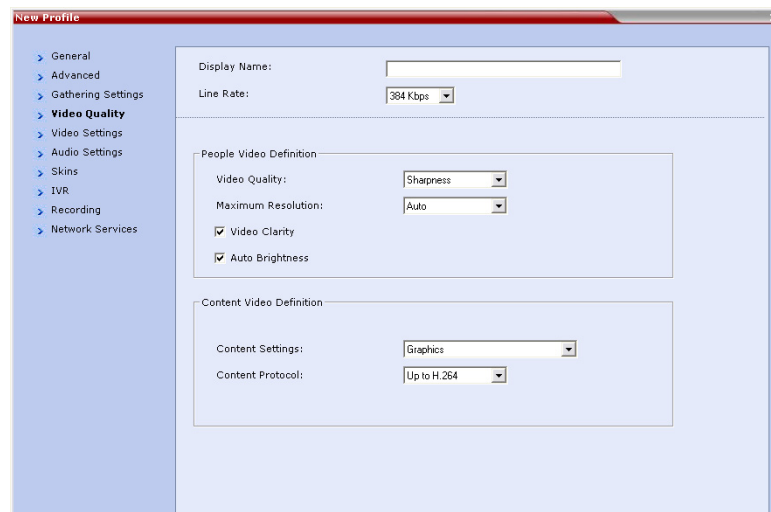
- 4 Select the *TIP Compatibility* mode. The *TIP Compatibility* mode affects in the user *Video* and *Content* experience as described in Table 1-1

**Table 1-1** *TIP Compatibility Mode*

TIP Compatibility Mode	Endpoint Type	
	HDX / ITP	CTS
None	People Video (up to 1080p30)  H.239 P+C	-
Video Only	People Video (up to 1080p30)  H.239 P+C	People Video (up to 1080p30)
Video & Content	People video (up to 1080p30)  Content (XGA 5fps)	People Video (up to 1080p30)  Content (XGA 5fps)

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

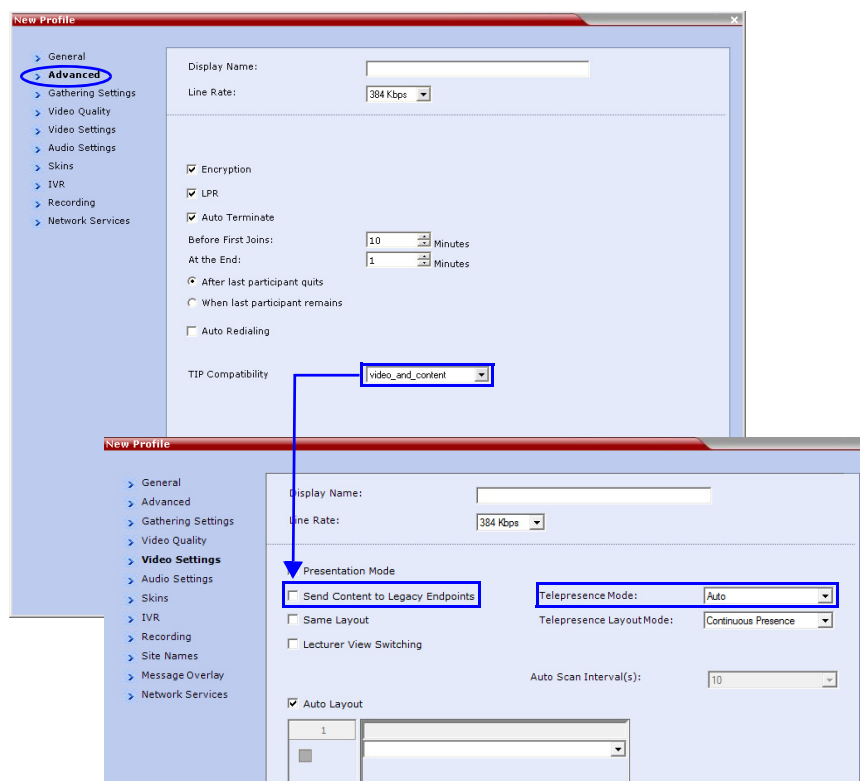
- 5 Click the *Video Quality* tab.



*Content Settings* is disabled if *TIP Compatibility* is set to **Video and Content** in the *Advanced* tab.

- 6 Click the *Video Settings* tab.

If the *TIP Compatibility Mode* was set to **Video and Content**, the *Send Content to Legacy Endpoints* disabled. This setting cannot be changed.



- 7 Set the *Telepresence Mode* to **Auto**.
- 8 Assign the *New Profile* to the *Meeting Room*. For more information see the *RMX1500/2000/4000 Administrator's Guide*, "Creating a New Meeting Room" on page 5-4.

### Procedure 5: Configuring an Ad Hoc Entry Queue on the RMX if DMA is not used

You must discuss the selection of the appropriate Profile for this EQ, as this Profile will be used to create the conferences on the RMX and they must be TIP enabled.

- 1 Create or select the *Entry Queue* as described in the *RMX 1500/2000/4000 Administrator's Guide*, "Entry Queues" on page 6-1.



- 2 In the *New Entry Queue* or *Entry Queue Properties* dialog box, ensure that **Ad Hoc** is selected.

The screenshot shows the 'New Entry Queue' dialog box. The 'Ad Hoc' checkbox is checked and highlighted with a blue rectangle. Other fields include 'Display Name' with the value 'SUPPORT\_2062483538', 'Routing Name', 'Profile' set to 'Factory\_Video\_Profile', 'ID', 'Entry Queue IVR Service', 'Cascade' set to 'None', and 'ISDN/PSTN Dial-in' options.

- 3 Ensure that the *Entry Queue* is designated as the **Transit Entry Queue** as described in the *RMX 1500/2000/4000 Administrator's Guide*, "Setting a Transit Entry Queue" on page 6-6.

The screenshot shows the RMX Management interface. The 'Entry Queues (5)' list is visible, showing entries like POLYCOM\_206563475, SUPPORT\_474611447, and DefaultEQ. The 'DefaultEQ' entry is selected, and a context menu is open with the option 'Set Transit EQ' highlighted.

Name	Status	ID	Start Time	End Time
SUPP		65412	12:21 P	1:21
POLY	Singl	78323	1:12 PM	2:12
HD_C		64332	6:51 AM	10:5

Name	ID	Profile
POLYCOM_206563475	08458	DefaultVideo384
SUPPORT_474611447	00682	DefaultVideo384
DefaultEQ	1000	DefaultVideo384
Link_In EQ		
HD_EQ		

## Procedure 6: Configuring a Meeting Room on the RMX

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

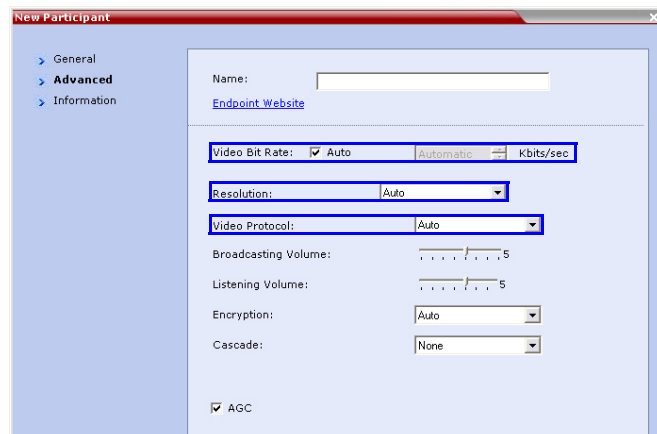
For more information see the *RMX1500/2000/4000 Administrator's Guide*, "Creating a New Meeting Room" on page 5-4.

## Procedure 7: Configuring Participant Properties for dial out calls

*Participant Properties* must be configured to ensure that defined participants inherit their *TIP* settings from the *Profile* assigned to the *Meeting Room*.

- a Define the *New Participant's General* settings. For more information see the *RMX1500/2000/4000 Administrator's Guide*, "Adding a Participant to the Address Book" on page 7-3.

- b Click the *Advanced* tab.



- c Ensure that:

- *Video Bit Rate* is set to **Automatic** or at least equal to or greater than the value specified by the **MIN\_TIP\_COMPATIBILITY\_LINE\_RATE** *System Flag*.
- *Resolution* is set to **Auto** or at least **HD 720**.
- *Video Protocol* is set to **Auto** or at least **H.264**.

## Operations During Ongoing Conferences

Moving participants between TIP enabled meetings and non TIP enabled meetings is not possible.

## Monitoring CTS Participants

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.

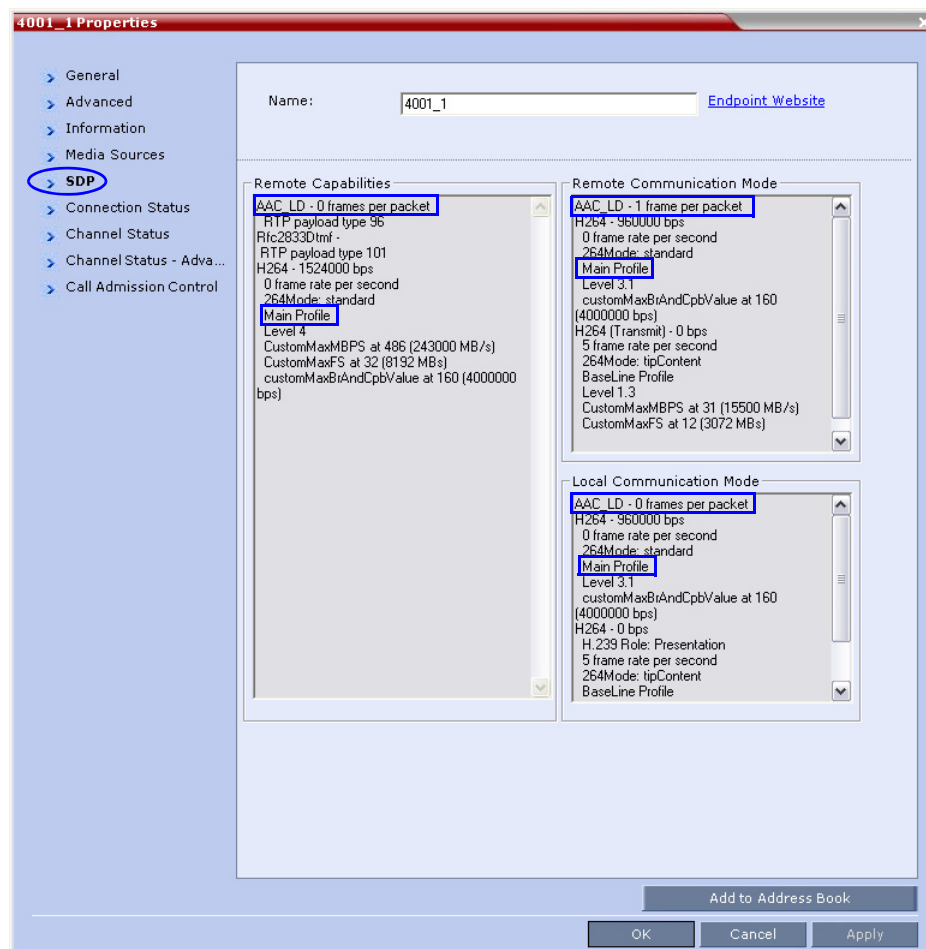
Participants (4/4)											
Name	Status	Role	IP Address	Alias Na	Network	Dialing Di	Audio	Video	Encryptio	Service N	FECC Tok
SUPPORT_419473727 (4 participants)											
1502_1	Connected		0.0.0.0	1502@1	SIP	Dial o				IP Netw	
1502_aux	Connected		0.0.0.0	1502@1	SIP	Dial o				IP Netw	
1502_3	Connected		0.0.0.0	1502@1	SIP	Dial o				IP Netw	
1502_2	Connected		0.0.0.0	1502@1	SIP	Dial o				IP Netw	

### Displaying Participants Properties:

- 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



The CTS Audio Auxiliary channel is used only for Content. In all other cases, the bit rate shown in the *Properties - Channel Status* dialog box for this channel is 0.

## SirenLPR

*SirenLPR* prevents audio degradation and maintains high audio quality if packet loss occurs.

The *SirenLPR* audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications.

### Guidelines

- Supported only in MPMx Card Configuration Mode.
- Available for Polycom CMAD and HDX “Canyon 3.0.1” endpoints.
- The recovery quality is impacted by percentage of packet loss. At higher packet loss percentages, recovery may be incomplete.
- *SirenLPR* is supported for Mono Audio at audio line rates of: 32Kbps, 48Kbps and 64Kbps.  
It is not supported for Mono Audio at audio line rates of: 24Kps, 96Kbps and 128Kbps.
- *SirenLPR* is supported for Stereo Audio at audio line rates of: 64Kbps, 96Kbps and 128Kbps.
- *SirenLPR* is enabled (default) or disabled by a system flag: **ENABLE\_SIRENLPR**.  
Flag values: YES (default)/NO.
- *SirenLPR* audio algorithm is supported only in IP calls.
- *SirenLPR* is available in all conference types.

### SIP Encryption

The **ENABLE\_SIRENLPR\_SIP\_ENCRYPTION** *System Flag* enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol.

The default value of this flag is **NO** meaning *SirenLPR* is disabled by default for *SIP* participants in an encrypted conference. To enable *SirenLPR* the *System Flag* must be added to *system.cfg* and its value set to **YES**.

## Auto Scan and Customized Polling in Video Layout

*Auto Scan* enables a user to define a single cell in the conference layout to cycle the display of participants that are not in the conference layout.

*Customized Polling* allows the cyclic display to be set to a predefined order for a predefined time period. The cyclic display only occurs when the number of participants is larger than the number of cells in the layout.

### Guidelines

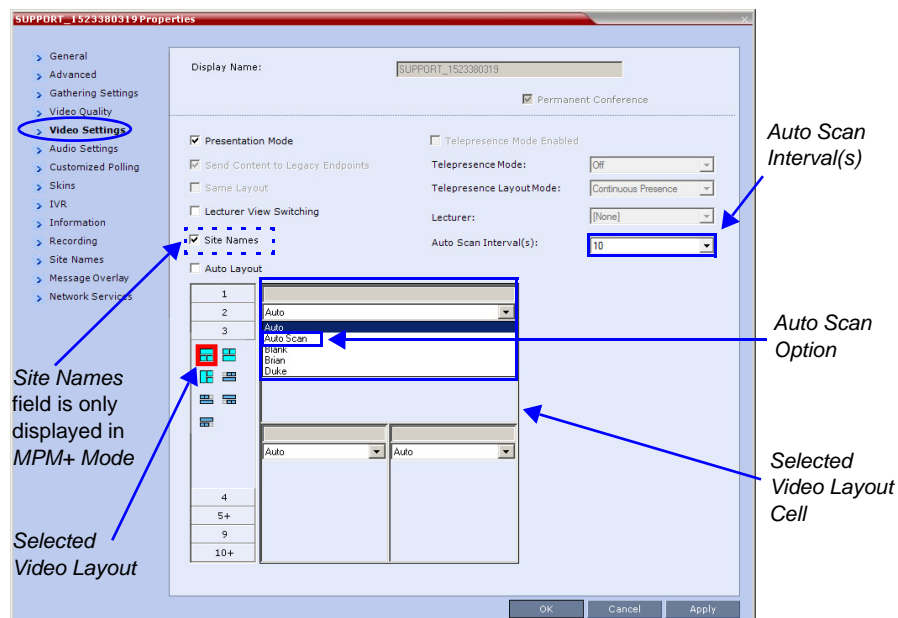
- *Auto Scan* and *Customized Polling* can only be enabled during an ongoing conference.

## Enabling Auto Scan and Customized Polling

### Auto Scan

To enable *Auto Scan*:

- 1 In the *RMX Web Client Main Screen - Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.
- 2 In the *Conference Properties - General* dialog box, click **Video Settings**. The *Video Settings* tab is displayed.

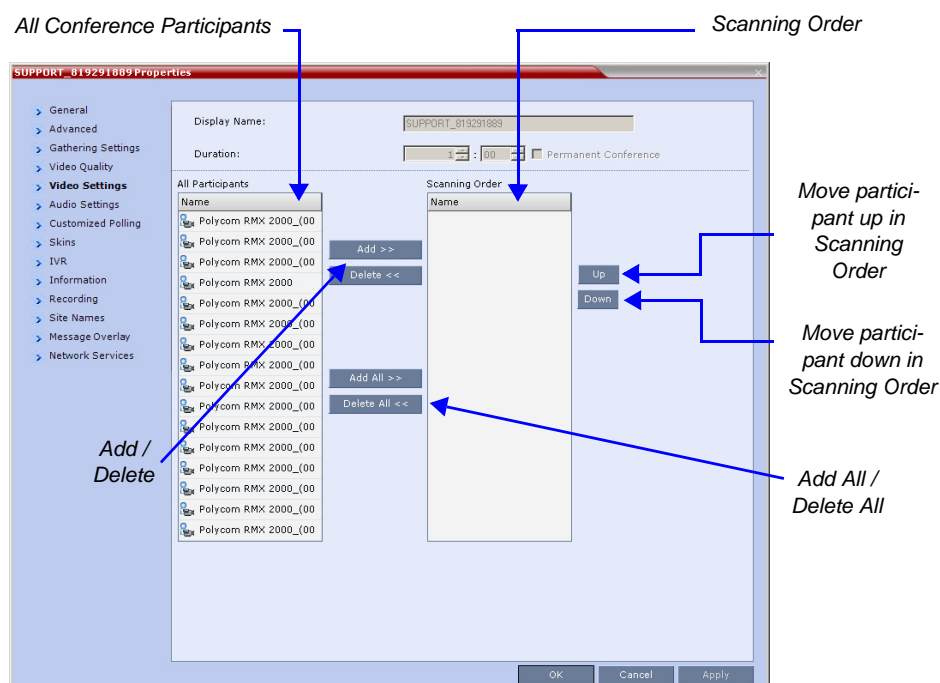


- 3 In the video layout cell to be designated for *Auto Scan*, click the drop-down menu button and select **Auto Scan**.
- 4 Select from the *Auto Scan Interval(s)* drop-down list the scanning interval in seconds.
- 5 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.  
-or-  
Click **OK** to confirm and close the *Conference Properties* dialog box.

## Customized Polling

The order in which the Auto Scanned participants are displayed in the *Auto Scan* enabled cell of the video layout can be customized.

- 1 Open the *Customized Polling* tab:
  - a If the *Video Settings* tab is open click the **Customized Polling** tab.
  - or
  - b In the *Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.
  - c In the *Conference Properties - General* dialog box, click **Customized Polling**.  
The *Customized Polling* tab is displayed.



All conference participants are listed in the left pane (*All Participants*) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (*Scanning Order*).

The dialog box buttons are summarized in Table 1-2.

**Table 1-2** Customized Polling - Buttons

Button	Description
<i>Add</i>	Select a participant and click this button to <i>Add</i> a the participant to the list of participants to be Auto Scanned. The participants name is removed from the <i>All Participants</i> pane.
<i>Delete</i>	Select a participant and click this button to <i>Delete</i> the participant from the list of participants to be <i>Auto Scanned</i> . The participants name is moved back to the <i>All Participants</i> pane.

**Table 1-2** Customized Polling - Buttons

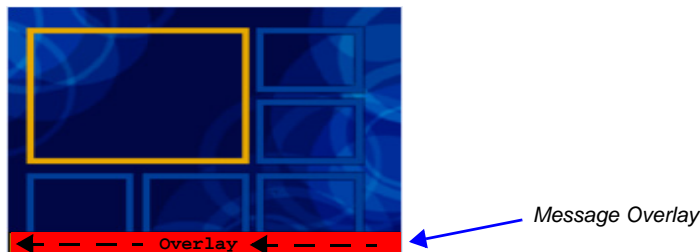
Button	Description
<i>Add All</i>	Add all participants to the list of participants to be <i>Auto Scanned</i> . All participants' names are removed from the <i>All Participants</i> pane.
<i>Delete All</i>	Delete all participant from the list of participants to be <i>Auto Scanned</i> . All participants' names are moved back to the <i>All Participants</i> pane.
<i>Up</i>	Select a participant and click this button to move the participant <i>Up</i> in the <i>Scanning Order</i> .
<i>Down</i>	Select a participant and click this button to move the participant <i>Down</i> in the <i>Scanning Order</i> .

- 2 **Optional.** Add a participant to the list of participants to be *Auto Scanned*:
  - a Click on the participant's name in the *All Participants* list.
  - b Click the **Add** button to move the participant to the *Scanning Order* pane.
- 3 **Optional.** Delete a participant from the list of participants to be *Auto Scanned*:
  - a Click on a participant's name in the *Scanning Order* list.
  - b Click the **Delete** button to move the participant back to the *All Participants* pane.
- 4 **Optional.** Add all participants to the list of participants to be *Auto Scanned*:
  - Click the **Add All** button.
- 5 **Optional.** Delete all participant from the list of participants to be *Auto Scanned*:
  - Click the **Delete All** button.
- 6 **Optional.** Move the participant up in the *Scanning Order*:
  - Click the **Up** button.
- 7 **Optional.** Move the participant down in the *Scanning Order*:
  - Click the **Down** button.
- 8 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.  
or  
Click the **OK** the button to confirm and return to the *RMX Web Client Main Screen*.

## Participant Message Overlay

*Participant Message Overlay* allows messages to be sent to participants during an ongoing conference. The Operator/Administrator can send a text message to a single participant or a selected number of participants during a conference. The text message is seen as part of the video information on screen or on a desktop display.

*Participant Message Overlay* supports a Unicode or ASCII characters per language but the numbers for each language can differ due to the type of font used. For example, the available number of Unicode/ASCII characters in Chinese is 32 and 48 for Russian.



## Guidelines

- *Participant Message Overlay* is supported in:
  - Continuous Presence (CP) conferences
  - in *Same Layout* mode
  - in encrypted conferences
- *Participant Message Overlay* is not supported in *Lecture* mode.
- Participants that have their video suspended do not receive *Message Overlays*.
- *Participant Message Overlays* cannot be sent via the *Content* channel.
- *Participant Message Overlay* is not displayed when the *PCM* menu is active.
- In some languages, for example Russian, when large font size is selected, rolling messages may be truncated if the message length exceeds the resolution width.
- Overlay Messages are overwritten when an additional or new *Conference* or *Participant Message Overlay* is sent.

## Enabling the Participant Message Overlay

*Participant Message Overlays* are created and activated in the *Participant Properties – Message Overlay* dialog box.



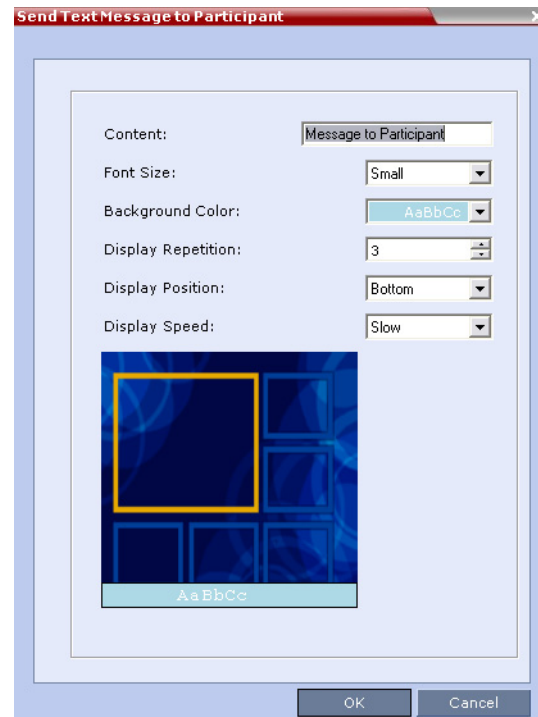
A single participant or a number of participants can be selected.

### To enable Participant Message Overlay:

- 1 In the *Participant List* pane, choose a participant or a number of participants (by pressing Ctrl+click).
- 2 Right-click and select **Send Text Message to Participant**.



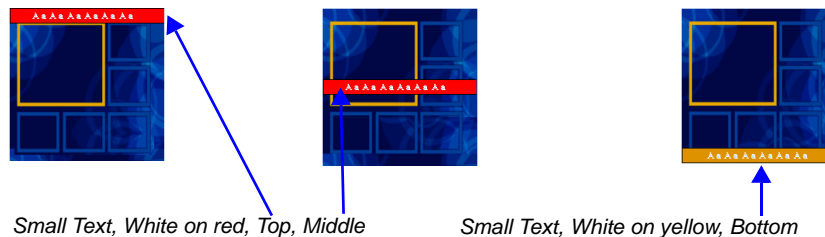
The *Message Overlay* window is displayed.



**3** Modify the following fields as set out in Table 1-6.

As the fields are modified the *Preview* changes to show the effect of the changes.


**For example:**



**Table 1-3** Conference Properties - Message Overlay

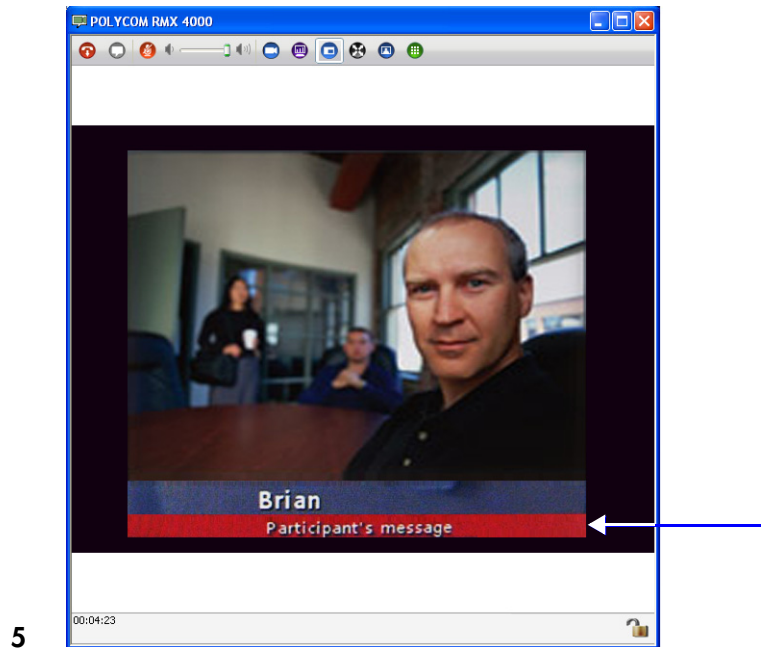
Field	Description
<i>Content</i>	Supports a maximum of 24 Unicode or 48 ASCII characters per language but the numbers for each language can differ due to the type of font used. For example, the available number of characters in Chinese is 32 and 48 for Russian.

**Table 1-3** Conference Properties - Message Overlay (Continued)

Field	Description
Font Size	<p>Select the size of the Message Overlay text from the drop-down menu options:</p> <ul style="list-style-type: none"> <li>• Small</li> <li>• Medium</li> <li>• Large</li> </ul> <p><b>Default:</b> Small</p> <p><b>Note:</b> In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.</p>
Color	<p>Select the color of the text and background of the Message Overlay from the following drop-down menu options:</p>  <p><b>Default:</b> White text on pale blue background</p>
Display Repetition	<p>Click the arrows (↔) to increase or decrease the number of times that the Message Overlay is to be repeated.</p> <p><b>Default:</b> 3</p>
Display Position	<p>Select the position for the display of the Message Overlay on the endpoint screen:</p> <ul style="list-style-type: none"> <li>• Top</li> <li>• Middle</li> <li>• Bottom</li> </ul> <p><b>Default:</b> Bottom</p>
Display Speed	<p>Select whether the Message Overlay is static or repeating:</p> <ul style="list-style-type: none"> <li>• Slow</li> <li>• Fast</li> </ul> <p><b>Default:</b> Slow</p>

- 4 Click the **OK** button.

A banner appears at the bottom of the participant's desktop video display.



The Participant's message banner *Display Position* shown here is the *Bottom* selection. The message can also appear at the *Top* or in the *Middle* of the window.

## Microsoft Call Admission Control (CAC) Support

Microsoft Call Admission Control (CAC), a protocol that enables bandwidth management via the Policy Server in federated (ICE) environment, is supported on the RMX.

The Policy server functionality enables the Lync server to manage the bandwidth allocated to the Lync client when connecting to another Lync client or a video conference running on the RMX. The bandwidth allocated by the Policy server may be the same or lower than the bandwidth requested by the Lync client, which is based on the line rate of the conference.

### Guidelines

- Microsoft CAC is available only with:
  - A Lync server (Wave 14)
  - Call Policy functionality enabled
  - The Call Admission Control enabled for the Lync Clients
  - ICE environment
  - Local network
  - RMX MPM+ and MPMx Card Configuration Modes
- Microsoft CAC is applicable only to dial-in calls
- Additional configuration on the Microsoft side is not required. It is based on the existing ICE environment configuration.
- Additional configuration (setting a system flag) may be required on the RMX to modify the system behavior when CAC is enabled in a local network; closing the ICE channel or keeping it open.
- Setting an additional system flag may be required on the RMX when running Video Switching conferences.

### RMX Configuration for CAC Implementation

To enable the Call Admission Control implementation in the RMX, you must manually add the flag **CAC\_ENABLE** to the System Configuration and set its value to **YES**.

In addition, when Call Admission Control is enabled in the local network, by default the local the ICE channel is closed after applying CAC bandwidth management.

This behavior can be changed so the ICE channel is preserved open throughout the call by manually adding the flag to *System Configuration*

**PRESERVE\_ICE\_CHANNEL\_IN\_CASE\_OF\_LOCAL\_MODE** and changing the its value to **YES**.

### Conferencing Behavior

#### Continuous Presence Conferences

In Continuous Presence conference, Lync clients connect with any allocated bandwidth.

#### Video Switching Conferences

In Video Switching conferences, Lync clients must connect with the same line rate as the conference, otherwise they will be connected as Secondary (Audio Only) participants.

Mitigation of the line rate requirement can be effected by modifying the system flag:  
**VSW\_RATE\_TOLERANCE\_PERCENT.**

This system flag determines the line rate tolerance.

Possible values are: **0 - 75.**

Setting this flag to **0** (0% - default) determines no line rate tolerance and the participant must connect at the conference line rate.

Setting this flag to a value between 1 and 75 determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference.

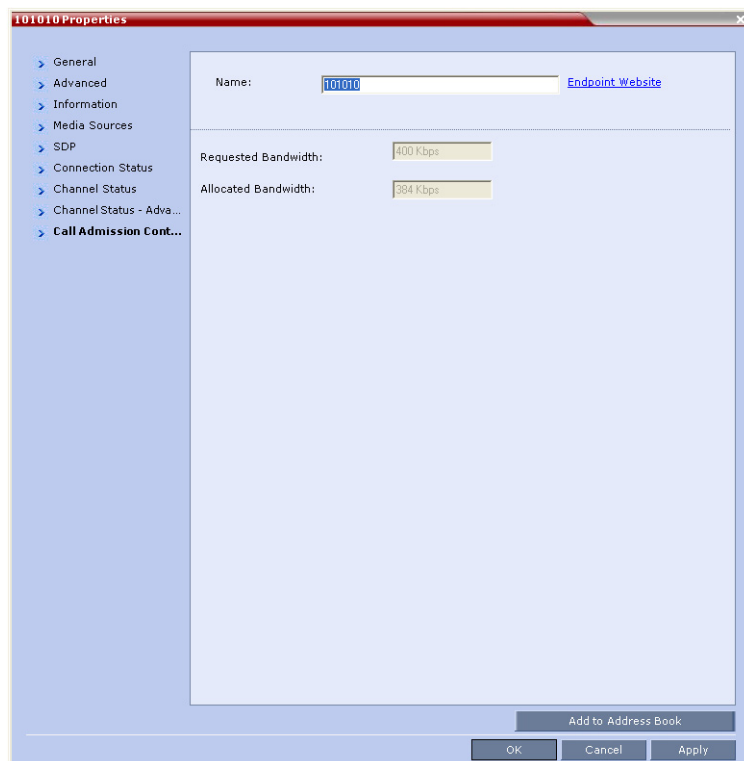
For example, if you enter 20 (for 20%) as the flag value, the participant will be able to connect to the conference if the allocated line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). If the conference line rate is 1024Kbps, participant with a line rate between 819Kbps and 1024Kbps will be able to connect to the conference.

When a tolerance is set, the Highest Common mechanism is enabled for the conference line rate. When a participant with a lower line rate connects to the conference, the line rate of all other connected participants is reduced accordingly and when that participant disconnects from the conference, the line rate of the remaining participants is increased to the highest possible rate common to all connected participants.

For example, if a participant with a line rate of 900Kbps connects to the conference to which all other participants are connected at a line rate of 1024kbps, the line rate of all participants will decrease to 900Kbps. When this participant disconnects, the line rate of the remaining participants will increase to 1024Kbps.

## Monitoring Participant Connections

Activation of the Call Admission Control for a call can be viewed in the *Participant Properties* - *Call Admission Control* dialog box.



This information applies only to dial-in participants.  
The following information is available:

**Table 1-4** Participant Properties - Call Admission Control Parameters

Field	Description
<i>Requested Bandwidth</i>	Indicates the bandwidth requested by the Lync client (usually the line rate set for the conference). NA - indicates that <i>Call Admission Control is disabled</i> .
<i>Allocated Bandwidth</i>	The actual bandwidth allocated by the Lync Policy Server. NA - indicates that <i>Call Admission Control is disabled</i> .

## SIP Proxy Failover With Polycom® Distributed Media Application™ (DMA™) 7000

*RMX* systems that are part of a *DMA* environment can benefit from *DMA*'s *SIP Proxy Failover* functionality.

*SIP Proxy Failover* is supported in *DMA*'s *Local Clustering* mode with redundancy achieved by configuring two *DMA* servers to share a single virtual *IP* address.

The virtual *IP* address is used by the *RMX* as the *IP* address of its *SIP Proxy*.

No additional configuration is needed on the *RMX*.

### **Should a SIP Proxy failure occur in one of the DMA servers:**

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

## Safe Software Version Installation

A safety mechanism has been added to RMX to ensure that a viable and safe software version installation is selected on an RMX. At the start of 7.6/7.6.1 software upgrade/downgrade, the safety mechanism ensures that the current RMX software version and the new software installation is matched to an internal logic table, and enables or rejects the software installation.

The user is able to control this mechanism by enabling or disabling the feature using the ENFORCE\_SAFE\_UPGRADE flag. Based on flag settings, the user may receive a notification or a warning when initializing an RMX version upgrade or downgrade. When the flag is enabled, if a viable upgrade/downgrade path is chosen no warning or notification is activated on the system. However, when an incorrect or non viable version upgrade/downgrade is attempted, an alarm and fault are activated on the RMX.

The ENFORCE\_SAFE\_UPGRADE flag has two possible values:

- **YES (Default)** - This flag setting enables the RMX system to notify users when an incorrect version upgrade/downgrade or upgrade/downgrade path is selected. The version upgrade/downgrade is rejected and the software installation does not continue. The upgrade/downgrade process aborts and a fault is activated on the RMX system: "Upgrade/downgrade rejected. Upgrade/downgrade from [current version] to a [new version] is not supported. For a list of valid upgrades and downgrades, refer to RMX documentation." For example, a fault is activated when a user attempts to upgrade from version 4.1.1 to 7.1, this an incorrect upgrade path since an intermediate upgrade from 4.1.1 version to 5.0.2 is required. In this example the version upgrade is rejected and the software installation does not continue.
- **NO** - When the safe software version installation flag value is NO, after initiating an upgrade or downgrade software installation, the RMX activates a fault alert in the *Faults List*: "Warning: Upgrade started and SAFE Upgrade protection is turned OFF". There is no other notification mechanism to further inform the user and the upgrade process continues.

Table 1 shows a list of the software versions that are supported with the Safe Software Version Installation for version 7.6.1.

**Table 2** RMX Version Software Version Upgrade/Downgrade Support for version 7.6.1

Software Version	1500X	1500Q	RMX 2000 MPM	RMX 2000 MPM+/MPMx	RMX 4000 MPM+/MPMx
2.x	-	-	-	-	-
3.x	-	-	-	-	-
4.x	-	-	-	-	-
4.7.2	✓	-	-	✓	✓
5.x	-	-	-	-	-
6.x	-	-	-	-	-
7.0	-	-	-	-	-
7.0.x/7.0.2C	✓	-	-	✓	✓



**Table 2** RMX Version Software Version Upgrade/Downgrade Support for version 7.6.1

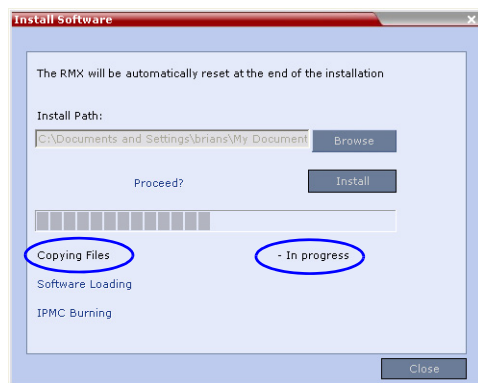
Software Version	1500X	1500Q	RMX 2000 MPM	RMX 2000 MPM+/MPMx	RMX 4000 MPM+/MPMx
7.1	✓	✓	-	✓	✓
7.2/7.2.x	✓	✓	-	✓	✓
7.5/7.5.1	✓	-	-	✓	✓
7.6/7.6.1	✓	✓	-	✓	✓

## Flag Settings

### Safe Software Version Installation Flag Enabled

When the safe software version installation flag ENFORCE\_SAFE\_UPGRADE value is YES, after initiating an upgrade or downgrade software installation, the RMX activates an active alarm and fault in the *Faults List*.

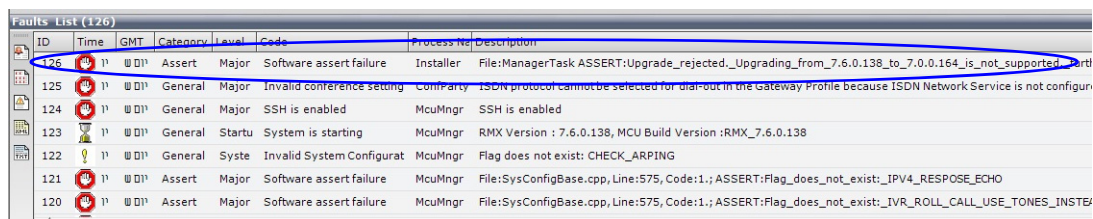
At the start of 7.6/7.6.1 software upgrade/downgrade procedure, the *Install Software* information box appears showing that the file copy is *In progress*.



When a non feasible software version upgrade path is selected, an RMX *Safe Software Version Installation* dialog box appears.



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

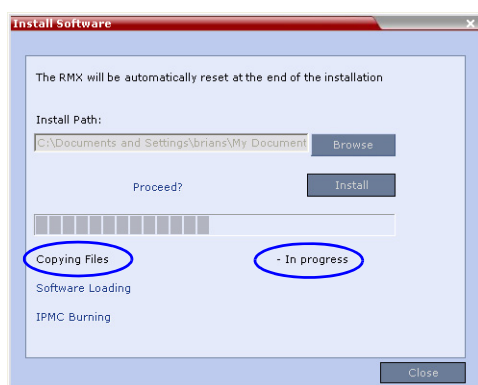


ID	Time	GMT	Category	Level	Code	Process	Description
126			Assert	Major	Software assert failure	Installer	File:ManagerTask ASSERT:Upgrade_rejected_Updating_from_7.6.0.138_to_7.0.0.164_is_not_supported_Part
125			General	Major	Invalid conference setting	ConfParty	ISDN protocol cannot be selected for dial-out in the Gateway Profile because ISDN Network Service is not configu
124			General	Major	SSH is enabled	McuMng	SSH is enabled
123			General	Startup	System is starting	McuMng	RMX Version : 7.6.0.138, MCU Build Version : RMX_7.6.0.138
122			General	System	Invalid System Configur	McuMng	Flag does not exist: CHECK_ARPING
121			Assert	Major	Software assert failure	McuMng	File:SysConfigBase.cpp, Line:575, Code:1.; ASSERT:Flag_does_not_exist_IPV4_RESPONSE_ECHO
120			Assert	Major	Software assert failure	McuMng	File:SysConfigBase.cpp, Line:575, Code:1.; ASSERT:Flag_does_not_exist_IVR_ROLL_CALL_USE_TONES_INSTE

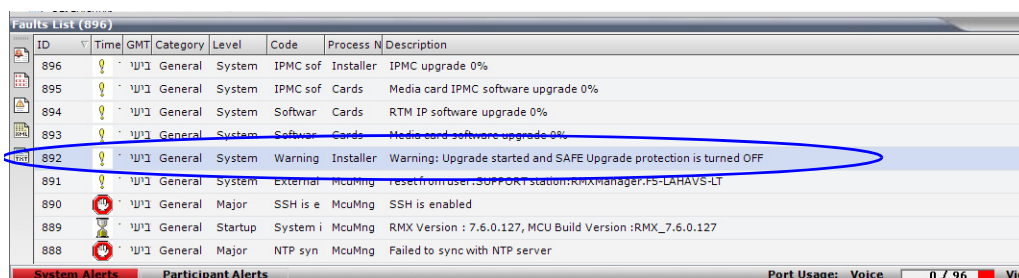
## Safe Software Version Installation Flag Disabled

When the safe software version installation flag `ENFORCE_SAFE_UPGRADE` value is NO, after initiating an upgrade or downgrade software installation, the RMX activates an fault alert in the *Faults List*.

At the start of 7.6/7.6.1 software upgrade/ downgrade procedure, the *Install Software* information box appears showing that the file copy is *In progress*.



The RMX then activates a fault alert in the *Faults List* as shown below.



ID	Time	GMT	Category	Level	Code	Process	Description
896			General	System	IPMC sof	Installer	IPMC upgrade 0%
895			General	System	IPMC sof	Cards	Media card IPMC software upgrade 0%
894			General	System	Softwar	Cards	RTM IP software upgrade 0%
893			General	System	Softwar	Cards	Media card software upgrade 0%
892			General	System	Warning	Installer	Warning: Upgrade started and SAFE Upgrade protection is turned OFF
891			General	System	External	McuMng	Reset from user: SUPPORT station: RMXmanager.FS-LAHAVS-LT
890			General	Major	SSH is e	McuMng	SSH is enabled
889			General	Startup	System i	McuMng	RMX Version : 7.6.0.127, MCU Build Version : RMX_7.6.0.127
888			General	Major	NTP syn	McuMng	Failed to sync with NTP server

There is no other notification mechanism to further inform the user and the software installation procedure continues.

# Version 7.6 Detailed Description - New Security Features

## (PKI) Public Key Infrastructure

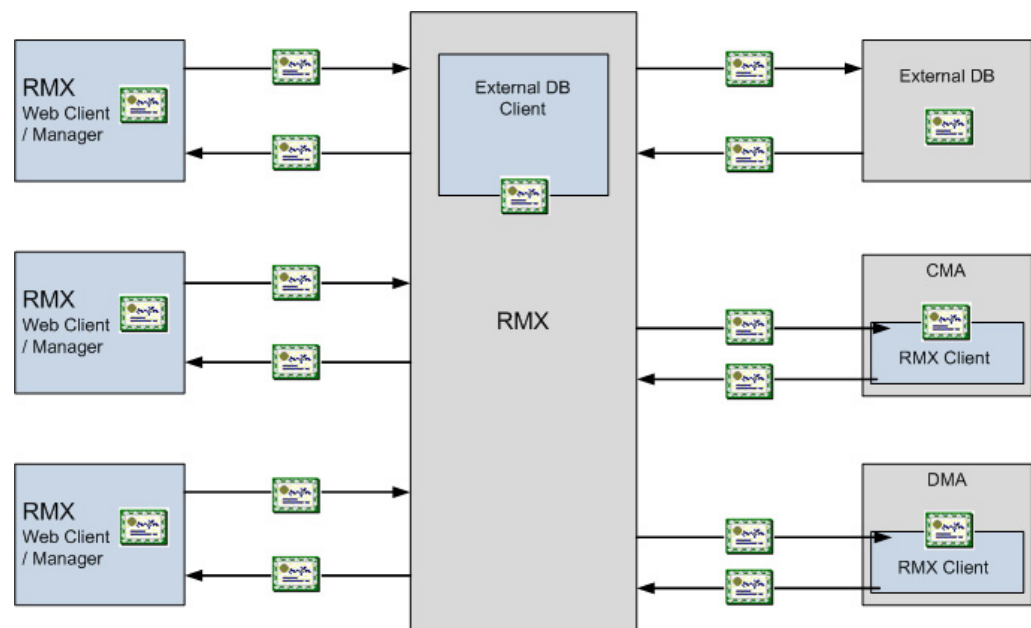
*PKI (Public Key Infrastructure)* is a set of tools and policies deployed to enhance the security of data communications between networking entities.

### Unique Certificates for all Networked Entities

The implementation of *PKI* on the *RMX* has been enhanced to ensure that all networked entities are checked for the presence of unique certificates by implementing the following rules and procedures during the *TLS* negotiation:

- The *RMX* identifies itself with the same certificate when operating as a server and as a client.
- The *RMX*'s management applications: *RMX Web Client* and *RMX Manager*, identify themselves with certificates.
- While establishing the required *TLS* connection, there is an exchange of certificates between all entities.
- Entities such as *CMA* and *DMA* that function as both client and server within the *Management Network* identify themselves with the same certificate for both their client and server functions.

The following diagram illustrates the certificate exchange during the *TLS* connection procedure.



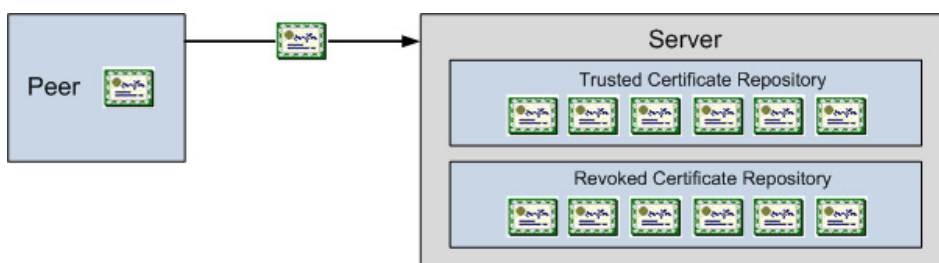
## Offline Certificate Validation

*Offline Certificate Validation* has been enhanced to include the following rules and procedures:

### Peer Certificates

The diagram below illustrates the peer certificate validation procedure.

- The credentials of each certificate received from a networked peer are verified against a repository of trusted certificates. (Each networked entity contains a repository of trusted certificates.)
- The digital signature of the certificate's issuing authority is checked along with the certificate's validity (expiration date).



### Self Validation of Certificates

- The *DNS* name field in the entity's certificate is checked for a match with the entity's *DNS* name.
- The date of the *RMX*'s certificate is checked for validity during power-up and when connecting to management applications (*RMX Web Client* and *RMX Manager*).

### Certificate Revocation List

- Each certificate received from a networked peer is verified against a repository of revoked certificates. (Each networked entity contains a repository of revoked certificates.)
- Revocation certificates are checked against a list of trusted issuers.
- The digital signature of the issuing authority of the revocation certificate is verified.

## Installing and Using Certificates on the RMX

The following certificate file formats are supported:

- *PEM*
- *DER*
- *PKCS#7/P7B*
- *PKCS#12/PFX*

## Default Management Network

The procedure necessary to purchase and install certificates for the *Default Management Network* of the RMX is unchanged and is described in the *RMX 1500/2000/4000 Administrator's Guide*, "Secure Communication Mode" on page [F-1](#).

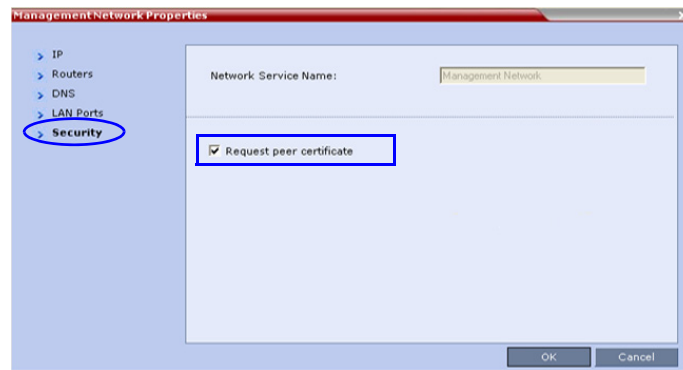
### Enabling Peer Certificate Requests

A new tab, *Security*, has been added to the *Management Network Properties* dialog box to enable the *Request Peer Certificate* feature to be enabled.

The *Request peer certificate* check box must be selected before enabling Secured Mode. If it is not selected an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.

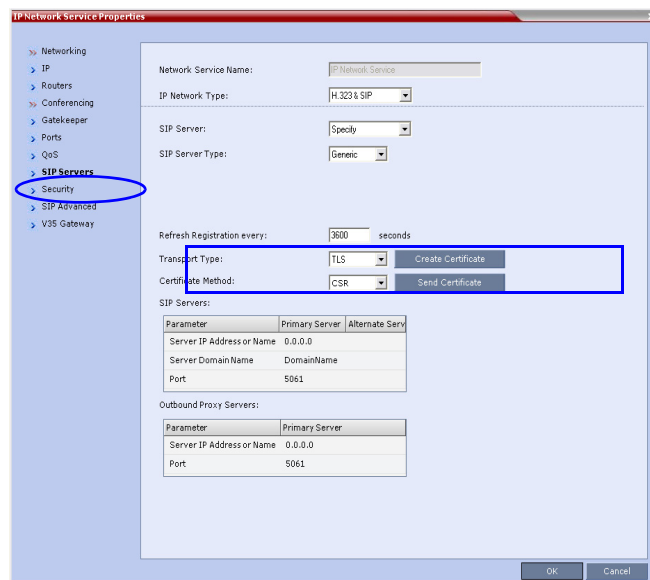
#### To enable Request Peer Certificate:

- 1 In the *RMX Management* pane, click the **IP Network Services** entry.
- 2 In the *IP Network Services* list pane, double-click the **Management Network** entry.
- 3 Click the **Security** tab.
- 4 Select the *Request Peer Certificate* check box.
- 5 Click the **OK** button.



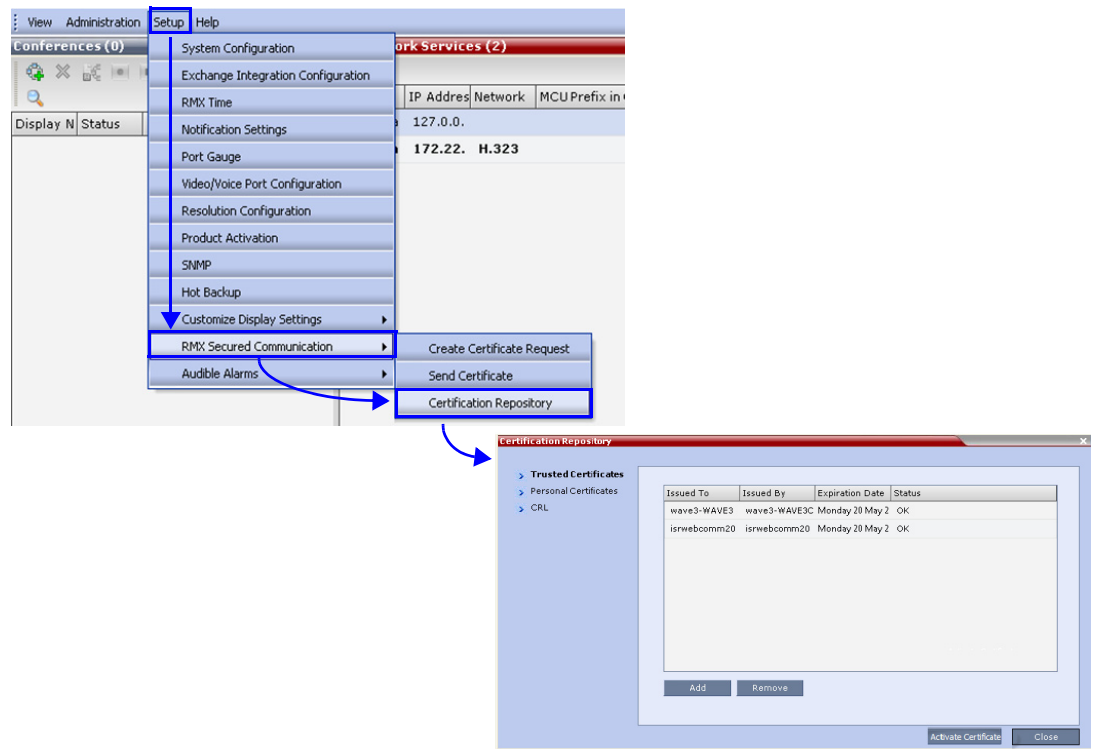
## Default IP Network Service

The steps needed to add a certificate to the *Default IP Network Service* are described in the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying the Default IP Network Service" on page 15-10.



## Managing Certificates in the Certification Repository

A *Certification Repository* dialog box has been added to enable the administrator to add remove and monitor certificates on the RMX. It is accessed via the *RMX Web Client / RMX Manager, Setup* menu.



For information about purchasing certificates see the *RMX 1500/2000/4000 Administrator's Guide*, "Purchasing a Certificate" on page **F-1**.

The *Certification Repository* dialog box contains tabs that display the following lists:

- *Trusted Certificates*
- *Personal Certificates (Management and Signaling Certificates)*
- *CRL (Certificate Revocation List)*

Double-clicking on a certificate in any of the displayed lists, displays the certificate's properties:



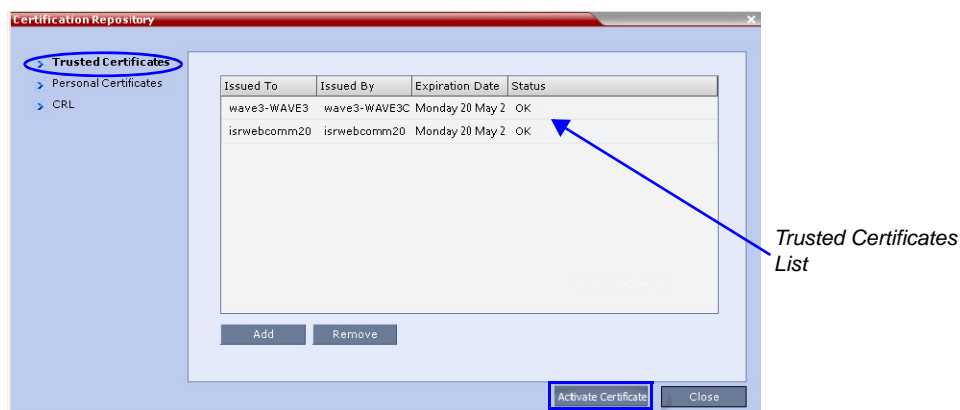
## Adding Trusted Certificates and CRLs to the Certification Repository

*Trusted Certificates* and CRLs added to the *Certification Repository* are not automatically activated. They remain in the *Trusted Certificates* and *CRL Lists* until the **Activate Certificate** button is clicked, at which time all *Trusted Certificates* and CRLs in the list are activated simultaneously.

## Trusted Certificates

By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*



## Adding Trusted Certificates

To add a certificate to the repository:

Repeat steps 1 - 4 for each certificate that is to be added to the *Certification Repository*.

- 1 In the *Trusted Certificates* tab click the **Add** button.



The *Send Certificate* dialog box is displayed.



**2** Send the certificate to the RMX.

Two options are available for sending the certificate to the RMX:

- **Paste Certificate and Send Certificate**  
Use this option if the certificate has been received from the *Certification Authority* in text format.
- **Send Certificate File**  
Use this option if the certificate has been received from the Certification Authority in file format.

**Option. Paste Certificate and Send Certificate**

After you have received the certificate from the *Certificate Authority*:

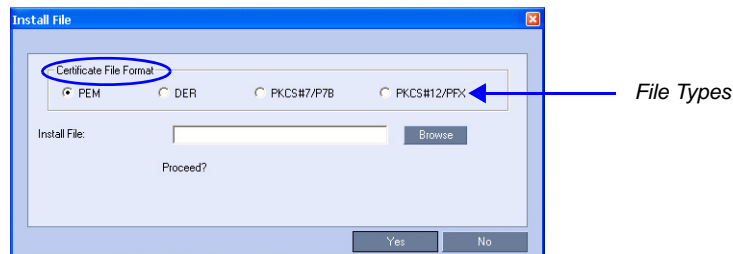
- a** **Copy (Ctrl + C)** the certificate information from the *Certificate Authority's* e-mail to the clipboard.
- b** Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.
- c** Click the **Send Certificate** button to send the certificate to the RMX.

### Option. Send Certificate File

After you have received the certificate file from the *Certificate Authority*:

- a Click **Send Certificate File**.

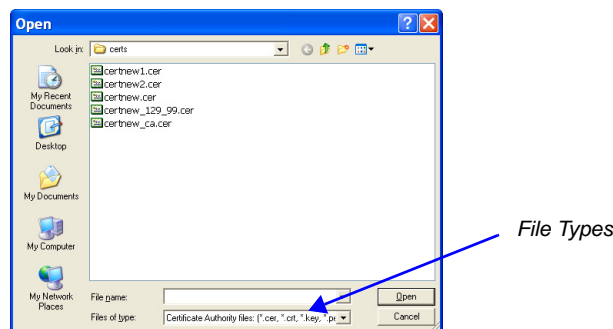
The *Install File* dialog box is displayed.



- b Select the *Certificate File Format*: PEM, DER, PKCS#7/P7B or PKCS#12/PFX.

- c Enter the certificate file name in the *Install File* field or click the **Browse** button.

The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.



- d Enter the certificate file name in the *File name* field or click to select the certificate file entry in the list.

- e Click the **Open** button.

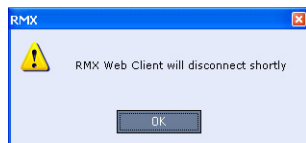
- f In the *Install File* dialog box, click the **Yes** button to proceed.

The certificate is added to the *Trusted Certificate List* in the *Certification Repository*.

- 3 If there are additional *Trusted Certificates* to be added to the *Certification Repository*, repeat steps 1 - 2, otherwise click the **Update Repository** button to complete *Trusted Certificate / CRL* installation.

Before clicking the **Activate Certificate** button ensure that all CRLs have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and CRLs are installed and the RMX displays an *RMX Web Client/Manager* disconnection confirmation dialog box.



- 4 Click **OK**.

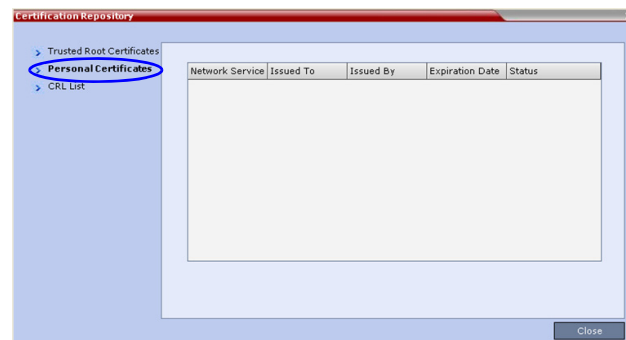
- 5 Login to the RMX to proceed with further management tasks.

## Personal Certificates (Management and Signaling Certificates)

Default Management and Default IP Network Service certificates can be viewed in the *Personal Certificates* tab.

They are listed alongside the service to which they are attached. By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Network Service*
- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*



## CRL (Certificate Revocation List)

A CRL contains a summary of the installed *Certificate Revocation Lists*.

By clicking the column headers the *Certificate Revocation List* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*



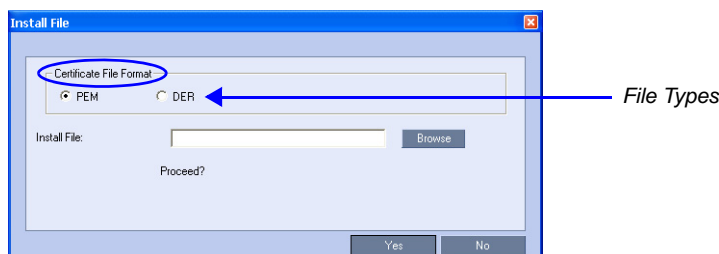
If the CRL List is not valid for any reason an *Active Alarm* is created and a message is displayed. The RMX Web Client/Manager connection to the RMX is not disabled.

## Adding a CRL

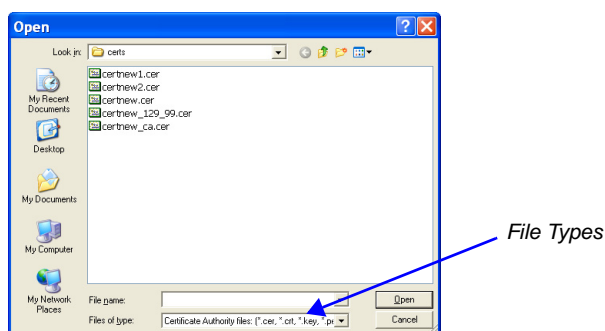
### To add a CRL to the repository:

Repeat steps 1 - 7 for each CRL that is to be added to the *Certification Repository*.

- 1 In the *CRL List* tab, click the **Add** button.
- 2 The *Install File* dialog box is displayed.



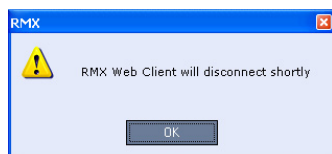
- 3 Select the *Certificate File Format*: PEM or DER.
- 4 Enter the certificate file name in the *Install File* field or click the **Browse** button.
- 5 The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.



- 6 Enter the *Certificate* file name in the *File name* field or click to select the certificate file entry in the list.
- 7 Click the **Open** button.
- 8 If there are additional CRLs to be added to the *Certification Repository*, repeat steps 1 - 7, otherwise click the **Activate Certificate** button to complete CRL / *Trusted Certificate* installation.

Before clicking the **Activate Certificate** button ensure that all *Trusted Certificates* have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and CRLs are installed and the RMX displays an *RMX Web Client/Manager* disconnection confirmation dialog box.



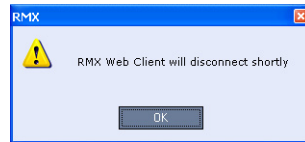
- 9 Click the **OK** button.
- 10 Login to the *RMX* to proceed with further management tasks

## Removing a CRL

To remove a CRL:

- 1 In the certificate list, select the *CRL List* to be removed.
- 2 Click the **Remove** button.

The certificate is removed and the *RMX* displays an *RMX Web Client/Manager* disconnection confirmation dialog box.



- 3 Click the **OK** button.
- Login to the *RMX* to proceed with further management tasks.

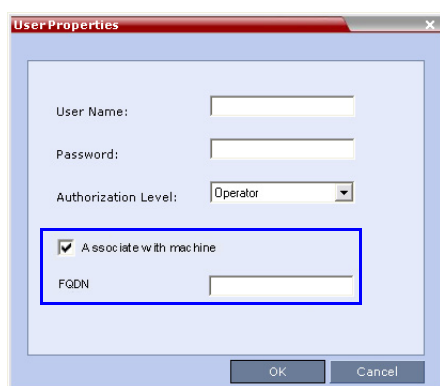
## Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.

For enhanced security reasons it is necessary for the RMX to process user connection requests in the same manner, whether they be from regular users accessing the RMX via the RMX Web Browser / RMX Manager or from *application-users* representing applications such as CMA and DMA.

Regular users can connect from any workstation having a valid certificate while *application-users* representing applications can only connect from specific servers. This policy ensures that a regular user cannot impersonate an *application-user* to gain access to the RMX in order to initiate an attack that would result in a *Denial of Service (DoS)* to the impersonated application.

A check box, *Associate with a machine* and a new field *FQDN (Fully Qualified Domain Name)* have been added to the *User Properties* dialog box.



The connection process for an *application-user* connecting to the RMX is as follows:

- 1 The *application-user* sends a connection request, including its *TLS* certificate, to the RMX.
- 2 The RMX searches its records to find the *FQDN* that is associated with the *application-user's* name.
- 3 If the *FQDN* in the received certificate matches that associated with *application-user*, and the password is correct, the connection proceeds.

### Guidelines

- *Application-users* are only supported when *TLS* security is enabled and *Request peer certificate* is selected. *TLS* security cannot be disabled until all *application-user* accounts have been deleted from the system.
- For *Secure Communications*, an administrator must set up on the RMX system a machine account for the CMA system with which it interacts. This machine account must include a fully-qualified domain name (*FQDN*) for the CMA system. This *FQDN* field on the RMX system is case-sensitive, so it must match the name in the CMA certificate (including case) exactly.
- *Application-user* names are the same as regular user names.  
**Example:** the CMA application could have an *application-user* name of CMA1.
- The *FQDN* can be used to associate all user types: *Administrator*, *Auditor*, *Operator* with the *FQDN* of a server.

- Multiple *application-users* can be configured the same *FQDN* name if multiple applications are hosted on the same server
- If the system is downgraded the *application-user's FQDN* information is not deleted from the *RMX's* user records.
- A *System Flag*, **PASS\_EXP\_DAYS\_MACHINE**, enables the administrator to change the password expiration period of *application-user's* independently of regular users. The default flag value is 365 days.
- The server hosting an *application-user* whose password is about to expire will receive a login response stating the number of days until the *application-user's* password expires. This is determined by the value of the **PASSWORD\_EXPIRATION\_WARNING\_DAYS** *System Flag*. The earliest warning can be displayed 14 days before the password is due to expire and the latest warning can be displayed 7 days before passwords are due to expire. An *Active Alarm* is created stating the number of days before the password is due to expire.
- The **MIN\_PWD\_CHANGE\_FREQUENCY\_IN\_DAYS** *System Flag* does not effect *application-user* accounts. Applications typically manage their own password change frequency.
- If an *application-user* identifies itself with an incorrect *FQDN*, its account will not be locked, however the event is written to the *Auditor Event File*.
- If an *application-user* identifies itself with a correct *FQDN* and an incorrect password, its account will be locked and the event written to the *Auditor Event File*.
- An *application-user* cannot be the last administrator in the system. The last administrator must be regular user.

### Monitoring

- An *application-user* and it's connection is represented by a specific icon.

### Active Directory

- When working with *Active Directory*, *CMA* and *DMA* cannot be registered within *Active Directory* as regular users. *CMA* and *DMA application-users* must be registered manually.

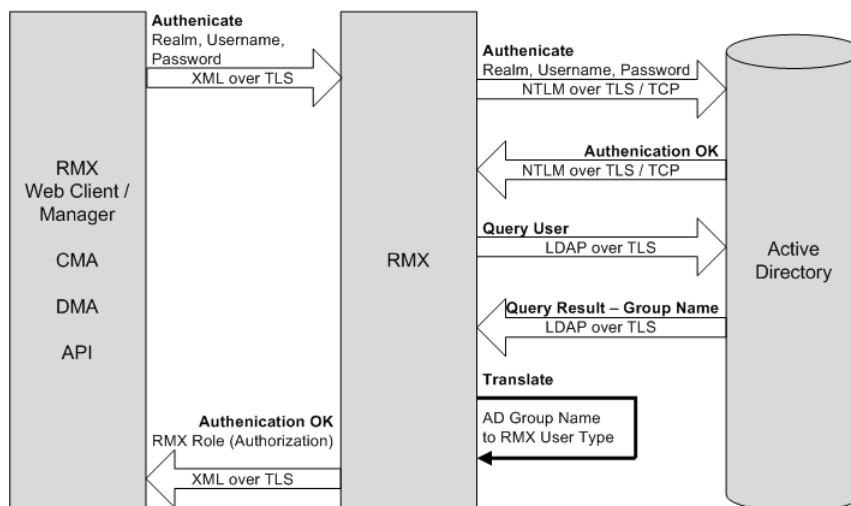
When defining a new user as described in the *RMX 1500/2000/4000 Administrator's Guide*, "Adding a New User" on page 14-4:

- 1 In the *User Properties* dialog box, select the **Associate with a machine** check box.
- 2 Enter the *FQDN* of the server that hosts the application who's application-user name is being added. Example: `cmal.polycom.com`
- 3 Click the **OK** button.

## MS Active Directory Integration

It is possible to configure direct interaction between the *RMX* and *Microsoft Active Directory* for *Authentication* and *Authorization* of *Management Network* users.

The following diagram shows a typical user authentication sequence between a *User*, *RMX* and *Active Directory*.



## Directory and Database Options

### Ultra Secure Mode

#### Internal RMX database and Active Directory

Authentication is first attempted using the internal RMX database. If it is not successful authentication is attempted using the *Active Directory*.

### Standard Security Mode

#### Internal RMX database + External Database

First authentication is via the internal RMX database. If it is not successful, authentication is via the *External Database*.

#### Internal RMX database + External Database + Active Directory

- **Management Logins**  
First authentication is via the internal RMX database. If it is not successful, authentication is via the *Active Directory*.
- **Conference Queries** (*Chairperson Password*, *Numerical ID* etc.)  
First authentication is via the internal RMX database. If it is not successful, authentication is via the *External Database*.



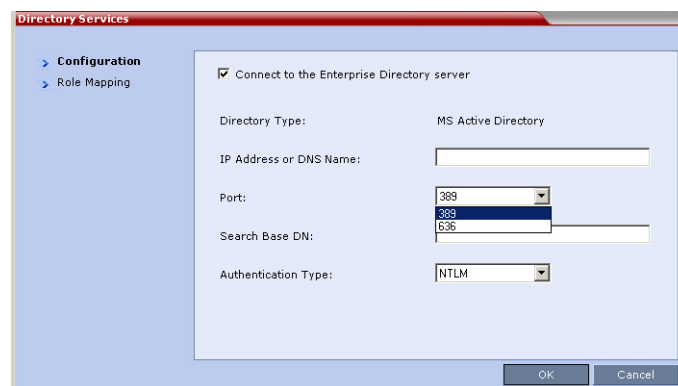
## Guidelines

- The RMX maintains a local record of:
  - *Audit Events* – users that generate these events are marked as being either internal or external.
  - Successful user logins
  - Failed user login attempts
- User passwords and user logout policy for external users are managed via *Active Directory's* integration with the user's host machine.
- Enabling or disabling *Active Directory* integration does not require a reset.
- In *Standard Security Mode* multiple accounts of all user types are supported. In *Ultra Secure Mode*, enabling *Active Directory* integration is only permitted if the RMX only has one local *Administrator User*.
- Multiple *Machine Accounts* with various roles are supported.
- *Microsoft Active Directory* is the only directory service supported.
- *Active Directory* integration is configured as part of the *Management Network*.
- Both *IPv4* and *IPv6* addressing are supported.
- In *Standard Security Mode*, the *Active Directory* can be queried using *NTLM* with or without *TLS* encryption. In *Ultra Secure Mode*, *TLS* encryption is required.
- Server and client certificate validation requests use *LDAP* with or without *TLS* encryption.

## Enabling Active Directory Integration

To configure Directory Services:

- 1 On the RMX menu, click **Setup > Exchange Integration Configuration**. The *Directory Services - Configuration* dialog box is displayed.



- 2 Modify the following fields.

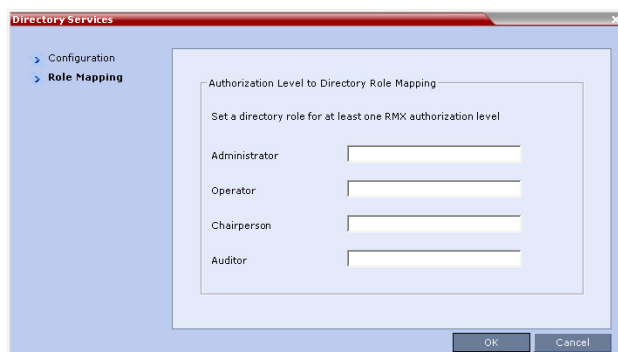
**Table 1-1** *Directory Services - Configuration*

Field	Description
<i>Connect to the Enterprise Directory Server</i>	Select this check box to enable or disable the <i>Active Directory</i> feature.

**Table 1-1** Directory Services - Configuration (Continued)

Field	Description
<i>IP Address or DNS Name</i>	Enter the IP address or DNS name of the Enterprise Directory Server (Active Directory).
<i>Port</i>	Select the <i>Port</i> according to the <i>Authentication Protocol</i> to be used: <ul style="list-style-type: none"> <li>• <b>389</b> - NTLM over TCP</li> <li>• <b>636</b> - NTLM over TLS</li> </ul>
<i>Search Base DN</i>	Enter the starting point when searching for <i>User</i> and <i>Group</i> information in the <i>Active Directory</i> . For example if the <i>Domain Name</i> is: mainoffice.bigcorp.com.uk The entry in this field should be: CN=Users,DC=mainoffice,DC=bigcorp,DC=com,DC=uk
<i>Authentication Type</i>	Only NTLM can be used.

- Click the **Role Mapping** tab.  
The *Directory Services - Role Mapping* dialog box is displayed.



Each of the RMX user types: *Administrator*, *Auditor*, *Operator* and *Chairperson* can be mapped to only one *Active Directory Group* or *Role* according to the customer's specific implementation.

- In *Ultra Secure Mode* there are only two user types: *Operator* and *Administrator*.
- An RMX user that belongs to multiple *Active Directory Groups* is assigned to the *Group* with the least privileges.

- Map the RMX *User Types*, to their *Active Directory* roles by modifying the following fields.

**Table 1-2** Directory Services - Role Mapping

Field	Description
<i>Administrator</i>	At least one of these <i>User Types</i> must be mapped to an <i>Active Directory Role</i> .
<i>Operator</i>	
<i>Chairperson</i>	
<i>Auditor</i>	

5 Click OK.

## Intrusion Detection

### Network Intrusion Detection System (NIDS)

The RMX system uses *iptables* for access control. For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the RMX must pass the rules applicable to it.

Depending on the nature of the suspect packets, the rules may reject, drop, or limit their arrival rate (dropping the rest)

The RMX maintains a log that includes all unpermitted access attempts blocked by the fire wall.

Unpermitted access includes:

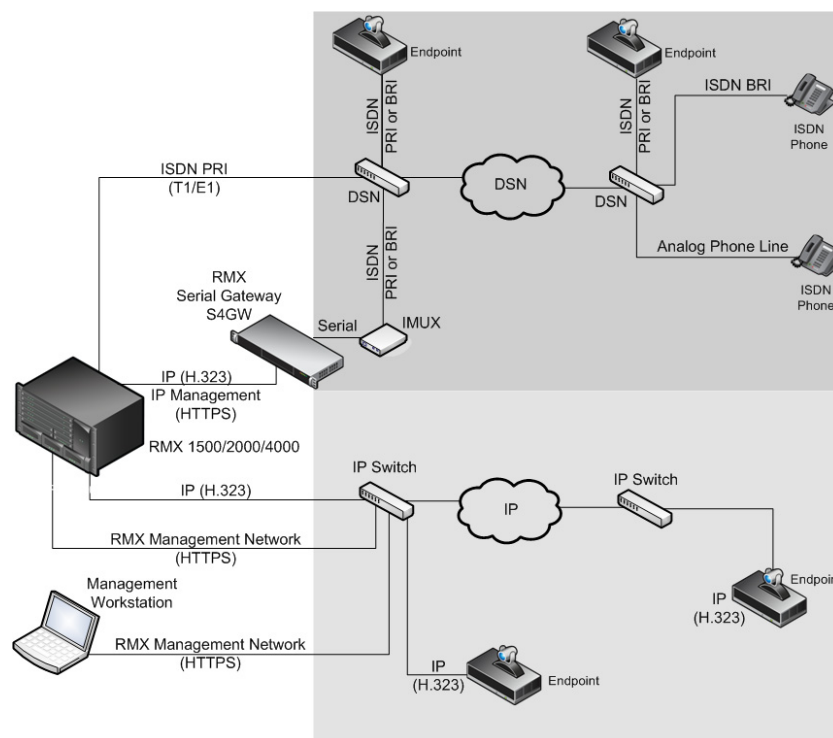
- Access to ports which are not opened on the RMX
- Invalid access to open ports.

The NIDS logs of these events can only be viewed using the *Information Collector*.

For more information the RMX 1500/2000/4000 *Administrator's Guide Maximum Security Environments, "Information Collector"* on page **17-142**.

## Polycom RMX™ Serial Gateway S4GW

UC APL Public Key Infrastructure (PKI) requires that the *Serial Gateway S4GW* be connected directly to the RMX and not to the H.323 network. The *Serial Gateway* effectively becomes an additional module of the RMX, with all web and H.323 traffic passing through the RMX.



**Figure 2** Network infrastructure with direct connection to Serial Gateway S4GW

After initial setup, the *Serial Gateway* is configured, managed and monitored via the RMX Web Client / RMX Manager. For more information see “Setting Up Your Polycom RMX Serial Gateway S4GW” in the *RMX Serial Gateway S4GW System User Guide*.

### Guidelines

- The *Serial Gateway* is supported on RMX 1500/2000/4000.
- Only one *Serial Gateway* can be connected directly to an RMX.
- The *Serial Gateway* can be associated with only one *Network Service*.
- Although the *Media* and *Signaling Network Service* on the RMX can be configured for IPv6 addressing, the *Network Service* assigned to the *Serial Gateway* can only support IPv4 addressing.
- The following *System Flags* must be set to **YES**:
  - **ULTRA\_SECURE\_MODE**
  - **V35\_ULTRA\_SECURED\_SUPPORT**
- When connecting the *Serial Gateway* to an RMX 2000:
  - It is essential that an RTM LAN card is installed.
  - The *Serial Gateway* must be physical connected to the RTM LAN card, LAN 1 port.

- The **SEPARATE\_MANAGEMENT\_NETWORK** *System Flag* must be set to **YES**.
- The following *System Flags* must be set to **NO**:
  - **MULTIPLE\_SERVICES**
  - **ENABLE\_EPC** (If this *System Flag* doesn't exist it must be created.)
- If *Content* is to be shared the conference *Profile* should have *Content Protocol* set to **H.263**.
- When the RMX is in *Ultra Secure Mode*, it requires that the *Serial Gateway* be in *Maximum Security Mode*. For more information see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments*, "Serial Gateway S4GW - Maximum Security Mode" on page **5-11**.
- H.323 connections to the RMX are 1024-bit encrypted TLS.
- RTP traffic between the RMX and the *Serial Gateway* are not encrypted.
- The *Certificate* installed on the *Serial Gateway* must be also be installed in the workstation that is used to run the *RMX Web Client / RMX Manager*.
- Table 1-3 summarizes the LAN port connections for each of the RMX platforms.

**Table 1-3** LAN Port Connections per RMX Platform

RMX	Management	Signaling	Media	V.35 Serial Gateway Direct Connection
1500	MNG B	MNG	LAN 2	LAN 1
2000	RTM IP LAN 3	RTM IP LAN 2	RTM IP LAN 2	RTM LAN LAN 1
4000	RTM IP LAN 2	RTM IP LAN 3	RTM LAN LAN 2	RTM LAN LAN 1

- When using a HDX endpoint, it should be configured as follows:

Manage the network bandwidth used for calls, specify the default and optional call settings for outgoing calls, and limit the call

- General Settings
- Network
  - IP Network
  - Telephony
  - Call Preference**
  - Network Dialing
  - Call Speeds
- Monitors
- Cameras
- Audio Settings
- Polycom Touch Control
- LAN Properties
- Global Services
- Tools

**Call Preference** Update

Call Preference

Enable

Basic Mode: ☐

H.239: ☒

IP H.323: ☒

SIP: ☒

Analog Phone: ☐

Transcoding: ☐

ISDN Gateway: ☐

IP Gateway: ☐

**Preferred Speeds**

Select the preferred speeds for placing calls.

IP Calls: 4096

Select the maximum speeds for receiving calls.

IP Calls: 4096

## Configuring the RMX - Serial Gateway Connection

Configuring the connection between the *Serial Gateway* and the *RMX* consists of the following procedures:

### **1 Initial Setup of the Serial Gateway**

For more information see “*Setting Up Your Polycom RMX Serial Gateway S4GW*” in the *RMX Serial Gateway S4GW System User Guide*.

### **2 Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX.**

These procedures are described in detail in *Chapter 5* of the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments*

# Version 7.6 Detailed Description - Changes to Existing Features

## H.264 High Profile Support in Video Switched Conferences

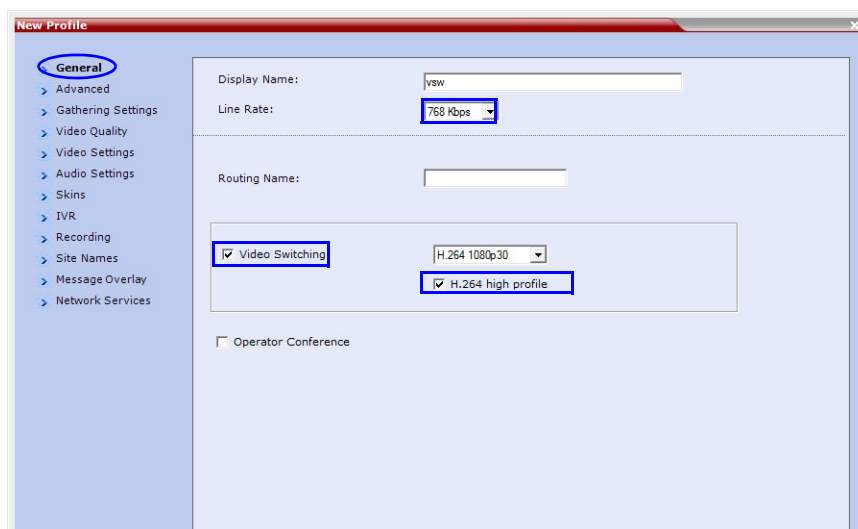
Beginning with *Version 7.6*, the *H.264 High Profile* video protocol is supported in *Video Switching* (VSW) conferences.

### Guidelines

- *H.264 High Profile* is supported in VSW conferences:
  - With MPMx cards.
  - In *H.323* and *SIP* networking environments only (VSW conferences are not supported in *ISDN* networking environments.)
- **For H.264 High Profile enabled VSW conferences:**
  - All endpoints connecting to the conference must support *High Profile*.
  - Endpoints that support *High Profile*, connecting to the VSW conference at the exact *line rate* and exact *resolution* defined for the conference are connected using the *High Profile* video protocol.
  - Endpoints that do not support *High Profile*, connecting to the VSW conference at the exact *line rate* and exact *resolution* defined for the conference are connected to the conference as secondary (audio only).
- **For non-H.264 High Profile enabled VSW conferences:**
  - *High Profile* supporting and non-*High Profile* supporting endpoints connecting to the VSW conference at the exact *line rate* and exact *resolution* defined for the conference are connected using the *H.264 non-High Profile* video protocol.
  - Endpoints that do not support the exact *line rate* and exact *resolution* defined for the conference will be connected to the conference as secondary (audio only).

## Enabling H.264 High Profile in VSW Conferences

- ◀ Select the *H.264 High Profile* check box, in the *Profiles - General* dialog box.



The *High Profile* check box is only displayed if *MPMx* cards are installed in the RMX. By default the check box is not selected. If *H.264* is not the selected video protocol the check box is inactive (grayed out).

## System Flags

Table 1-4 lists the *System Flags* that control the *minimum threshold line rates* for the various *resolutions* available for *High Profile*-enabled *VSW* conferences.

**Table 1-4** System Flags - Minimum Threshold Line Rates

Flag Name	Minimum Threshold Line Rate (Kbps)
VSW_CIF_HP_THRESHOLD_BITRATE	64
VSW_SD_HP_THRESHOLD_BITRATE	128
VSW_HD720p30_HP_THRESHOLD_BITRATE	512
VSW_HD720p50-60_HP_THRESHOLD_BITRATE	832
VSW_HD1080p_HP_THRESHOLD_BITRATE	1024

- *Line rate* and *resolution* combinations are checked for validity. If the selected *line rate* is below the *minimum threshold line rate* required for the selected *resolution*, the *line rate* is automatically adjusted to the *minimum threshold line rate* value for the selected *resolution*.
- The value of the **SUPPORT\_HIGH\_PROFILE** *System Flag* (used for *CP* conferences) has no effect on *VSW* conferences.
- Before they can be modified, all of the *System Flags* mentioned above must be added to the *system.cfg* file using the *RMX Menu – Setup* option. For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying System Flags" on page 21-1.



## IVR Tone Notifications

Roll Call announcements played upon a participant's connection or disconnection from a conference (Entry and Exit announcements) can be replaced by tones. These tones can be used as notification when participants join or leave the conference but the identification of the participant is not required. The system is shipped with two default tones: Entry Tone and Exit tone.

When the Tone Notifications option is enabled, all Roll Call options are disabled. No recording of the participant names will occur and the conference chairperson will not be able to ask for a name review during the conference.

Tone Notifications option replaces the system flag `IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE` which was removed from the System Configuration list of flags.

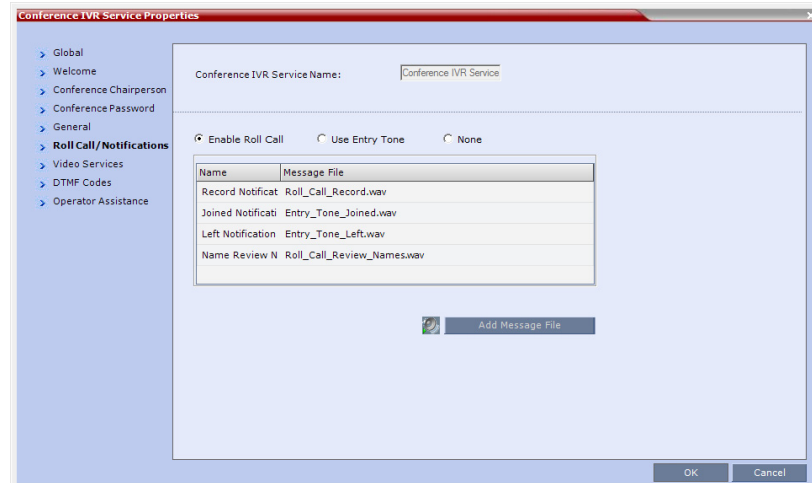
## Using Tone Notifications

The Notification Tones are defined in the *Conference IVR Service - Roll Call/Notifications* tab.

**To define the Notification Tones:**

- 1 In the IVR Services list pane, double-click an existing IVR Service to modify its properties, or click the **New Conference IVR Service** (🔧) button on the toolbar. The *Conference IVR Service - Global* dialog box opens.
- 2 Click the **Roll Call/Notifications** tab.

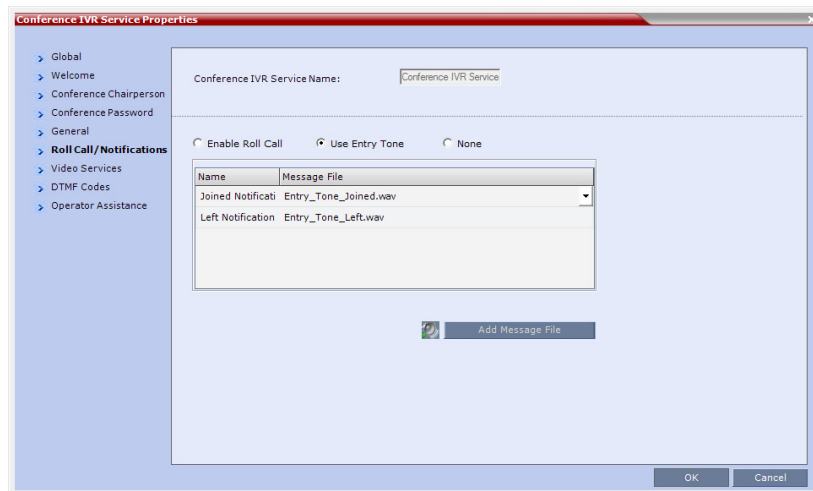
The *Conference IVR Service Properties - Roll Call/Notifications* dialog box opens.



When the **Enable Roll Call** option is selected, the Roll call option behaves as in previous versions.

- 3 Select **Enable Tones**, or select **None** to disable the *Roll Call* and *Notification* options. If *None* is selected, all Roll Call and Tone Notification options are disabled.

If *Enable Tones* is selected, the dialog box changes to display the tone notification options.



- 4 To select the Entry Tone or Exit tone:
  - a Click the appropriate table entry in the *Message File* column. A drop-down list is enabled.
  - b From the list, select the audio file to be assigned to the event/indication.



If the Tones option is enabled, you must assign the appropriate audio files to all notification types. The RMX system is shipped with two default tones: Entry\_tone.wav and Exit\_tone.wav. If required, you can upload customized audio files that will be played when participants join or leave the conference.

If the option to play a tone when a cascading link connection is established, make sure that the tone selected for Entry or Exit notification differ from the cascading link tone as the latter one cannot be customized.

## Play Tone Upon Cascading Link Connection

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

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

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

The option to play a tone when the cascading link is established is enabled by setting the *System Flag*: **CASCADE\_LINK\_PLAY\_TONE\_ON\_CONNECTION** to **YES**.

Default value: **NO**.

The tone volume is controlled by the same flag as the IVR messages and tones: **IVR\_MESSAGE\_VOLUME**.

## Adjust Reservations Start Time

When utilizing GMT offset (for example, *Daylight Saving Time* change), the start time of the reoccurring reservations scheduled before the RMX time change are not updated accordingly (although their start times appear correctly in the *Reservations* list, but when checking the reservation properties the start time is incorrect)

Following the RMX time change, the start time of all reoccurring reservations must be manually adjusted in one operation.

Using this option, the start times of **all** reservations currently scheduled on the RMX are adjusted with the same offset.

**To adjust the reoccurring reservations start time after the GMT Offset has been changed for Daylight Saving Time (DST) or a physical move:**



Adjustment of *Reservation Time* should only be performed after adjustment of *RMX Time* is completed as a separate procedure.

- 1 On the RMX menu, click **Setup > MCU Time**.  
The *RMX Time* dialog box opens.
- 2 Click the **Adjust Reservations Time** button.

The *Adjust Reservations Time* dialog box opens.

Click the arrows to adjust the start time by hours.  
Range is between 12 hours and -12 hours  
A positive value indicates adding to the start time  
(-) indicates subtracting from the start time

Click the arrows to adjust the start time by minutes.  
Range is between 45 minutes and -45 minutes.  
A positive value indicates adding to the start time  
(-) indicates subtracting from the start time

- 3 Click the arrows of the *Offset - Hours* box to indicate the number of hours to add or subtract from the current start time; a positive value indicates adding time, while minus (-) indicates subtracting time.
- 4 Click the arrows of the *Offset - minutes* box to indicate the number of minutes to add or subtract from the current start time of the reservations. Increments or decrements are by 15 minutes.  
  
For example, to subtract 30 minutes from the start time of all the reservation, enter 0 in the *hours* box, and -30 in the *minutes* box.  
To add one hour and 30 minutes to the start time, enter 1 in the hours box and 30 in the minutes box.
- 5 Click the **Adjust** button to apply the change to all the reoccurring reservations currently scheduled on the RMX.



When adjusting the start time of 1000 - 2000 reservations, an "Internal communication error" message may appear. Ignore this message as the process completes successfully.

## CDR Additions

Participants connect to the conferences as standard participants and they are designated as chairpersons either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code. The RMX user can also designate participants as chairpersons in the RMX Web Client or RMX Manager applications.

The change in the participant's role will now be reflected in the CDR file by a new event (in previous versions the participant role as chairperson was not reflected and was always false):

- Event ID=33
- Event Title: PARTY CHAIR UPDATE
- Event Fields:
  - Participant name
  - Participant ID
  - Chairperson
 Possible values:
  - True - participant is a chairperson
  - False - Participant is not a chairperson participant (is a standard participant)

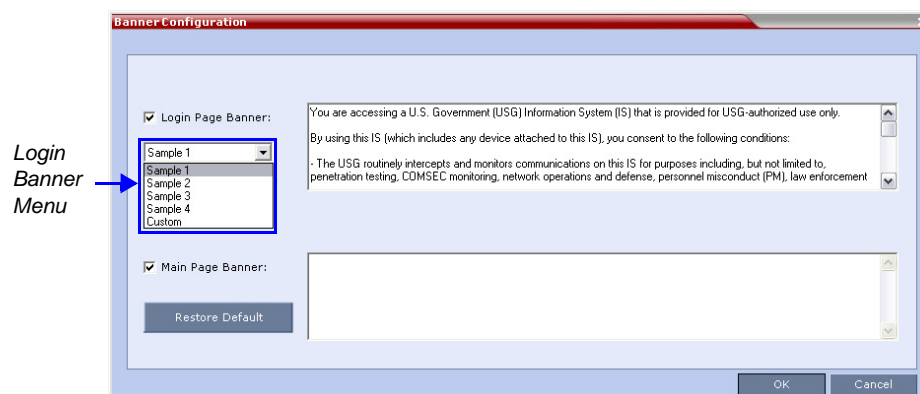
```
PARTY CHAIR UPDATE
Participant Name: DAVE
Participant ID: 0
Chairperson: True
```

## Login Page/Main Page Banners

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A *Custom* banner (default) can also be defined.

The *Main Page Banner* is blank and can be defined.

The *Banner Configuration* dialog box allows the administrator to select a *Login Banner* from a drop-down menu.



One of the the following *Login Banners* can be selected:

- **Non-Modifiable Banners**
  - *Sample 1*
  - *Sample 2*
  - *Sample 3*
  - *Sample 4*
- **Modifiable Banner**
  - *Custom* (Default)

### Guidelines

- The *Login Banner* cannot be disabled when the RMX is in *Ultra Secure Mode*.
- The *Login Banner* must be acknowledged before the user is permitted to log in to the system.
- If a *Custom* banner has been created, and the user selects one of the alternative, non-modifiable banners the *Custom* banner not deleted.
- The *Custom Login Banner* banner may contain up to 1300 characters.
- An empty *Login Banner* is not allowed.
- Any attempt to modify a non-modifiable banner results in it automatically being copied to the *Custom* banner.

## Non-Modifiable Banner Text

### Sample 1 Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

## **Sample 2 Banner**

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

## **Sample 3 Banner**

You are about to access a system that is intended for authorized users only. You should have no expectation of privacy in your use of this system. Use of this system constitutes consent to monitoring, retrieval, and disclosure of any information stored within the system for any purpose including criminal prosecution.

## **Sample 4 Banner**

This computer system including all related equipment, network devices (specifically including Internet access), is provided only for authorized use. All computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored. Use of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

## User Management

### User Name - Case Sensitivity

User names are case sensitive.

## Strong Passwords

### User Passwords

#### Maximum Repeating Characters

A *System Flag* **MAX\_PASSWORD\_REPEATED\_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password.

**Range:** 1 - 4

**Default:** 2

### Conference and Chairperson Passwords

#### Maximum Repeating Characters

A *System Flag* **MAX\_CONF\_PASSWORD\_REPEATED\_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a password.

**Range:** 1 - 4

**Default:** 2



*Chairperson users are not supported in Ultra Secure Mode.*



## USB Restore Defaults

The *USB* port of an *RMX* in *Ultra Secure Mode* can be used to:

- Restore the *RMX* to *Factory Security Defaults* mode (*https* → *http*).
- Perform a *Comprehensive Restore to Factory Defaults*
- Perform an *Emergency CRL (Certificate Revocation List) Update*

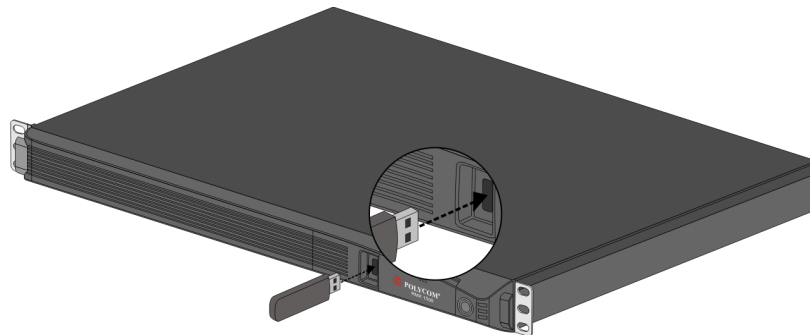
## USB Ports on RMX 1500/2000/4000



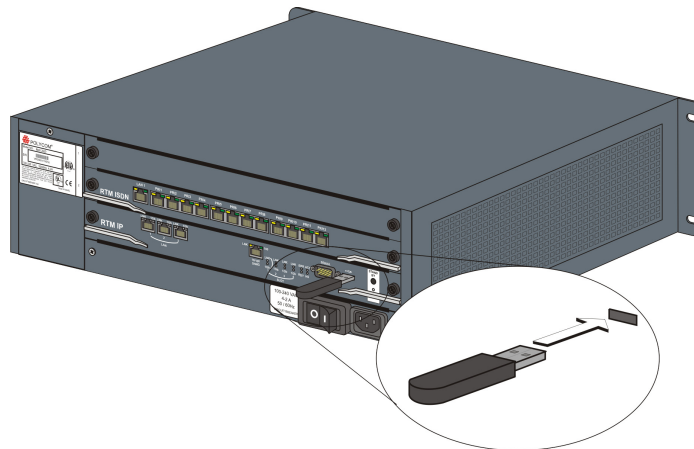
Do **not** use any *USB* ports other than the ones indicated in the following diagrams.

When performing *USB Operations*, the following *USB* ports are used:

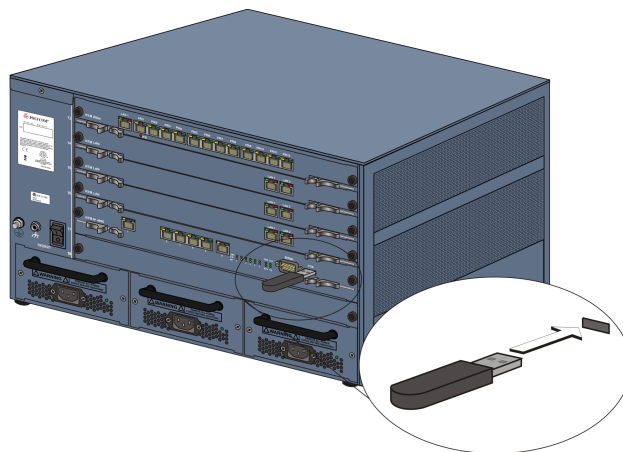
- *RMX 1500* - left most *USB* port on the **front panel**.



- *RMX 2000* - at the bottom right corner of the *RTM IP* card on the **back panel**.



- *RMX 4000* - at the bottom right corner of the *RTM IP 4000* card on the **back panel**.



## Restore to Factory Security Defaults

Restore to Factory Security Defaults can be performed by either:

- Inserting a *USB* device such as a mouse or a keyboard into the *RMX's USB Port* causing it to exit *Ultra Secure Mode* and return to *Factory Security Defaults* mode. After performing this procedure, *Logins* to the *RMX* use the **http** command and not the **https** command.
- or
- Inserting a *USB* key containing a file named *RestoreFactorySecurityDefaults.txt*.

**To restore the RMX to Factory Security Defaults:**

- 1 Insert a *USB* device or a *USB* key containing a file named *RestoreFactorySecurityDefaults.txt* into the *USB* port of the *RMX*.

The *USB* port locations for *RMX 1500/2000/4000* are shown in "*USB Ports on RMX 1500/2000/4000*" on page **1-147**.

- 2 Power the *RMX* **Off** and then **On**.
- 3 Login using **http://<Control Unit IP Address>**.

## Comprehensive Restore to Factory Defaults

Inserting a *USB* key containing a file named *RestoreToFactoryDefault.txt* **and** a *lan.cfg* file will cause the *RMX* to exit *Secure Mode* **and** perform a *Comprehensive Restore to Factory Defaults*.

The *Comprehensive Restore to Factory Defaults* deletes the following files:

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

- Notes

In addition all the conferencing entities are deleted:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service
- Log Files
- CFS license information
- Management Network Service

The RMX is restored to the settings it had when shipped from the factory. The *Product Activation Key* is required to re-configure the *Management Network Service* during the *First Entry Configuration*.

## Comprehensive Restore to Factory Defaults Procedure

**To perform a Comprehensive Restore to Factory Defaults:**

Restoring the RMX to *Factory Defaults* consists of the following procedures:

### **A Backup Configuration Files**

- These files will be used to restore the system in Procedure C.

### **B Restore to Factory Defaults**

- Restart the system with a *USB* device containing a file named *RestoreToFactoryDefault.txt* and a *lan.cfg* file plugged into the *USB* port.

### **C Optional. Restore the System Configuration From the Backup**

- Apply the backup file created in procedure A.
- Restart the RMX.

(If the RMX is unresponsive after these procedures a further restart may be necessary.)

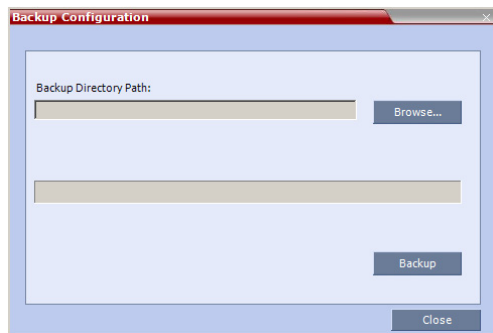
## Procedure A: Backup Configuration Files

The *Software Management* menu is used to backup and restore the RMX's configuration files and to download MCU software.

**To backup configuration files:**

- 1 On the RMX menu, click **Administration > Software Management > Backup Configuration**.

The *Backup Configuration* dialog box opens.



- 2 Browse to the *Backup Directory Path* and then click **Backup**.

## Procedure B: Restore to Factory Defaults

To perform a Comprehensive Restore to Factory Default perform the following steps:

- 1 Insert a USB device containing a file named *RestoreToFactoryDefault.txt* and a *lan.cfg* file into the USB port of the RMX.  
For more information on creating a *lan.cfg* file see the RMX 1500/2000/4000 Getting Started Guide, "Modifying the Factory Default Management Network Settings on the USB Key" on page 2-7.
- 2 Power the RMX Off.
- 3 Power the RMX On
- 4 Proceed from Step 2 of "Procedure 1: First-time Power-up" on page 2-24, continuing to the end of Chapter 2 of the RMX 1500/2000/4000 Getting Started Guide.
- 5 Optional. Restore the system using "Procedure C: Restore the System Configuration From the Backup" below.

## Procedure C: Restore the System Configuration From the Backup

To restore configuration files:

- 1 On the RMX menu, click **Administration > Software Management > Restore Configuration**.
- 2 Browse to the *Restore Directory Path* where the backed up configuration files are stored.
- 3 Click the **Restore** button.
- 4 When the **Restore** is complete, restart the RMX.  
*RMX system settings, with the exception of User data, are restored.*
- 5 Restore *User data* by repeating **Step 1** to **Step 3** of this procedure.

## Emergency CRL (Certificate Revocation List) Update

Administrators maintaining RMX systems are required to perform an update of the CRLs used on the systems within the validity period of the current CRLs.

Should the current CRLs expire; the system will not allow administrators to login and perform administrative tasks using the *RMX Web Client* or *RMX Manager*.

The *Emergency CRL Update* procedure disables client certificate validation enabling an administrator to access the system and install an updated CRL file without having to perform a full system rebuild.

### Emergency CRL Update Procedure



This procedure must only be performed on a secured network as the system must disable the client certificate validation process resulting in management traffic being sent over the network without the use of SSL encryption.



The RMX must be powered on before starting this procedure.

The *Emergency CRL Update* procedure consists of the following steps:

- 1 Download and save the updated CRL files from the CA Server.
- 2 Disable *Secured Communications Mode*.
- 3 Open the *Certification Repository*.
- 4 Update the CRL files.
- 5 Update the *Repository*.
- 6 Re-connect to the RMX.
- 7 Re-enable *Secured Communications Mode*.

#### Step 1: Download and save the updated CRL files from the CA Server.

These files are saved on the workstation.



The RMX supports the use of *PEM* and *DER* formats.

Take note of the format you download as you will need to make a selection later in this process when uploading the new CRL files.

#### Step 2: Disable Secure Communications mode

- a Connect a USB keyboard or mouse to the USB port of RMX.

The USB port locations for RMX 1500/2000/4000 are shown in "There are also administrative operations that cannot be performed on a secured or ultra secured system that require the RMX to be set back to its default (normal) security mode." on page E-1.

- b Power the RMX **Off** and then **On** using the power switch and allow the RMX to complete its startup.

System restart can take 5 - 10 minutes, depending on the RMX's configuration.

Using the *RMX Manager*:

- c In the MCUs list, select the RMX to be updated.
- d In *MCU Properties*, change the *Port* number from **443** to **80**.

- e Click **OK**.
- f In the *MCUs* list, select the *RMX* to be updated.
- g Right-click in the *MCUs* list entry and select **Connect**.
- h Click **Accept** to accept the warning banner.
- i Enter an administrator *Username* and *Password*.
- j Click **OK**.

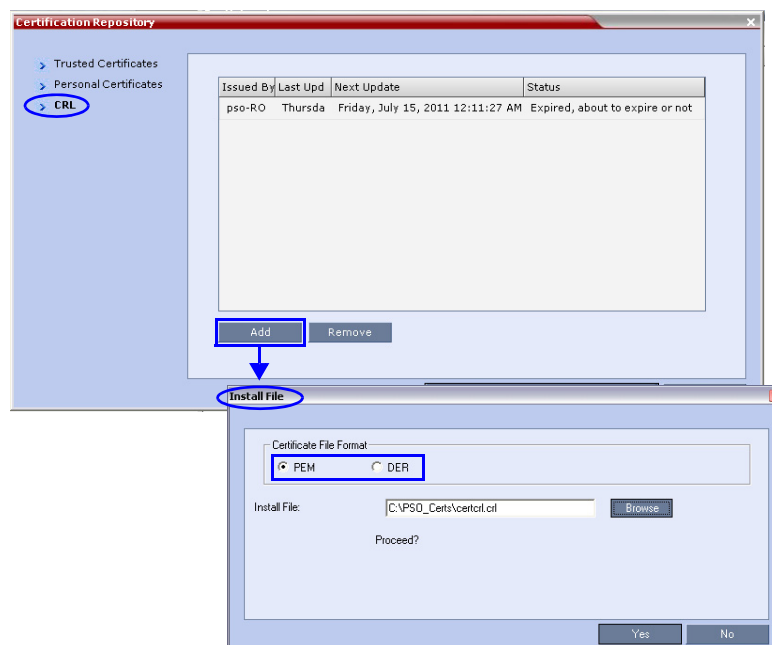
**Step 3: Open the Certification Repository.**

On the *RMX* menu, click **Setup > RMX Secured Communication > Certification Repository**.

**Step 4: Update the CRL files.**

In the *Certification Repository*:

- a Click the **CRL** tab.
- b Click **Add**.



- c In the *Install File* dialog box, select the **DER** or **PEM** format depending on which file format was chosen in *Step 1* of this procedure.
- d Click the **Browse** button to navigate to the folder on the workstation where you saved the *CRL* files in *Step 1* of this procedure.
- e Select the *CRL* file that you want to upload.
- f Click **Yes** to proceed.  
The system checks the *CRL* file and displays a message that the certificate was loaded successfully.
- g Repeat Steps *d* through *f* until all of the required *CRL* files has been updated.

**Step 5: Update the repository.**

When all the *CRL* files have been updated as described in *Step 4*:

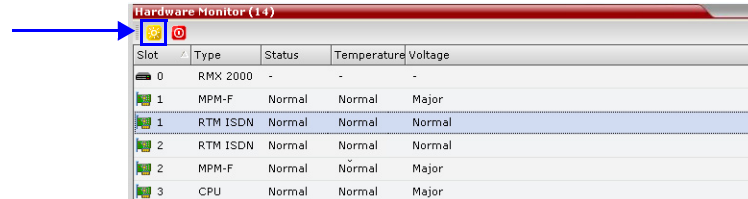
- a Click **Update Repository**.

A repository update confirmation message is displayed.

- b** Click **OK** to update the repository.

**Step 6: Re-connect to the RMX.**

- a** Remove the *USB* device that was connected in *Step 2a*.
- b** Restart the RMX.
- c** In the *RMX Management* pane, click the **Hardware Monitor** button.  
The *Hardware Monitor* pane is displayed.



- d** Click the **Reset** button.

The RMX restarts. System restart can take 5 - 10 minutes, depending on the RMX's configuration.

Using the *RMX Manager*:

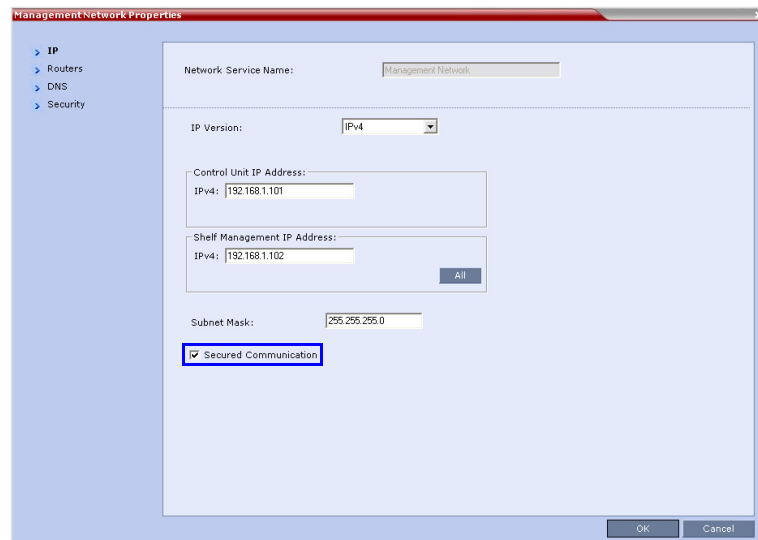
- e** In the *MCUs* list, select the RMX to be updated.
- f** Right-click in the *MCUs* list entry and select **Connect**.
- g** Click **Accept** to accept the warning banner.
- h** Enter an administrator *Username* and *Password*.
- i** Click **OK**.

**Step 7: Re-enable Secured Communications Mode.**

Using the *RMX Manager*:

- a** In the *RMX Management* pane, click the **IP Network Services** button. (Depending on the *RMX Manager* configuration, you may have to click **Rarely Used** first.)
- b** In the *IP Network Services* list pane, double-click **Management Network**.

The *Management Network Properties* dialog box is displayed.



**c** Select the *Secured Communication* check box.

**d** Click **OK**.

A message informs you that your session will be disconnected and that you must re-connect the RMX using **https** in the browser *URL*.

**e** Click **OK**.

A system restart confirmation message is displayed.

**f** Click **Yes** to restart the RMX.

The RMX restarts. System restart can take 5 - 10 minutes, depending on the RMX's configuration.

**g** In the *MCUs* list, select the RMX to be updated.

**h** In *MCU Properties*, change the *Port* number from **80** to **443**.

**i** Click **OK**.



# Corrections and Known Limitations

## Corrections Between Version 7.6 and Version 7.6.1

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
1	VNGR-24432	Hardware	When the temperature on the CPU of the CNTL unit reaches major or critical, the fans do not respond and the card resets to prevent overheating.	V7.6.1
2	VNGR-24090	General	After upgrading to version 7.6.1, the RMX Time dialog box lists the NTP Server statuses as Fail. As a workaround, in the RMX Time dialog box select Retrieve Client Time and click OK.	V7.6.1
3	VNGR-23938	General	In the Hardware Monitor - LAN List, all the LAN ports appear Inactive, when they are in fact Active.	V7.6.1
4	VNGR-23937	General	In the Hardware Monitor - LAN List, all the LAN ports appear Inactive, when they are in fact Active.	V7.6.1
5	VNGR-23400	General	Calling the RMX during the startup process may result in call failure.	V7.6.1
6	VNGR-23093	Diagnostics	Occasionally, RMX 1500 remains in startup when switching to Diagnostics mode.	V7.6
7	VNGR-22999	Interoperability	In DMA Supercluster RMX fails to register to alternate gatekeeper node when primary gatekeeper node is available.	V7.6
8	VNGR-22799	General	After initiating a Network Traffic Capture from the Administration/Tools menu and pressing Start, the Network Traffic Capture does not initialize and the File(s) are not created.	V7.6
9	VNGR-22707	Partners - Microsoft	Sometimes Lync clients are unable to connect to th conference video when dialing-in to a CP conference set to a line rate of 768Kbps and a resolution of 720p .	V7.6
10	VNGR-22692	Partners - Microsoft	The Presence status of Meeting Rooms is not shown in the Lync clients after upgrading from version 7.2.2 to 7.6.	V7.6

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
11	VNGR-22666	Hardware	The RTM IP 1500 RDY Led should flash during startup and then remain ON.	V7.6
12	VNGR-22665	Hardware	On the RMX, when the user in the RMX Manager/Client presses the System Shut Down button in the Hardware Monitor toolbar, all RMX cards should enter into a standby mode and the STANDBY led must be lit (On) on the RTM IP card.	V7.6
13	VNGR-22608	IVR	In the IVR Services, when attempting to load a music message file, the RMX client exits the dialog box and the browser must be restarted.	V7.6
14	VNGR-22564	Content	In a 4Mb dial out H.323 conference, after HDX and Tandberg C90 endpoints connect and the HDX sends 1080p Content, after dialing out Radvision RV endpoint, HDX content dropped to 720p.	V7.6
15	VNGR-22406	ISDN	During a conference with up to 20 IP and mixed ISDN endpoints, when an ISDN endpoint sent content, several endpoints viewed content as a black screen.	V7.6
16	VNGR-22366	Upgrade Process	When initiating a downgrade from version 7.6 to 7.0 and below on the RMX 1500/1500Q, the Safe Software Version Installation alarm message does not appear and a fault is not recorded in the Fault List.	V7.6
17	VNGR-22347	SIP	In the IP Network Service Properties - Security tab, when enabling SIP Authentication and configuring the User Name and Password, the password is missing after RMX reset.	V7.6
18	VNGR-22301	Partners - Microsoft	In an ICE environment with an OCS server present, when MOC Clients first attempt to connect to the conference on an RMX, a SIP/2.0 500 Server Internal Error message appears and the connection disconnects.	V7.6
19	VNGR-22209	Hardware	The RTM IP - MNG and MNGB LNK LEDs never lit and do not turn green.	V7.6
20	VNGR-22202	General	Sometime when accessing the Hardware Monitor of the RMX 1500 and displaying the LAN List, the pane appears empty.	V7.6.1
21	VNGR-22172	General	On any RMX type, after Backup and Restore, RMX Time remains unchanged.	V7.2.2

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
22	VNGR-22127	General	After initiating the Information Collector from the Administration/Tools menu and pressing the Collect Information, if closing the window before completing the process the download file is not created in the specified path.	V7.2.2
23	VNGR-22110	SIP	In the IP Network Service Properties - Security tab, when enabling SIP Authentication and configuring the User Name and Password, the password is missing after RMX reset.	V7.6
24	VNGR-21911	Partners - Microsoft	In an ICE environment, a Lync 2010 Client dial-in connects and then disconnects after a few seconds on an RMX 4000 after a few calls were made to the RMX.	V7.6
25	VNGR-21886	General	When accessing the Hardware Monitor of the RMX 1500 and selecting the MPMx-D card, the MPMX card displays a "Normal" Status although it has no units, and an assert message appears.	V7.6
26	VNGR-21859	Audio	When an Audio Only participant is connected to an Event Mode conference running on RMX 2000, the audio from an HDX 8000 already connected to the conference using SirenLPR cannot be heard by the audio only participant.	V7.6
27	VNGR-21624	Video	During a 512 Kbps conference with the video protocol set to H.264 at 30 fps, the RMX sends CIF video resolution at 15 fps to a QDX endpoint after an HDX 9004 endpoint connects to the conference.	V7.6
28	VNGR-21504	General	On an RMX with version 7.6 and MPM+80, MPM+40 installed, after removing one of the cards the Hardware Monitor updated correctly, however port usage and the resource report settings were not updated accordingly and an active alarm was not issued.	V7.6
29	VNGR-21148	RMX Manager	After changing the Daylight Savings / Daylight Standard Time, the start times & end times of Re-occurring reservations are shifted by one hour in the RMX scheduler. When manually changing the GMT offset value or clicking "Retrieve Client Time" there are no changes in the time settings of standard reservations or re-occurring reservations.	V7.2, V7.1
30	VNGR-21109	General	System Reset is required when changing the Gatekeeper configuration in the default IP Network Service while there are no ongoing conferences.	V4.7.2

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
31	VNGR-20887	<i>RMX Manager</i>	The Participant Properties - Channel Status tab, list the Jitter buffer size as a negative number which is incorrect.	V7.1
32	VNGR-20805	<i>ISDN</i>	On an RMX 2000, H.320 endpoints failed to connect to the Meeting Room while H.323 endpoints connected normally. An RMX reset solved the problem.	V7.0.2
33	VNGR-20522	<i>Partners - Microsoft</i>	Green artifacts and patches of black and white appear on the HDX endpoints after a few minutes of their connection to a 384Kbps CP conference with encryption and LPR enabled using the RTV video protocol. RMX and HDX are registered to the Lync 2010 server.	V7.2
34	VNGR-20471	<i>Content</i>	After starting a 4048 kbps conference from a Profile with 1080p content enabled, when dialing out to an SIP HDX8000 endpoint the Content session is dropped after connecting another SIP endpoint.	V7.2
35	VNGR-20421	<i>General</i>	In the Network Traffic Capture (Administration-->Tool-->Network Traffic Capture) pane select Start Network Traffic Capture. The "storage in use" "time elapsed" indications do not respond.	V7.2
36	VNGR-20418	<i>General</i>	In the Network Traffic Capture (Administration-->Tool-->Network Traffic Capture) pane select Start Network Traffic Capture. Illegal string filters do not activate a message alert.	V7.2
37	VNGR-20417	<i>General</i>	In the Network Traffic Capture (Administration-->Tool-->Network Traffic Capture) pane select Start Network Traffic Capture. The network traffic capture file size is limited to 5MB (media) or 10MB (management) instead to 0.5Gb.	V7.2
38	VNGR-20363	<i>SIP</i>	When opening a connection from Central Signalling to SIP proxy IP, a connection not be established with the SIP registrar.	V7.1
39	VNGR-20279	<i>Video</i>	On an RMX 4000 with an CP Ad Hoc conference, when two HDX endpoints connect, one HDX views a screen that looks like it is in gathering mode and the other has extremely blurry video.	V7.2

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
40	VNGR-20186	<i>Interoperability</i>	On an RMX 4000 with MPMx cards running a 384 kbps CP conference with LPR and Encryption enabled, after the RMX dials out to the two Lync endpoints, the Lync endpoints cannot transfer the call.	V7.2
41	VNGR-20140	<i>Upgrade Process</i>	After upgrading from version 7.1.0.121 to 7.2.0.57 a "Core Dump" message appears.	V7.2
42	VNGR-20078	<i>Video</i>	On an RMX with MPMx cards running a 384 kbps CP conference, after connecting two MOC, HDX and VSX 3000 endpoints, a DSP recovery occurred.	V7.2
43	VNGR-20068	<i>Interoperability</i>	On an RMX 2000 with MPMx cards running a conference, after connecting two MOC, HDX 8000, VSX 3000 and VVX 1500 endpoints, zebra and white artifacts appear in the video in the MOC endpoint.	V7.2
44	VNGR-19992	<i>Security</i>	After restoring the version from keyboard, the RMX IP address is missing.	V7.5
45	VNGR-19932	<i>Hot Backup</i>	When the Master MCU in a Hot backup configuration fails and the Slave MCU activates, DNS host name still lists the _bck (backup) extension.	V4.7.1
46	VNGR-19931	<i>Hot Backup</i>	When Hot backup synchronization is initialized, the status listing indicates "OK" instead of "Attempting".	V4.7.1
47	VNGR-19928	<i>Content</i>	Chroma shift viewed on Legacy endpoints when sending content in a conference running on RMX 2000 with MPMx at a line rate of 512kbps and the Send Content to Legacy Endpoint option enabled.	V7.2
48	VNGR-19632	<i>Video</i>	In an 1080p VSW conference with Motion and Sharpness enabled on HDX8000 endpoints, when video forcing, endpoints see gray artifacts.	V4.7.1
49	VNGR-19424	<i>Partners - Microsoft</i>	When ICE is disabled on the RMX, the ICE server connection status in the User Interface does not change to show that the connection is not available and the status remains as if the Connection is OK. Only after manually resetting the RMX, does the status finally change to connection not available.	V7.1
50	VNGR-19075	<i>Gateway</i>	In an ISDN cascaded conference that places a call using the Codian Gateway, after switching the Content sender, a black screen can be seen.	V7.1

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
51	VNGR-19058	Video	On the RMX1500Q in the IVR Services you cannot upload a new Video Welcome Slide.	V7.1
52	VNGR-19045	Content	In a mixed H.323, SIP, ISDN, PSTN conference with 20 HDX, VSX, Tandberg, LifeSize and CMAD endpoints, when an ISDN endpoint stops and re-sends Content endpoints view a black screen.	V7.1
53	VNGR-18947	CMA	In a 832 kbps H.323 conference registered with the CMA, when connecting CUPC, CMA-D and HDX endpoints the video is bad.	V7.1
54	VNGR-18740	Hot Backup	When the Master MCU in a Hot backup configuration fails, an error occurs.	V4.7
55	VNGR-18317	Hot Backup	When Hot Backup is disabled and then re-enabled in the Master, the status "Attempting" appears for a long time.	V4.7
56	VNGR-18186	Cascading	During an ISDN Cascaded conference when connecting an IP HDX endpoints with 16:9 screen formats, the video changes to 4:3 format instead of 16:9.	V7.1
57	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
58	VNGR-17791	General	DTMF Tones (Click&View) are heard by all conference participants in a conference running on RMX 2000 with MPMx.	V7.0.2
59	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
60	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
61	VNGR-17456	IVR	On an RMX running a 768 kbps conference with multiple H.323 HDX8000 endpoints, after connecting SIP H.263 endpoint the IVR Slide does not appear.	V7.2

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
<b>62</b>	VNGR-17092	<i>Video</i>	In a 384 kbps Meeting Room with LPR, Auto Brightness and Video Clarity enabled, when dial-in VSX and HDX endpoints connect, the default Welcome Slide is blacked out.	V7.0
<b>63</b>	VNGR-16963	<i>IVR</i>	In a 384 kbps conference with IVR, LPR and Sharpness enabled, when dialing-out to a VSX3000 endpoint, the default Welcome Slide does not appear.	V7.1
<b>64</b>	VNGR-16793	<i>General</i>	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
<b>65</b>	VNGR-16780	<i>HD</i>	During VSW conference at 720p60p resolution using direct connections or via DMA, endpoints display only their own video.	V7.0
<b>66</b>	VNGR-16582	<i>General</i>	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
<b>67</b>	VNGR-16581	<i>General</i>	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
<b>68</b>	VNGR-16264	<i>ISDN</i>	During a conference the ISDN line is functional but the line has no clock source.	V7.0
<b>69</b>	VNGR-15837	<i>General</i>	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
<b>70</b>	VNGR-14840	<i>Encryption</i>	No video is seen and the Aethra VegaStar Gold endpoint remains connected with a problem when connecting over H320 to an encrypted conference at a line rate of 384Kbps.	V6.0
<b>71</b>	VNGR-14720	<i>Upgrade Process</i>	After software Upgrade is completed, an Active Alarm "Connection to Exchange Server failed" appears in the Alarms List on the RMX4000.	V6.0

**Table 1-5** Corrections between Version 7.6 and Version 7.6.1

#	Key	Category	Description	Detected in Version
72	VNGR-14386	RMX 4000	Display information for Slot 5, FSM (Fabric Switch Module), in the RMX 4000 Hardware Monitor is incomplete.	V5.1
73	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
74	VNGR-10054	IVR	Customized CIF slide is not displayed on the HDX screen when connecting to a 1080p High Definition Video Switching conference.	V4.0.1

## Corrections Between Version 7.2.2 and Version 7.6

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
<b>Corrections in version 7.6.0.172</b>				
1	VNGR-23064	Hardware	Sometimes the RTM ISDN installed in the RMX 4000 fails to load during start up.	V7.6
2	VNGR-22788	Hardware	Irrelevant sensor information (sensor 8) is displayed in the Hardware Monitor of the RMX 1500-Q.	V7.6
<b>Corrections in version 7.6.0.170</b>				
3	VNGR-22517	Video	In a RMX Telepresence conference with OTX 300 and RPX 200 systems, the RPX 200 4:3 video layout occasionally causes partial 16:9 video format problems on the left display of the OTX 300.	V7.6
4	VNGR-21319	Cascading	Video artifacts are seen on the VVX connected to a slave conference, when the speaker changes between the Slave and the Master conferences. Both conferences were set to line rate of 3072Kbps with resolutions levels of 1080p>720p>4cif>cif263.	V4.7.2
5	VNGR-21290	Video	In VSW (NxM) mode, an endpoint does not view the video from the new lecturer after the lecturers have switched.	V4.7.2
6	VNGR-21255	SIP	SIP endpoint failed to connect at a line rate of 384Kbps when connecting to a conference running at a line rate of 4096Kbps.	V4.7.2



**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
7	VNGR-21193	General	Only 8 Chinese characters (instead of 24) can be input and displayed in the text of the Message Overlay.	V4.7.2
8	VNGR-21182	Upgrade Process	On an RMX4000 with V7.2.0.70 and MPM+ cards V7.2.0.70, After standard Restore Factory Defaults there was no connection with switch. Hard reset solved the problem.	V4.7.2
9	VNGR-21157	General	RMX 2000 unexpectedly rebooted while using the information collector to retrieve log files	V6.0.2
10	VNGR-21138	Diagnostics	When selecting the MPM, CNTL and RTM IP for Advanced Mode Diagnostics, some of the tests do not run on the cards. RMX restart or selecting Basic Mode Diagnostics solves the problem.	V7.2.1
11	VNGR-21113	SIP	Conferencing entity routing name must include lower case characters or numbers to enable dialing from SIP endpoints to conferences and Meeting Rooms in Microsoft environment.	V7.2.1
12	VNGR-21104	RMX Manager	When using an API to define participants in a conference, after conference start the participants appear as chairpersons.	V7.2.2
13	VNGR-21101	General	RTM ISDN Voltage alerts is added to Event log during startup and indicate 0 voltage on current status although ISDN is working properly indicates 0 voltage on current status although ISDN is working properly.	V7.2.1
14	VNGR-21098	Video	On an RMX 1500 with version 7.0.2 installed, during a conference with CP Layout, outlines, silhouettes and shadows from another conference/participant could be seen.	V7.0.2
15	VNGR-21066	RMX Manager	After activating the RMX shutdown button in the RMX hardware monitor pane, the RMX turned ON after 39 minutes.	V7.2, V7.1
16	VNGR-21061	General	In a conference with over 400 participants, when the chairperson joins, the other participants hear no audio.	V7.2.1
17	VNGR-21049	RMX Manager	On the RMX Manager an internal error; 65012 appears, cause unknown.	V7.1
18	VNGR-21017	IP	On an RMX 2000 with two MPM+20 cards, when running an H.323 512Kbps conference, VSX 9.0.61 and HDX 2.6 endpoints disconnected after 30 seconds.	V7.1

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
19	VNGR-20988	<i>RMX Manager</i>	During an Ongoing Meeting Room on the RMX, a media card alert appears and the local and remote endpoints view blue video.	V7.1
20	VNGR-20961	<i>General</i>	The Information Collector does not always download all the log files as requested.	V7.0.2C
21	VNGR-20957	<i>RMX Manager</i>	An RMX 1500 in a conference call with two HDXs endpoints, disconnected for no reason Reconnected end points experienced video freezes and the disconnected from conference. The RMX list a major alarm and shows a number of error messages in the Faults List.	V7.1
22	VNGR-20949	<i>Video</i>	After changing the resolution slider manually on an RMX with MPM+ cards, endpoints connected using H.263 4CIF instead of H.264 CIF.	V7.2
23	VNGR-20887	<i>RMX Manager</i>	The Participant Properties - Channel Status tab, list the Jitter buffer size as a negative number which is incorrect.	V7.1
24	VNGR-20844	<i>RMX Manager</i>	On an RMX 4000, when running a conference with 47 connected endpoints a CPU load alarm appeared; "Major alarm CPU is over 54%".	V7.1
25	VNGR-20843	<i>IVR-RMX 4000</i>	On a fully loaded RMX 4000, some participant and chairperson IVR messages are not played when they join a conference	V7.1
26	VNGR-20839	<i>General</i>	In the CDR, GMT offset is not supported and value will always show 0. This causes billing systems not able to capture the date/time according to local time.	V7.0
27	VNGR-20835	<i>Gateway</i>	When placing a Gateway call on the RMX, the Gateway call status indication display is unreadable.	V7.1
28	VNGR-20828	<i>Content</i>	When dialing out to a second SIP HDX8000 endpoint from a conference running at a line rate of 4048Kbps with 1080p content enabled, the Content session ends.	V4.7.2
29	VNGR-20822	<i>IVR</i>	On the RMX manager version 7.1, you cannot load IVR welcome message when using Windows 7.	V7.1
30	VNGR-20820	<i>General</i>	When the RMX is in a Fixed Ports mode, the first TCP port is set to 49152, and cannot be changed. There is no restriction for UDP ports.	V7.1

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
31	VNGR-20807	General	In Multiple Networks configuration when there are several IP Network Services defined in the system, deleting an IP Network Service that is assigned to certain Profiles does not remove it from these Profiles.	V7.2
32	VNGR-20791	Software Version	After upgrading to version 7.0.2, when moving the Video/Voice port slider from 78/10 to a 80/0 configuration, the voice ports are not changed to video ports.	V7.0.2
33	VNGR-20786	IVR	In an Ad Hoc conference with a Dial-in Entry Queue and IVR, after the second participant connects the first participant views the welcome slide and hears audio. The second participant does have audio and video.	V7.1
34	VNGR-20784	Upgrade Process	Sometimes during upgrade, the message "Activation key required" is not displayed.	V7.1
35	VNGR-20769	Partners - Microsoft	Although PCM is successfully initiated on Microsoft Office Communications client or Lync client, since FECC feature is not available on these clients none of the PCM options are accessible as the only available keys are #, *, 1..9 and not the navigation keys ("LEFT", "RIGHT", etc.).	V7.2
36	VNGR-20768	Video	On an RMX with MPMx cards and with version 7.0.2 installed, endpoints in a conference viewed frozen video. The Faults list show DSP crashes.	V7.0.2
37	VNGR-20735	Video	On some PC workstations running Windows 7, Video Preview does not show video.	V4.7.2
38	VNGR-20716	Interoperability	In a 4096Kbps conference started from a Profile with Content, Send Content to Legacy Endpoints and Telepresence Layout Mode enabled, after registering the RMX to Avaya Session Manager and CMA, 1XC SIP endpoints registered to Avaya Session Manager connected with no video.	V7.2
39	VNGR-20693	General	The frequency with which a user can change an RMX user password is longer than 7 days is incorrect, as a user password cannot be changed for 7 days.	V7.5
40	VNGR-20680	Interoperability	When an endpoint is registered to an ACM Gatekeeper and the RMX MCU is registered with a CMA Gatekeeper, the endpoint is unable to place calls to the RMX.	V7.2

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
41	VNGR-20671	Interoperability	In a 512 Kbps conference with CP Auto Layout, Gathering, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, an Tandberg C90 H323 endpoint cannot view content from VSX7000A H320 endpoint.	V7.2
42	VNGR-20670	Interoperability	In a 512 Kbps conference with CP Auto Layout , Gathering, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, an Scopia XT1000 H323 endpoint cannot view content from VSX7000A H320 endpoint.	V7.2
43	VNGR-20658	SIP	Only 97 conferences could be registered with the SIP server, although the limitation is 1000, and an active alarm is displayed: RMX reached to the limitation of registration.	V7.2
44	VNGR-20633	IVR	In the conference IVR Service, you cannot preview the default gateway slide from RMX Client.	V7.1
45	VNGR-20625	Interoperability	In a 4096 Kbps CP conference with Auto Layout , Gathering, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, when an SIP VSX8000 endpoint connects to a SIP VSX7000A endpoint, they do not view video.	V7.2
46	VNGR-20603	Interoperability	An RMX 4000 with version 7.2.0.78 and MPMx cards, when starting a conference, HDX8006 endpoint connected as Audio only.	V7.2
47	VNGR-20571	Interoperability	On an RMX 1500 after configuring the DNS and SIP server, registration failed on the Cisco VSC.	V7.2
48	VNGR-20568	ISDN	When two conferences are created with the same profile and then cascaded, when ISDN endpoints connected, Video Sync Loss issues were encountered.	V7.2
49	VNGR-20547	Interoperability	On an RMX 2000 when the flag MULTIPLE SERVICES is set to NO, the DNS cannot be configured in IP Management Service.	V7.2
50	VNGR-20545	Interoperability	In a 4096Kbps conference with Send Content to Legacy Endpoints enabled, when connecting Legacy endpoints the decoder failed to release.	V7.2
51	VNGR-20544	Diagnostics	When running RTM IP diagnostic tests the load MPM1 test is missing.	V7.2

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
52	VNGR-20537	<i>RMX Manager</i>	After making changes and selecting restart in Hardware Monitor, when clicking "NO" in the confirmation pane, the RMX automatically resets, the login screen appears and changes are lost.	V7.2
53	VNGR-20514	<i>General</i>	On RMX 1500 with MPMx High System CPU Usage, a "High CPU utilization" and "Low processing memory" alert occurs.	V7.0.2
54	VNGR-20504	<i>General</i>	After starting a 2024Kbps conference from a Profile with Content enabled, when dialing out to an H.323 (HDX8000) endpoint and then disconnecting and then reconnecting using SIP, the drop down properties are not changed to SIP.	V7.2
55	VNGR-20489	<i>Upgrade Process</i>	When Upgrading from version 7.2.0.68\7.0.2.69 to 7.0.2.70 the process took to long (40 min.).	V7.2
56	VNGR-20474	<i>RMX Manager</i>	re-opening the network services tab on the saved Profile, the SIP registration check-box is not selected.	V7.2
57	VNGR-20467	<i>Interoperability</i>	In a 1024 Kbps conference with AES enabled, after connecting LYNC endpoints, green artifacts appeared in the video.	V7.2
58	VNGR-20466	<i>SIP</i>	After configuring the RMX and assigning a PROXY, after adding a new participant and then dialing out using SIP, the endpoint cannot connect.	V7.2
59	VNGR-20465	<i>RMX Manager</i>	When accessing the RMX Shelf Manager the banner does not display the RMX type.	V7.2
60	VNGR-20452	<i>RMX Manager</i>	On any RMX type, after completing the Backup and Restore functions, RMX Time is remain unchanged.	V7.2
61	VNGR-20443	<i>Software Version</i>	Active Alarm triggered by high CPU usage during RMX2000 startup.	V7.5
62	VNGR-20427	<i>General</i>	When the RMX is configured to Multiple Services after a system reset an active alarm appeared: "process is approaching memory utilization limit 80%".	V7.2
63	VNGR-20393	<i>General</i>	When defining the RMX Time and selecting "use NTP server" check box, if a single IP address is added then a message alert "please enter valid address" appears.	V7.2

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
64	VNGR-20390	<i>SIP</i>	After specifying Avaya Session Manager as the SIP server, the SIP dial-out connection failed on the RMX.	V7.2, V7.6
65	VNGR-20381	<i>Interoperability</i>	In a 512 Kbps CP conference with Auto Layout , Gathering, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, HDX7001 and HDX9001 endpoints display video stretched vertically in 4SIF calls.	V7.2
66	VNGR-20371	<i>General</i>	When the RMX and HDX endpoints are registered to a Broadsoft gatekeeper, after the VSW conference was started from a Profile, HDX endpoints failed to or partially connected to the conference.	V7.2
67	VNGR-20365	<i>Interoperability</i>	In a 768 Kbps conference, after connecting HDX, VSX, CMAD and Lync endpoints, HDX,VSX, CMAD endpoints view elliptical video from Lync endpoints.	V7.2
68	VNGR-20364	<i>IVR</i>	After Upgrading from V7.1.0.121 to V7.2.0.64 all IVR Profiles are missing.	V7.2
69	VNGR-20345	<i>Interoperability</i>	On an RMX1500 running a 2048 Kbps conference with LPR and AES enabled, when the H.320 HDX 7006 dials out to H.323 HDX 4500, the video from the HDX freezes and has artifacts.	V7.2
70	VNGR-20333	<i>General</i>	Message Overlay does not update after clicking Apply.	V7.2
71	VNGR-20330	<i>RMX Manager</i>	On the RMX 2000, the LAN Tab in the Management network properties pane is missing.	V7.1
72	VNGR-20313	<i>Partners - Microsoft</i>	Call line rate of HDX endpoints downspeed when connected to a conference running on RMX system using RTV video protocol. RMX and HDX endpoints are registered to the same Microsoft Lync server.	V7.2
73	VNGR-20299	<i>Interoperability</i>	In a 1MB CP conference started from a profile, when changing the layout with Click & View, CMAD endpoints view artifacts in their video.	V7.2
74	VNGR-20293	<i>General</i>	On an RMX 4000 with a number of calls, an error message: "Voltage problem in PWR1", keeps reappearing.	V7.2

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
75	VNGR-20289	ISDN	When a dial-in ISDN participant connected to the conference using a PRI line, all audio only endpoints experienced echo.	V7.0.2
76	VNGR-20222	General	After a Hot backup changeover, a SIP dial-in participant was not reconnected on the new Master RMX	V7.2
77	VNGR-20221	General	After a RMX Hot backup changeover, a "Core Dump" message appears.	V7.2
78	VNGR-20206	General	When on the Master MCU the LAN cable Disconnects, the Slave MCU does not become the Master and Hot backup functionality failed.	V7.2
79	VNGR-20141	Upgrade Process	After upgrading from version 7.1.0.121 to 7.2.0.57 a "Core Dump" message appears.	V7.2
80	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.	V7.5
81	VNGR-20133	SIP	In the IP Network Service Properties - SIP Servers properties, the RMX is registered to the Lync SIP server but the Status shows is listed as Fail, however SIP calls can be made and the registration status is incorrect.	V7.2
82	VNGR-20122	Interoperability	On an RMX 1500 running a conference, after connecting HDX9004 and FX 6.0.5 endpoints, green artifacts appeared in their video.	V7.2
83	VNGR-20093	General	On an RMX2000 with MPM+40 cards, when adding ISDN endpoints the Central Signaling module crashes.	V7.0.2
84	VNGR-20070	IVR	In the IVR Services - Welcome tab after "Enabling Welcome Messages " and selecting and Adding a Message File , when clicking Yes there is no response and no IVR file is added.	V7.2
85	VNGR-20062	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
86	VNGR-20050	Interoperability	On an RMX 2000 with MPMx cards running a conference, after connecting a Lync endpoint and attempting to start PCM with ##, the PCM does not load.	V7.2

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
87	VNGR-20041	<i>Content</i>	On an RMX 2000 with MPMx cards running a conference, when a Legacy endpoint sends Content, the Content is cut off and appears cropped.	V7.2
88	VNGR-20028	<i>Interoperability</i>	On an RMX 2000 with MPMx cards running a conference, after connecting a Lync endpoint the Blast Presence function does not appear in the menu list.	V7.2
89	VNGR-19982	<i>Hot Backup</i>	When the Master MCU is turned off in a Hot backup configuration activates as required, however a "core dump" alarm is activated.	V4.7.1
90	VNGR-19933	<i>Hot Backup</i>	When the Master MCU in a Hot backup configuration fails and the Slave MCU activates, in the participant properties information is missing.	V4.7.1
91	VNGR-19932	<i>Hot Backup</i>	When the Master MCU in a Hot backup configuration fails and the Slave MCU activates, DNS host name still lists the _bck (backup) extension.	V4.7.1
92	VNGR-19928	<i>Content</i>	Chroma shift viewed on Legacy endpoints when sending content in a conference running on RMX 2000 with MPMx at a line rate of 512kbps and the Send Content to Legacy Endpoint option enabled.	V7.2
93	VNGR-19927	<i>Interoperability</i>	Register the RMX to the Lync server and then start a new conference, when SIP endpoints connect they do not view the Welcome Slide.	V7.2
94	VNGR-19925	<i>Hot Backup</i>	In a Hot backup configuration both the Master and Slave RMX are registered with same prefix to the Gatekeeper and calls cannot connect.	V4.7.1
95	VNGR-19915	<i>General</i>	When dialing out to an H.323 HDX endpoint and then disconnecting and then reconnecting using SIP, the drop down properties are not changed to SIP.	V7.6
96	VNGR-19909	<i>Hot Backup</i>	When the Master MCU in a Hot backup configuration fails and the Slave MCU activates, the recording link is not copied from master to slave.	V4.7.1
97	VNGR-19891	<i>Interoperability</i>	On an RMX 2000 running a conference, after connecting HDX9004 HDX7006, HDX8006, VSX8000, VSX8000, iPower9000, ViewStation MP512, ViewStation FX endpoints, the ISDN HDX7006 endpoint viewed green artifacts in the video and 15 minutes later disconnected.	V7.2



**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
98	VNGR-19888	IVR	On an RMX 2000 running a 128 Kbps conference, after connecting HDX9004 HDX7006, HDX8006, VSX8000, VSX8000, iPower9000, ViewStation MP512, ViewStation FX endpoints, the ISDN HDX7006 endpoint continuously views the Welcome screen.	V7.2
99	VNGR-19884	ISDN	During a Conference with High Profile enabled, H.320 endpoints view bad video.	V7.2
100	VNGR-19881	Content	Chroma shift viewed on Legacy endpoints when sending content in a conference running on RMX 2000 with MPMx at a line rate of 512kbps and the Send Content to Legacy Endpoint option enabled.	V7.5
101	VNGR-19880	Interoperability	On an RMX with MPMx cards when connecting HDX endpoints using their own subnet the endpoints encounter 15% packet loss during conferences.	V7.0.2
102	VNGR-19856	Interoperability	On an RMX 2000 with MPM+ cards, start a Conference from a Profile with multiple HDX4000/8000 endpoints, after connecting a dial-out SIP H.261 endpoint, no video could be seen.	V7.2
103	VNGR-19781	Interoperability	On an RMX 1500 in a Real Life 384 Kbps conference, all endpoints have their audio and video halted for 25 seconds.	V7.2
104	VNGR-19759	General	When configuring Multiple Networks on the RMX 2000, the RMX2000_RTM_LAN flag must be set to YES in addition to the MULTIPLE_NETWORKS=YES flag.	V7.1
105	VNGR-19736	Video	During a 512 Kbps COP conference in a Lecture Mode with HDX, VSX and VVX endpoints, when switching the Lecturer, the video is interlaced with artifacts.	V4.7.1
106	VNGR-19722	General	Audio card fails to initialize during startup on RMX4000 resulting in no utilizable unit for audio controller. Reset the RMX to correct the problem.	V7.5
107	VNGR-19686	IP	On RMX 2000/4000, system reboots, displays several alarms and remains unresponsive after trying to configure IPv6 addressing mode.	V7.0.2
108	VNGR-19683	Video	On an RMX 2000 with 2 MPMx cards when connecting 120 SD endpoints, jumpy video & video freezes occur.	V4.7.1

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
109	VNGR-19645	<i>Hot Backup</i>	When Hot Backup is disabled in the Master, the Slave status remains OK.	V4.7.1
110	VNGR-19638	<i>Video</i>	In a COP conference with 8 endpoints, when changing multiple layouts and speakers, an assert occurs.	V4.7.1
111	VNGR-19633	<i>Video</i>	In a COP conference with four levels and 120 endpoints, errors appeared after participants disconnected and reconnected.	V4.7.1
112	VNGR-19598	<i>Video</i>	In a 1080p VSW conference with Motion and Sharpness enabled on the HDX8000 endpoints, green artifacts can be seen in the video slide.	V4.7.1
113	VNGR-19566	<i>Upgrade Process</i>	After upgrading to version 7.1.0.121 on an RMX 1500, the following message appears: "FAILED to start during Startup !!!".	V7.1
114	VNGR-19562	<i>IP</i>	On RMX 2000/4000, system reboots, displays several alarms and remains unresponsive after trying to configure IPv6 addressing mode.	V7.0.2
115	VNGR-19363	<i>Audio</i>	On an RMX 2000 during an ISDN call, frequently audio echo can be heard during the conference.	V7.0.2
116	VNGR-19300	<i>HD</i>	On an RMX 1500, when the system flag and resolution are set to SD, HD resolutions are available.	V7.2
117	VNGR-19230	<i>Video</i>	In a COP conference with Static Message Overlay and Static enabled, the display does not appear in the middle of the Layout when it should.	V4.7.1
118	VNGR-19228	<i>RMX Manager</i>	After upgrading to version 4.7.1 the Address Book appears empty and does not respond.	V4.7.1
119	VNGR-19164	<i>General</i>	On the RMX 1500/2000, the Event Log Tab in Hardware Monitor pane does not show the Event Log with their status.	V7.1
120	VNGR-19114	<i>ISDN</i>	In an 1472 Kbps CP ISDN conference with Encryption, Gathering, LPR, Sharpness and Video Clarity enabled, when sending content from an VSX7000A endpoint, VSX8000 endpoints cannot view content.	V7.1
121	VNGR-19095	<i>General</i>	Fast Configuration Wizard does not appear after license activation has completed.	V7.5

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
<b>122</b>	VNGR-19065	<i>General</i>	If setting the Gatekeeper prefix to the digits that are used for Conference ID (for example prefix is set to 10 and the conference ID is 1001), the system will not be able to dial to the destination conference as the prefix digits are truncated from the conference ID, preventing the system from locating it.	V7.1
<b>123</b>	VNGR-18947	<i>CMA</i>	In a 832 Kbps H.323 conference registered with the CMA, when connecting CUPC, CMA-D and HDX endpoints the video is bad.	V7.1
<b>124</b>	VNGR-18917	<i>Video</i>	In a 1920 Kbps H.323 conference with AES and LPR enabled, when an HDX endpoint views the Welcome Slide there is no video in the background.	V7.1
<b>125</b>	VNGR-18811	<i>General</i>	An RMX1500 with a Permanent Meeting Room enabled, the conference properties displays the conference duration values prior to Permanent check box selection.	V7.0.2
<b>126</b>	VNGR-18691	<i>Hot Backup</i>	In a Hot backup configuration the Master is registered with an alias and prefix to the Gatekeeper, however on the Slave the Alias does not appear.	V4.7
<b>127</b>	VNGR-18669	<i>IVR</i>	On the RMX 4000, IVR Service Properties tab you cannot upload the Welcome Slide after clicking OK.	V4.7
<b>128</b>	VNGR-18668	<i>Multilingual</i>	The words "Enable Gathering Phase" are not translated into Simplified Chinese.	V7.1
<b>129</b>	VNGR-18606	<i>Interoperability</i>	An RMX 2000 and endpoints are registered with a Broadsoft proxy, when the dial-in conference starts from an LPR enabled Profile, HDX endpoints connect with problems.	V7.1
<b>130</b>	VNGR-18588	<i>Upgrade Process</i>	During the upgrade from version 4.7 an unexpected reset occurred on a media card.	V4.7
<b>131</b>	VNGR-18542	<i>RMX Manager</i>	After defining a permanent conference's properties and reopening the conference properties, In the General tab the End Time field still appears.	V4.7
<b>132</b>	VNGR-18314	<i>Hot Backup</i>	When Hot Backup is disabled in the Master, the Master status is not updated on the Slave.	V4.7
<b>133</b>	VNGR-18285	<i>Hardware</i>	After removing manually an MPMx card from the RMX4000, an assert appears.	V4.7

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
134	VNGR-18259	General	The Log and faults files are time stamped at different times, when the time should be concurrent.	V7.0
135	VNGR-17914	Interoperability	When two IBM Sametime clients connect to a conference, the ST client connecting from a desktop views video artifacts.	V7.1
136	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
137	VNGR-17830	Diagnostics	With version 7.2.0.38 on an RMX2000 with two MPMx cards, when running diagnostic tests on all components, test 115 LAN Load CNTL failed.	V7.6
138	VNGR-17778	RMX 4000	When trying to connect 180 V500/VSX to each of the two conferences running simultaneously on RMX 4000 with 4 MPMx-D cards, both conferences running at a line rate of 384, Video Quality set to Motion and Max CP resolution set to CIF, 180 participants connected to the first conference, while several participants out of the 180 could not connect to the second conference.	V7.0.2
139	VNGR-17653	General	An RMX 1500 failed to ping devices within the network and can't establish connection to the exchange server.	V7.0.1
140	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
141	VNGR-17524	General	When using Internet Explorer version 6.0/7.0 on an RMX 4000 version 7.0, you cannot upload a video resolution slide in the IVR - Video Services tab.	V7.0
142	VNGR-17342	IVR	After attempting to upload a video slide in the IVR Service Properties, the corrupted video slide then cannot be deleted.	V7.0
143	VNGR-17306	Diagnostics	After accessing the Logger Files, an Active Alarm was triggered: "Logger Process startup exceeded allowed time under Process idle code".	V6.0
144	VNGR-17082	Video	On an RMX 2000/4000 with an Ad-hoc conference when the Avaya 1XC Softphone and HDX 9004 dial-in to the conference, they view discoloration in the upper segment of their video.	V7.0

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
<b>145</b>	VNGR-17070	<i>Interoperability</i>	On an RMX 4000 with MPM+ cards, when running a 512 Kbps conference with Echo suppression enabled and HDX 8000 and VSX 3000 endpoints connected, audio cuts ON and OFF.	V7.0
<b>146</b>	VNGR-16807	<i>Content</i>	Bad audio quality experienced on PVX endpoint while it sends content when connected to RMX 1500.	V7.0
<b>147</b>	VNGR-16806	<i>Interoperability</i>	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
<b>148</b>	VNGR-16785	<i>Hardware</i>	Run 8 512Kbps conferences and connect to each conference 2 H.323, 2 SIP, 1 ISDN, 1 PSTN & 1 VOIP endpoints, change the conference layout on each, when terminating the conferences an "MCU Internal Problem 50020" occurred on the MPMx cards.	V7.0
<b>149</b>	VNGR-16646	<i>Interoperability</i>	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
<b>150</b>	VNGR-16644	<i>Interoperability</i>	In a conference started from the default conference profile, when the RMX dials-out to the H.323 iPower 9000 endpoint, it views the IVR welcome screen for about 40 seconds before viewing conference video.	V7.0
<b>151</b>	VNGR-16617	<i>IP</i>	When CMAD endpoint running on Lenovo R61 connects to a Meeting Room whose Line rate is 1024 Kbps, Video quality is set to Motion, Content is set is HiResGraphics and LPR, Same Layout and Echo Suppression option are enabled, after few minutes in the conference the CMAD observes packet loss in the People Rx although QoS is enabled	.V7.0
<b>152</b>	VNGR-16529	<i>General</i>	After Restoring Factory Defaults on the RMX and defining the IP Network Service, after RMX restart the MCU Host Name parameter appears empty in the "Management Network - DNS" tab.	V7.0
<b>153</b>	VNGR-16447	<i>General</i>	When you add an MCU to RMX Manager (v6, v7) the password is displayed in plain text if you selected the "Remember Login" check box during Login.	V6.0.1
<b>154</b>	VNGR-16297	<i>Interoperability</i>	CMAD receives distorted video while calling to RMX.	V7.0

**Table 1-6** Corrections Between Version 7.2.2 and Version 7.6

#	Key	Category	Description	Detected in Version
155	VNGR-16044	General	After downloading and opening an auditor file of the MPMx, the MPMx name appears as MPM_PLUS.	V7.0
156	VNGR-15906	Interoperability	when connecting SIP/H.323 HDX & PVX dial-in and dial-out endpoints to a conference running at a line rate of 384Kbps with no IVR on an MCU whose resources are set to Fixed Mode, low quality video is received by the SIP endpoints.	V7.0
157	VNGR-15637	General	After creating a conference template with 6 participants, when adding and removing participants to a conference the template does not update.	V7.0
158	VNGR-14739	Interoperability	When a Codian ISDN GW 8321 accesses the RMX via an Entry Queue and then enters the Meeting Room, video loopback could not be seen.	V5.0.0
159	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
160	VNGR-10849	Interoperability	A black screen may appear in the following instances: * On HDX8000 HD Hardware version B endpoints when the conference line rate is set in the range of 256-768 Kbps. (The Hardware version can be found on the HDX endpoint's System Information page.) * On HDX SD endpoints using the PAL mode when the conference line rate is set above 128 Kbps.	V4.1
161	VNGR-9571	Hardware	In D-type chassis, when hot-swapping an MPM card, unit failure may occur.	V4.0.0
162	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

## Version 7.6.1 System Limitations

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
1	VNGR-24435	<i>Event Mode</i>	When creating an Event Mode Profile without selecting Same Layout or Lecture Mode in the Video Settings tab, an error message is displayed, the RMX Web Client freezes when trying to access the Video Settings tab followed by logout from the RMX Web Client.	V7.6.1	
2	VNGR-24433	<i>Hardware</i>	In the Hardware Monitor when the RMX 1500 fan speed is at 16000RPM and the operating temperature is a low 5C, the fans statuses are in Major.	V7.6.1	
3	VNGR-24430	<i>Hardware</i>	In the Hardware Monitor when the RMX 2000/4000 fans speed is at 40% and the operating temperature is low, the fans statuses are in Major.	V7.6.1	
4	VNGR-24363	<i>Encryption</i>	When RMX 2000 (V7.6.1) is connected to OpenScapeVoice over TLS (MTLS), ODC-PE and ODC-WE cannot decrypt the Audio and Video received from RMX, and they appear as "connected with Problem" in the RMX Web Client/Manager	V7.6.1	
5	VNGR-24249	<i>Interoperability</i>	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.
6	VNGR-24209	<i>General</i>	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.
7	VNGR-24199	<i>Video</i>	In a conference set to Auto Layout and 6 connected endpoints, the automatically selected layout was 2x2 instead of 5+1 resulting with an endpoint missing from the layout.	V7.6.1	
8	VNGR-24182	<i>Diagnostics</i>	When the RMX is in a Diagnostic mode, in the Hardware Monitor, Loop Tests fail on the ISDN card.	V7.6.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
9	VNGR-24132	Interoperability	In a conference set to Motion, MOC and Lync clients connect in VGA video instead of HD 720p.	V7.6.1	
10	VNGR-24072	Interoperability	On an RMX 1500, calls from a Cisco SIP phone to VRM fail when routed over an H.323 CUCM trunk to DMA (pre-release 4.0.2).	V7.6	
11	VNGR-24071	Video	In a CP conference with a Lync client connected, the clients video jumps between HD and QCIF VGA.	V7.6.1	
12	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	
13	VNGR-23902	Audio	When self muting the VVX1500 endpoint during a conference running on the RMX, the audio mute icon does not appear in the Participants pane of the RMX Web client/ Manager.	V7.7	
14	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	
15	VNGR-23767	Partners - Microsoft	Microsoft R1 is not supported with the RMX systems.	V7.6.1	
16	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	
17	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	
18	VNGR-23267	General	Message Overlay parameters are not saved when saving the ongoing conference to a template.	V7.6.1	
19	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	
20	VNGR-23182	General	In cascaded conferences with Message Overlay enabled, participant line rate and frame rate may decrease.	V7.0.2C	



**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
21	VNGR-23123	General	During a conference, many endpoints could not connect, and intermittently viewed the Welcome Slide for just a few seconds.	V7.1	
22	VNGR-23061	Cascading	A Slave conference cannot be connected to two Master conferences simultaneously.	V7.0.2C	
23	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	
24	VNGR-22893	General	HDX endpoints may randomly connect to a conference set to 1080p resolution and Sharpness video quality at a frame rate lower than 30 fps when called by RMX 1500 using blast dial-out.	V7.2.2	
25	VNGR-22840	Interoperability	Siemens endpoints cannot connect to conference with TIP Compatibility enabled when running on an RMX configured with Multiple Network Services.	V7.6	
26	VNGR-22830	General	When configuring the RMX with Multiple Network Services and defining the DNS for each Network Service, after RMX reset the Lync client cannot connect to the RMX as it cannot resolve the RMX address using the configured DNS.	V7.6	
27	VNGR-22828	Partners - Microsoft	The aspect ratio of the video display on the Lync client running on a MAC workstation is always 4:3 and does not change according to the actual screen aspect ration (16:9), after changing the Video layout from a big screen to a smaller screen.	V7.6	
28	VNGR-22824	Partners - Microsoft	After upgrading from version 7.2.2 to 7.6, the Faults List of the RMX registered to a Lync server occasionally reports DSP crashes.	V7.6	
29	VNGR-22815	Interoperability	HDX endpoints are stuck at the IVR Welcome slide with no audio when connecting to an encrypted conference through the DMA over TLS.	V7.6	
30	VNGR-22801	General	On an RMX with MPMx cards, when Message Overlay is enabled in a conference, the frame rate of the endpoints may drop due to bandwidth consumption.	V7.2.2	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
31	VNGR-22796	General	When the RMX is in a Diagnostic mode, in the Hardware Monitor, Loop Tests fail on the ISDN card.	V7.6	
32	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	
33	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	
34	VNGR-22694	Video	Lync clients may randomly connect at frame rate lower than 30 fps when connecting to a conference at a line rate of 768Kbps and a resolution of 720p.	V7.6	
35	VNGR-22657	Upgrade Process	When initiating a downgrade from version 7.6 to 7.5.0/ 7.5.1 on the RMX 1500Q, the Safe Software Version Installation alarm message is not generated warning that you cannot perform the downgrade.	V7.6	
36	VNGR-22648	Interoperability	In a dial-out SIP conference on the RMX 1500, Polycom Immersive TelePresence rooms are not receiving content from DMA registered HDX endpoints or CUCM registered CTS endpoints.	V7.6	
37	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	
38	VNGR-22646	Security	When the RMX is set to a Maximum Security Mode, verify that there are address book entries, when disconnecting the LAN cables, the LAN connection is lost but the entry book entries are not cleared. The RMX Address Book entries should no longer be displayed when the connection to the RMX is lost as this could lead to disclosure of information to unauthenticated users.	V7.6	
39	VNGR-22636	SIP	When starting a 348 kbps conference from a profile on the RMX with LPR and Encryption disabled, after connecting LifeSize and a HDX endpoint using SIP, the Content channel and SIP BFCP on the Lifesize endpoints are turned off.	V7.6	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
40	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	
41	VNGR-22620	Content	In a 1472 kbps conference with H.239 content enabled, H.320 HDX endpoints view frozen or black video slides.	V7.6	
42	VNGR-22569	Video	After viewing the Gathering screen and changing layouts, HDX endpoints view a green bar on the bottom of their video where the participant's name should appear.	V7.6	
43	VNGR-22560	Calendaring	When the Cascading Link Participant is connected on each end (Master Conference/ Slave Conference) to a different gatekeeper, link may fail to reconnect if it was previously disconnected and the re-dialing occurs before the disconnection process was terminated.	V7.0.2C	
44	VNGR-22533	General	In a conference with Recording enabled, after dialing out to an H.320 HDX, the HDX does not view the recording icon.	V7.6	
45	VNGR-22532	Partners - Microsoft	After a Lync 2010 Client enables its video to full screen, the gathering phase disappears but reappears when reverting to the initial video layout.	V7.6	
46	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.
47	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 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
48	VNGR-22431	<i>Interoperability</i>	When Telepresence endpoints connect with a problem to a conference set to Auto Telepresence Mode and Telepresence Layout Mode, instead of their cell display being blank, video from other Telepresence endpoints is displayed in those cells.	V7.6	
49	VNGR-22407	<i>General</i>	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	
50	VNGR-22390	<i>General</i>	After changing the gatekeeper registration on the RMX 1500/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	
51	VNGR-22353	<i>Video</i>	In a Telepresence conference, when a Telepresence endpoint disconnects from the conference the video from another endpoint that is still in the conference is displayed briefly where the disconnected endpoint used to be displayed.	V7.6	
52	VNGR-22334	<i>RMX Manager</i>	When the RMX is set to a Maximum Security Mode, login with the RMX Manager as an Administrator and then select Hardware Monitor, the Shutdown button is disabled for no apparent reason.	V7.6	
53	VNGR-22319	<i>Software Version</i>	Lans List - Ethernet Settings dialog box doesn't display all of the LANS in the RMX.	V7.2.2	
54	VNGR-22217	<i>General</i>	After removing an MPM+80 card from an RMX 4000, the <i>Video/Voice Port Configuration</i> dialog box is not updated and does not reflect the change in port number.	V7.2.2	
55	VNGR-22208	<i>IVR</i>	When using Internet Explorer version 8.0, you cannot upload a low resolution Welcome slide in the IVR - Video Services tab.	V7.6	
56	VNGR-22181	<i>General</i>	In the Hardware Monitor, Slots 1 & 2 may sometimes appear as duplicates in the Slot list.	V7.6	
57	VNGR-22158	<i>RMX Web Client</i>	After configuring RMX's IP and default router IP address correctly in the Network Services, you cannot Ping the RMX address using the RMX Client.	V7.6	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
58	VNGR-22100	<i>Hot Backup</i>	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	
59	VNGR-22018	<i>Partners - Microsoft</i>	Click to Conferences is supported only with Microsoft OCS R2 and Lync clients. HDX endpoints are not supported.	V7.6	
60	VNGR-21902	<i>Event Mode</i>	In an Event Mode conference with Lecture Mode enabled, only the Lecturer can see the Message Overlay text, while other participants on the lecturer's level cannot. Participants on other levels can see the Message Overlay text.	V7.6	
61	VNGR-21878	<i>Video</i>	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	
62	VNGR-21780	<i>Event Mode</i>	Siren 14 audio protocol is not supported in Event Mode conferences.	V7.6	
63	VNGR-21748	<i>General</i>	In an Event Mode conference, after selecting an HDX to be the chairperson, nothing happened when using a PCM remote control to Mute& Block audio / suspend video of the chairperson.	V7.6	
64	VNGR-21729	<i>General</i>	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	
65	VNGR-21514	<i>Software Version</i>	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	
66	VNGR-21429	<i>Audio</i>	HDX endpoints with versions prior to 3.0.3 fail to connect to conferences when SirenLPR is enabled on the RMX.	V7.6	
67	VNGR-21396	<i>Recording</i>	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	
68	VNGR-21159	<i>IVR</i>	In the IVR Services when replacing/changing a music file and clicking on Play, the music file does not start.	V7.6	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
69	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.
70	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.
71	VNGR-20918	General	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.	V7.2	
72	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	
73	VNGR-20855	SIP	When resetting the RMX from the Hardware Monitor, SIP endpoints may remain connected, although the conference ended.	V7.2	
74	VNGR-20854	Upgrade Process	The installation of a new RMX software fails when performed while there are ongoing conferences and all the command buttons in the Software Installation dialog box including the Cancel button are disabled. The only way to close this dialog box is by clicking its X button on the top right corner.	V7.2	
75	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	
76	VNGR-20783	Upgrade Process	Sometimes during upgrade, the message "Activation key required" is not displayed.	V7.0.3	
77	VNGR-20752	Video	In a 4 MB 720p Sharpness conference on an RMX with MPMx cards, LifeSize Express 220 endpoints view video with tiling and artifacts.	V7.2	
78	VNGR-20738	SIP	The Meeting Room and Entry Queue are register twice with the SIP registrar instead of once.	V7.2.1	
79	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
80	VNGR-20723	<i>Software Version</i>	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	
81	VNGR-20660	<i>Interoperability</i>	When registered to an Avaya Aura proxy server and starting a 2Mb conference with Content, after connecting HDX, Legacy & Avaya Video Conferencing System (1000-series) endpoints, the Avaya and Legacy endpoints cannot not view content.	V7.2	
82	VNGR-20646	<i>General</i>	After reducing the header packet size using the system flag; MTU_SIZE, the MCMS doesn't calculate the additions (IP header, UDP header, encryption, LPR etc.), and therefore packets are exceeding the allowed size as set in the flag.	V7.6.1	
83	VNGR-20645	<i>General</i>	After reducing the header packet size using the system flag; MTU_SIZE, the MCMS doesn't calculate the additions (IP header, UDP header, encryption, LPR etc.), and therefore packets are exceeding the allowed size as set in the flag.	V7.0.1	
84	VNGR-20637	<i>IP</i>	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.	V7.2	
85	VNGR-20608	<i>Interoperability</i>	After registering the RMX 1500 to the VCS as Generic server type and starting a conference, when connecting MOC endpoints and sending DTMF "****", Click & View does not load.	V7.2	
86	VNGR-20574	<i>Software Version</i>	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	
87	VNGR-20572	<i>Interoperability</i>	On an RMX 1500, after configuring the SIP server & domain, registration failed with the Cisco VSC.	V7.2	
88	VNGR-20534	<i>Content</i>	In a 128Kbps conference with content started from a Profile, when 20 ISDN endpoints connected the video froze.	V7.2	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
89	VNGR-20521	<i>RMX Manager</i>	On an RMX with Multiple Services enabled, when configuring the Network service to support LYNC server, after resetting the RMX an active alarm "SIP secured communication failed" appears.	V7.2	
90	VNGR-20492	<i>RMX Manager</i>	Previously on the RMX Manager you could Login and Logout in version 7.2 after viewing a "browser env. error" message you need to close all browsers sessions and re-login.	V7.2	
91	VNGR-20478	<i>RMX Manager</i>	Internet Explorer 8 crashed while loading the RMX Manager.	V7.2	Not an RMX issue - an Internet Explorer issue.
92	VNGR-20434	<i>General</i>	When Hot Swapping MPM+/MPMx cards, Port Usage and Resource reports do not display correctly.	V7.2	
93	VNGR-20432	<i>Diagnostics</i>	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	
94	VNGR-20419	<i>General</i>	In the Network Traffic Capture (Administration-->Tool-->Network Traffic Capture) pane select Start Network Traffic Capture. No network traffic capture file of Central Signaling (CS) created.	V7.2	
95	VNGR-20416	<i>General</i>	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	
96	VNGR-20406	<i>General</i>	On the RMX 1500/2000 High CPU utilization may occur during startup.	V7.0.3	
97	VNGR-20372	<i>General</i>	During RMX 4000 startup, the following message appears: "No connection to switch". This message is not displayed in the Hardware Monitor.	V5.0.2	
98	VNGR-20357	<i>General</i>	After creating a new conference and adding a new participant, in the General Tab, the Extension/Identifier String always deleted number of characters after clicking OK.	V7.2	
99	VNGR-20353	<i>Interoperability</i>	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.



**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
100	VNGR-20326	<i>Interoperability</i>	When the RMX and HDX endpoints are registered with a CMA, after dialing out from an HDX endpoint a numerical error message appears.	V7.2	
101	VNGR-20321	<i>Interoperability</i>	When the RMX1500 system is started on the MPMY card an IPMC message: "A2D read error" appears.	V7.2	
102	VNGR-20317	<i>Partners - Microsoft</i>	Microsoft Lync client disconnected from a conference running on an RMX2000 with MPMx cards several minutes after connecting to the Meeting Room.	V7.2	
103	VNGR-20305	<i>General</i>	On an RMX 2000, after accessing; Setup>> Ethernet Settings pane, the properties listed belong to an RMX 4000.	V7.2	
104	VNGR-20297	<i>Video</i>	On an RMX with multiple Serves enabled, when a 2 MB conference is started from a template and three H.323 HDX dial-in endpoints connect, no video could be seen.	V7.2	
105	VNGR-20273	<i>Upgrade Process</i>	On an RMX 4000, after downgrading from version 7.0.2.0.61 to 5.0.2.9, the following message appears: " No connection to switch".	V7.2	
106	VNGR-20269	<i>ISDN</i>	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	
107	VNGR-20267	<i>General</i>	When terminating a 384 Kbps conference with 60 CIF participants, its takes more than 30 seconds for the conference to close.	V7.2	
108	VNGR-20262	<i>Upgrade Process</i>	When downgrading from version 7.2.0.61 to version 7.0.2.69, the IP addresses of default IP Network Service that were defined via the Fast Configuration Wizard are erased and must be redefined.	V7.2	
109	VNGR-20247	<i>Video</i>	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 Telpresence mode. The display is updated after the next layout change	V7.2	
110	VNGR-20243	<i>Hardware</i>	On an inactive RMX 1500, an active alarm: " High CPU utilization - Process CPU usage is high:99%" appears.	V7.2	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
111	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	
112	VNGR-20207	General	After using the USB method of restoring to factory defaults, the RMX should no longer be in Ultra Secure mode but in the Management Network IP tab the "Secure Communication" check box remains selected.	V7.6	
113	VNGR-20195	Partners - Microsoft	On an RMX with MPM+ cards running a 384 kbps CP conference with LPR and Encryption enabled, after connecting two Lync endpoints, green artifacts appear briefly in the video.	V7.2	
114	VNGR-20152	Interoperability	On an RMX 1500 running an 4096 kbps CP conference with Auto Layout, LPR, Sharpness, Video Clarity, Graphics and Send Content to Legacy Endpoints enabled, after sending content from an HDX9006, the LifeSize Express 220 endpoint displays video tiling and ghosting.	V7.2	
115	VNGR-20097	Cascading	During a Cascaded conference, the cascaded link sometimes send a "need help" message to participants.	V6.0.1	
116	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	
117	VNGR-20048	General	After changing the conference name and the Profile to the SIP Registration profile and then clicking OK, the changes do not take affect nor are they registered.	V7.2	
118	VNGR-20036	Video	When attempting to switch the Lecture Mode between endpoints, the video froze.	V4.7.1	
119	VNGR-20000	Video	On an RMX4000 with 4MPMx cards, during an Event Mode conference when participants connected using different Line Rates, processing units failed.	V4.7	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
120	VNGR-19952	<i>Upgrade Process</i>	On an RMX 1500, a Power Supply voltage active alarm is triggered in error on sensor 8.	V4.7.1	
121	VNGR-19889	<i>Video</i>	During a 1728 Kbps Cascaded (RMX 2000 to MGC) COP conference with 12 dial-in and dial-out endpoints, endpoint's video border's and edges smudge.	V4.7.1	
122	VNGR-19881	<i>Content</i>	Chroma shift viewed on Legacy endpoints when sending content in a conference running on RMX 2000 with MPMx at a line rate of 512kbps and the Send Content to Legacy Endpoint option enabled.	V7.5	
123	VNGR-19879	<i>General</i>	During a conference, many endpoints could not connect, and intermittently viewed the Welcome Slide for just a few seconds.	V7.1	
124	VNGR-19873	<i>ISDN</i>	During a Conference with High Profile enabled, H.320 endpoints view bad video.	V7.2	
125	VNGR-19826	<i>Video</i>	During a 1536 Kbps conference with HDX and VVX endpoints, when a H.263 CIF participant views a H.263 4CIF participant, the video is interlaced with black horizontal stripes.	V4.7.1	
126	VNGR-19797	<i>Interoperability</i>	On an RMX 2000 with MPMx cards running a 128 Kbps conference, after connecting Lync endpoints, the background video blinks.	V7.2	
127	VNGR-19782	<i>Resource Capacity</i>	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	
128	VNGR-19767	<i>Encryption</i>	A Tandberg 6000 DMA registered endpoint requires several attempts to connect to an AES encrypted ISDN conference.	V7.6	
129	VNGR-19628	<i>SIP</i>	The RMX system changes the Call-ID for each new registration. This may trigger a boot cycle on certain SIP Servers.	V7.0.2	
130	VNGR-19606	<i>Cascading</i>	During a 2Mb/384 kbps cascaded conferences with H.239 People+Content enabled, both conferences cannot view content.	V7.0.2C	
131	VNGR-19587	<i>Video</i>	In a COP conference with four levels and 16 endpoints, errors appeared after participants disconnected and reconnected.	V4.7.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
132	VNGR-19573	Video	In a COP conference with four levels and 16 endpoints, a video DSP recovery occurred after participants disconnected and reconnected.	V4.7.1	
133	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	
134	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	
135	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	
136	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	
137	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	
138	VNGR-19455	General	"Layout.CPP" assert is displayed when changing the conference layout via Conference Properties dialog box of a conference running on RMX 1500 at a line rate of 512Kbps with 20 ISDN/H.323 and SIP endpoints connected to the conference.	V7.1	
139	VNGR-19432	Interoperability	When RMX 4000 with MPM+ dials out to CX700 over SIP connection, the call is disconnected after the CX700 accepted the call.	V7.1	
140	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
141	VNGR-19394	General	On an RMX 2000, when creating a 768 kbps Telepresence Conference and selecting a Skin, after conference start a green screen appears instead of the selected conference Skin.	V7.2	
142	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	
143	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	
144	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 256Kbps 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
145	VNGR-19248	Interoperability	When endpoints are registered with an Avaya Call Manager, VSX endpoints view a black video pane from the 1XC Softphone endpoint.	V7.1	
146	VNGR-19221	IVR	On an RMX 4000 in the Ultra Secure Mode, when a dial-out conference is started from a Profile and the IVR initiates, audio and video problems occur.	V7.5	
147	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	
148	VNGR-19087	Video	On an RMX 1500 in a Real Life conference, all endpoints have their audio and video halted for 10 seconds.	V7.1	
149	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	
150	VNGR-19077	Content	In a ISDN cascaded conference that places a call using the Codian Gateway, after sending Content the call disconnects.	V7.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
151	VNGR-19076	Gateway	When an IP call is forwarded from the RadVision Gateway to RMX over ISDN, bad video can be seen.	V7.1	
152	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	
153	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	
154	VNGR-19033	Video	In a 512 kbps H.323 conference with AES, LPR and single layout enabled, when HDX one endpoint uses PCM the other HDX endpoint's video becomes blurred.	V7.1	
155	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	
156	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	
157	VNGR-18975	FECC	In an dial-in H.323 VSW conference, HDX SIP endpoints cannot use FECC.	V7.1	
158	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	
159	VNGR-18936	Interoperability	In a conference on an RMX with MPMx cards, H.320 LifeSize Room endpoints do not receive content.	V7.1	
160	VNGR-18924	Interoperability	After a Radvision Gateway call disconnects from the conference, a ticking sound can be heard in the conference.	V7.1	
161	VNGR-18918	Recording	Display of recording icon when recording an ongoing conference is not supported in MPM+ Card Configuration mode.	V7.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
162	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	
163	VNGR-18697	RMX Manager	On the RMX Manager the port gauge flashes but the system alert is no longer generated in the faults list like in previous versions.	V6.0	
164	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	
165	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.
166	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	
167	VNGR-18606	Interoperability	An RMX 2000 and endpoints are registered with a Broadsoft proxy, when the dial-in conference starts from an LPR enabled Profile, HDX endpoints connect with problems.	V7.1	
168	VNGR-18571	General	A conference with event mode settings, after connecting the endpoints, the connection rates at the 4 levels do not match what has been defined for the Event mode settings.	V4.7	
169	VNGR-18567	Interoperability	Create a COP conference with a 720p Event Mode profile with 2 endpoints, after defining a participant as the Chairperson sometimes the PCM menu doesn't display on chairperson's screen after pressing ## on remote control.	V4.7	
170	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	
171	VNGR-18536	Video	In a Event Mode conference with four levels and 15 endpoints, a video assert appeared.	V4.7	
172	VNGR-18531	General	When forbidden characters are used in the conference name, when retrieving the CDR file an error message will appear "Invalid Directory or path".	V7.1	
173	VNGR-18528	FECC	Documentation has been updated to reflect time out behavior for PCM and FECC remote camera control.	V7.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
174	VNGR-18522	<i>Interoperability</i>	When using PCM to use Click & View, the menu appears in the middle of the screen.	V7.1	
175	VNGR-18510	<i>Video</i>	On the RMX 2000/4000 with MPMx cards and H.261 endpoints connected, when there is motion in the video, video artifacts can be seen.	V7.1	
176	VNGR-18443	<i>Security</i>	RMX Manager is designed not to Remember Login, Username and Password when in Ultra Secure Mode.	V7.5	
177	VNGR-18438	<i>Upgrade Process</i>	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	
178	VNGR-18414	<i>RMX Manager</i>	Active Directory user cannot open the Hardware Monitor section in the RMX Manager.	V7.5	
179	VNGR-18378	<i>Recording</i>	After creating a new profile with a recording link, and a new conference initiates the recording link does not activate.	V7.1	
180	VNGR-18370	<i>Interoperability</i>	In Meeting Rooms where the conference line rates are higher than 384 kbps, Sony PCS1600 endpoints connect as Audio Only.	V7.0.1	
181	VNGR-18357	<i>Multilingual</i>	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	
182	VNGR-18344	<i>RMX Manager</i>	After changing the status of an Ongoing Meeting Room to "Permanent Conference", in the Meeting Room pane the status remains unchanged.	V4.7	
183	VNGR-18330	<i>Resource Capacity</i>	On the in RMX 4000, the maximum number of video participants in one conference is limited to 180.	V7.2	
184	VNGR-18279	<i>Video</i>	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	
185	VNGR-18211	<i>RMX Manager</i>	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	



**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
186	VNGR-18116	<i>Interoperability</i>	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	
187	VNGR-18111	<i>General</i>	An unclear message "No utilizable unit for audio controller" is displayed when removing all Media cards from the RMX.	V7.1	
188	VNGR-18102	<i>RMX Manager</i>	In Event mode, the Lecture mode is not disabled.	V4.7	
189	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	
190	VNGR-17944	<i>ISDN</i>	ISDN HDX endpoints may disconnect from ongoing conferences following a recovery of the processing unit.	V7.1	
191	VNGR-17889	<i>RMX Manager</i>	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	
192	VNGR-17888	<i>Video</i>	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	
193	VNGR-17861	<i>RMX Manager</i>	RMX Manager failed to install from login page. The request is aborted with the message: "Could not create SSL/TLS secure channel".	V7.5	<ol style="list-style-type: none"> <li>1. Install RMX Manager before initiating Secured Communications Mode.</li> <li>2. Install from a network .</li> <li>3. Install locally from RMX Manager folder.</li> </ol>
194	VNGR-17843	<i>General</i>	HDX H323 endpoints are unable to remain connected to a CP conference running on RMX1500 at a line rate of 1920kbps with LPR, Video Clarity and Send Content to Legacy Endpoint options enabled. The disconnect status displays MCU internal problem 32212.	V7.0.2	
195	VNGR-17818	<i>General</i>	Video Preview cannot be disabled.	V7.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
196	VNGR-17807	Interoperability	Radvision Scopia XT1000 does not transmit video when connected at a line rate of at 1920kbps to a CP conference running on RMX 2000 with MPMx and its Resource Configuration set for "Video Quality Optimized".	V7.0.2	
197	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.
198	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	
199	VNGR-17724	General	After Comprehensive Restore to Factory Defaults, an active alarm displayed, indicating voltage problem on MPM-f - card.	V7.0.2	
200	VNGR-17689	ISDN	Blured (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	
201	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	
202	VNGR-17640	Video	Video freeze occur when connecting the 74th HD 720p participants (out of 80) to a conference running on RMX 4000 with 4 MPM+80 cards at a line rate of 1MB, Video Quality set to Sharpness and Video Clarity, encryption and LPR options enabled.	V7.0.2	
203	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).

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>204</b>	VNGR-17586	<i>RMX Manager</i>	Selecting to save the Alarms and Faults to a text file when "Group by MCU" is selected in RMX Manager results in an empty text file.	V7.0.2	* Choose "Group by MCU" again. This time the text is saved to the file. * Save the file as XML.
<b>205</b>	VNGR-17525	<i>Video</i>	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)
<b>206</b>	VNGR-17509	<i>Hardware</i>	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.
<b>207</b>	VNGR-17496	<i>Software Version</i>	DSP recoveries 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	
<b>208</b>	VNGR-17409	<i>Upgrade Process</i>	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.
<b>209</b>	VNGR-17395	<i>Interoperability</i>	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	
<b>210</b>	VNGR-17333	<i>General</i>	When you add an MCU to RMX Manager (v6, v7) the password is displayed in plain text if you selected the "Remember Login" check box during Login.	V6.0	
<b>211</b>	VNGR-17291	<i>Video</i>	In a Dial-in Meeting Room, endpoints viewed impaired video and occasionally received bad audio.	V7.0	
<b>212</b>	VNGR-17104	<i>FECC</i>	In a 512 kbps H.323 conference with two HDX endpoints, FECC is extremely slow.	V7.0	
<b>213</b>	VNGR-17062	<i>IVR</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>214</b>	VNGR-17001	<i>Hardware</i>	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	
<b>215</b>	VNGR-16997	<i>LPR</i>	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	
<b>216</b>	VNGR-16981	<i>Audio</i>	Audio volume of PSTN audio-only participants connecting via GW is approximately three times lower than that audio volume of video participants.	V6.0	
<b>217</b>	VNGR-16974	<i>ISDN</i>	Dial-in or dial-out ISDN endpoints do not connect at line rates higher than 768kbps, irrespective of profile setting.	V7.0	
<b>218</b>	VNGR-16968	<i>Software Version</i>	Personal Conference Manager (PCM) is not supported with MPMx Cards on the RMX.	V7.0	
<b>219</b>	VNGR-16955	<i>Interoperability</i>	iPower 9000 endpoint in H.323 call with RMX with MPM+ or MPMx does not transmit audio in encrypted calls.	V7.0	
<b>220</b>	VNGR-16954	<i>Upgrade Process</i>	On an RMX4000 after upgrading to version 7.0, build 148, the RMX "Could not complete MPM Card startup procedure".	V7.0	
<b>221</b>	VNGR-16938	<i>Video</i>	Artifacts and choppy occur in video for 10 seconds, after connecting Tandberg H.323 or SIP MXP endpoints to a conference on an RMX 1500.	V7.0	
<b>222</b>	VNGR-16924	<i>Interoperability</i>	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.
<b>223</b>	VNGR-16919	<i>Audio</i>	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).
<b>224</b>	VNGR-16901	<i>Software Version</i>	On RMX 1500 Video Preview is preceded by a green screen momentarily before Video Preview starts.	V7.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
225	VNGR-16886	<i>Upgrade Process</i>	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	
226	VNGR-16877	<i>Interoperability</i>	Avaya 1XC Softphone endpoints connected to conference on RMX do not receive content, while HDX endpoints do.	V7.0	
227	VNGR-16871	<i>Software Version</i>	When LPR is activated in a conference, the actual HDX endpoint's "Used Call Rate" is approximately 100kbps lower than expected.	V7.0	
228	VNGR-16841	<i>Interoperability</i>	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	
229	VNGR-16839	<i>SIP</i>	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	
230	VNGR-16817	<i>Upgrade Process</i>	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	
231	VNGR-16809	<i>Software Version</i>	DTMF Code *71 (Secure Conference) sent to RMX 1500 displays Gathering Slide Text instead of "Secured" indicator text.	V7.0	
232	VNGR-16794	<i>Audio</i>	On RMX 4000 with MPM+, G.728 algorithm is not declared as 1st algorithm in conference at 96kbps.	V7.0	
233	VNGR-16776	<i>Interoperability</i>	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	
234	VNGR-16757	<i>RMX Manager</i>	When starting a new conference from a conference template, the new conference is not selected or highlighted in the conferences pane.	V6.0	
235	VNGR-16754	<i>Diagnostics</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>236</b>	VNGR-16752	<i>Upgrade Process</i>	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	
<b>237</b>	VNGR-16745	<i>General</i>	In the RMX manager 7.0, the "new conference" icon suddenly appears in the conferences properties window.	V7.0	
<b>238</b>	VNGR-16742	<i>Diagnostics</i>	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	
<b>239</b>	VNGR-16724	<i>Video</i>	On RMX 1500, video display freezes momentarily during Video Layout changes before the new Video Layout is displayed.	V7.0	
<b>240</b>	VNGR-16722	<i>Video</i>	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	
<b>241</b>	VNGR-16663	<i>SIP</i>	In ICE environment, when connecting endpoints from all NAT environments 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)
<b>242</b>	VNGR-16624	<i>General</i>	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	
<b>243</b>	VNGR-16610	<i>General</i>	The Column width displayed in Web Client and in the RMX Manager UI need to be made broader.	V7.0 , V6.0, V5.0.1, V5.0.0, V4.6.1	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>244</b>	VNGR-16595	<i>Interoperability</i>	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 an MFA card error occurs.	V7.0	
<b>245</b>	VNGR-16562	<i>Gateway</i>	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	
<b>246</b>	VNGR-16560	<i>General</i>	After log-in to the RMX 1500 Web Client, a Microsoft .NET Framework error message appears.	V7.0	
<b>247</b>	VNGR-16539	<i>IVR</i>	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	
<b>248</b>	VNGR-16537	<i>Hardware</i>	On the RMX 1500 when the RMX is in a "Diagnostic Mode" the listed slot numbers of the modules are incorrect.	V7.0	
<b>249</b>	VNGR-16535	<i>SIP</i>	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	
<b>250</b>	VNGR-16523	<i>FECC</i>	On the RMX 1500 running a mixed H.323 & SIP 384Kbps conference, when connecting an Tandberg SIP endpoint, FECC does not work.	V7.0	
<b>251</b>	VNGR-16466	<i>Software Version</i>	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	
<b>252</b>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
253	VNGR-16460	Software Version	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	
254	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	
255	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.
256	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	
257	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	
258	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	
259	VNGR-16363	Interoperability	On the RMX2000 with an MPMx card, when starting a new a 2MB conference, lpower endpoints take a long time to connect.	V7.0	
260	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	
261	VNGR-16301	ISDN	After starting a VSW conference with LPR enabled, when dialing out using ISDN a message appears:"SIP cannot connect to VSW with LPR enabled"	V7.0	



**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>262</b>	VNGR-16296	<i>General</i>	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	
<b>263</b>	VNGR-16283	<i>General</i>	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	
<b>264</b>	VNGR-16281	<i>Content</i>	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	
<b>265</b>	VNGR-16237	<i>General</i>	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	
<b>266</b>	VNGR-16210	<i>RMX Web Client</i>	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	
<b>267</b>	VNGR-16120	<i>General</i>	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	
<b>268</b>	VNGR-16103	<i>General</i>	After running diagnostics on the RMX, LED functionality is not documented.	V7.0	
<b>269</b>	VNGR-15953	<i>General</i>	When copying and pasting conferences based on a Profile, the pasted conference is added to conference templates.	V7.0	
<b>270</b>	VNGR-15939	<i>Interoperability</i>	In a "Fixed resource Capacity" mode, Legacy endpoints can still receive content when they should not.	V7.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
271	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	
272	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	
273	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	
274	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	
275	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	
276	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	
277	VNGR-15737	General	In the Resolution Configuration Slider, the CIF30 slider is absent from the UI.	V7.0	
278	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	
279	VNGR-15719	Interoperability	Tandberg C20 endpoint stops receiving video when the HDX8006 sends content during 6 mbps HD1080p encrypted conference.	V5.1	
280	VNGR-15718	General	Incorrect disconnection cause after pulling LAN cable from RMX. The endpoints reports that the "call close normal".	V7.0	
281	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>282</b>	VNGR-15706	<i>Video</i>	Tandberg H.320 6000 MXP endpoint displays video freezes throughout the duration of a conference set to motion & encryption.	V5.1	
<b>283</b>	VNGR-15704	<i>Content</i>	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	
<b>284</b>	VNGR-15700	<i>Software Version</i>	When PCM is initiated, site names are displayed over the PCM menu.	V7.0	
<b>285</b>	VNGR-1569	<i>CDR</i>	When the conference termination time is changed, the CDR is not updated.	V1.0.0	
<b>286</b>	VNGR-15649	<i>Interoperability</i>	In a continuously running conference, after disconnected two HDX7000 and VSX7000 endpoints, the HDX4000 endpoint's video freezes.	V7.0	
<b>287</b>	VNGR-15541	<i>Video</i>	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	
<b>288</b>	VNGR-15523	<i>Partners - Microsoft</i>	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	
<b>289</b>	VNGR-15452	<i>General</i>	When using the RMX Web Client with Internet Explorer 7, when right clicking any option, the properties are transferred to the next page.	V5.0.1	
<b>290</b>	VNGR-15386	<i>Software Version</i>	Artifacts present in the Gathering Slide in 2560kbps, CP conference with Motion selected.	V7.0	
<b>291</b>	VNGR-15324	<i>Software Version</i>	<ul style="list-style-type: none"> <li>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.</li> </ul>	V7.0	
<b>292</b>	VNGR-15320	<i>General</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
293	VNGR-15281	<i>Interoperability</i>	Aethra VegaStar Gold endpoint, when connecting via ISDN to 384kbps conference creates CDR Event - Participant status "Connected with problem" .	V7.0	
294	VNGR-15256	<i>Encryption</i>	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	
295	VNGR-15222	<i>RMX Manager</i>	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 shows the disconnected power supply status appearing as "Normal".	V5.0.1	
296	VNGR-15155	<i>Video</i>	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	
297	VNGR-15131	<i>IVR</i>	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	
298	VNGR-15101	<i>IVR</i>	In a Video Switched 4Mbps conference, only the last part of DTMFs *6 (mute) and #6 (unmute) messages are heard.	V7.0	
299	VNGR-14780	<i>Interoperability</i>	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	
300	VNGR-14778	<i>RMX Web Client</i>	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	
301	VNGR-14767	<i>General</i>	H.323 party disconnect due to MCU Internal Problem 32212.	V6.0	
302	VNGR-14688	<i>General</i>	When a conference is deleted in the RMX Manager, conference participants are not deleted in the participants list.	V6.0	
303	VNGR-14687	<i>Audio</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>304</b>	VNGR-14667	<i>General</i>	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	
<b>305</b>	VNGR-14624	<i>General</i>	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	
<b>306</b>	VNGR-14578	<i>Audio</i>	On an RMX with a license for 800 audio only participants, a disconnection cause always occurs after connecting the 767th participant.	V6.0	
<b>307</b>	VNGR-14417	<i>General</i>	On an RMX 2000, when QoS is selected in the IP Network Service and connecting more than 5 HDX endpoints in an HDX call, packet loss occurs when sending audio and video.	V5.0.1	
<b>308</b>	VNGR-14175	<i>RMX Manager</i>	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	
<b>309</b>	VNGR-14159	<i>General</i>	Operator assistance function is blocked when the TelePresence mode is enabled.	V6.0	
<b>310</b>	VNGR-14151	<i>General</i>	A Shelf Voltage problem is always displayed in the System Alerts pane regardless of the actual status.	V6.0	
<b>311</b>	VNGR-14124	<i>Video</i>	On rare occasions in 2Mbps ISDN calls, ISDN participants connected without their endpoints sending video for a few seconds.	V6.0	
<b>312</b>	VNGR-14062	<i>General</i>	On a fully loaded RMX 4000, endpoint may disconnects with Call Disconnection Cause stated as " MCU internal problem - 11122".	V6.0	
<b>313</b>	VNGR-14047	<i>Interoperability</i>	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	
<b>314</b>	VNGR-13965	<i>General</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
315	VNGR-13951	<i>RMX Manager</i>	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	
316	VNGR-13832	<i>RMX Manager</i>	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	
317	VNGR-13808	<i>General</i>	On an RMX 2000, you able to enter an invalid flag (CS_TUNNELING instead of H245_TUNNELING) onto the system.	V4.1.1	
318	VNGR-13729	<i>Unified Communication Solution</i>	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	
319	VNGR-13314	<i>Partners - Microsoft</i>	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	
320	VNGR-13152	<i>Video</i>	Message overlay is limited to 32 Chinese characters OR 96 ASCII characters.	V4.6	
321	VNGR-13001	<i>Video</i>	Video display freezes momentarily with every speaker or layout change in a conference with HDX and SVX endpoints.	V4.6	
322	VNGR-12732	<i>Upgrade Process</i>	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	
323	VNGR-12415	<i>Interoperability</i>	In a conference running at a line rate of 1728 kbps set to Same Layout, when PVX/VSX7000 participants connect in CIF264/263, an error message appears.	V4.6	
324	VNGR-12373	<i>Interoperability</i>	HDX endpoint connected via H.320 does not receive Content from Tandberg MXP endpoint connected via H.323.	V5.0.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>325</b>	VNGR-12372	<i>Interoperability</i>	Tandberg 6000 E and B series, H.320 endpoints do not connect to conferences when encryption is enabled.	V5.0.0	
<b>326</b>	VNGR-12369	<i>Interoperability</i>	Tandberg C20 endpoint periodically displays fast updates in HD1080p conferences.	V5.0.0	
<b>327</b>	VNGR-12355	<i>Interoperability</i>	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.
<b>328</b>	VNGR-12266	<i>Interoperability</i>	Tandberg MXP endpoint receives ghosted video from HDX9004 endpoint during H.323 conference.	V5.0.0	
<b>329</b>	VNGR-12257	<i>RMX Web Client</i>	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	
<b>330</b>	VNGR-12202	<i>Encryption</i>	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	
<b>331</b>	VNGR-12178	<i>Content</i>	RMX does not support H.264 Content in ISDN calls.	V5.0.0	
<b>332</b>	VNGR-12177	<i>Interoperability</i>	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	
<b>333</b>	VNGR-12172	<i>RMX Web Client</i>	In the RMX Web Client, the main window opens up as full screen and cannot be resized.	V5.0.0	
<b>334</b>	VNGR-12116	<i>General</i>	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	
<b>335</b>	VNGR-12100	<i>General</i>	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.
<b>336</b>	VNGR-12034	<i>ISDN</i>	In a conference running at a line rate of 384 Kbps, H.320 encrypted participant cannot connect and an assert appears.	V5.0.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
337	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	
338	VNGR-12031	IVR	A conference running at a line rate of 1920Kbps and IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	V5.0.0	
339	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	
340	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	
341	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	
342	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.
343	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	
344	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	
345	VNGR-11953	Cascading	When connecting to a cascaded CP conference with a 768Kbps line rate and the video quality set to Sharpness, HDX endpoints experience bad video quality.	V5.0.0	
346	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	
347	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	



**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>348</b>	VNGR-11883	<i>General</i>	After software upgrade, it is necessary to close and reopen Internet explorer.	V5.0.0	
<b>349</b>	VNGR-11843	<i>Video</i>	In a 2 Mb Video Switched conference with 10 or more H.323 endpoints connected, random video refreshes may occur.	V5.0.0	
<b>350</b>	VNGR-11830	<i>Interoperability</i>	Sony XG80 endpoint cannot send Content in H.323 384 Kbps call.	V6.0	
<b>351</b>	VNGR-11810	<i>H.323</i>	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	
<b>352</b>	VNGR-11798	<i>Interoperability</i>	When Tandberg C20 endpoint sends Content, the far end indicates that Content is being received but received Content is black.	V5.0.0	
<b>353</b>	VNGR-11767	<i>Interoperability</i>	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	
<b>354</b>	VNGR-11746	<i>CDR</i>	GMT Time Offset is written to the unformatted CDR as 0.	V4.1	
<b>355</b>	VNGR-11563	<i>Interoperability</i>	Legacy endpoints occasionally cannot switch to Content when Content switched from H,264 to H.263.	V4.1	
<b>356</b>	VNGR-11531	<i>IVR</i>	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	
<b>357</b>	VNGR-11523	<i>Interoperability</i>	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	
<b>358</b>	VNGR-11489	<i>Interoperability</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
359	VNGR-11417	<i>Interoperability</i>	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	
360	VNGR-11401	<i>Encryption</i>	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	V4.1	
361	VNGR-11383	<i>General</i>	When updating the Profile assigned to a Conference Template, changes are not applied when the conference becomes ongoing.	V4.1	
362	VNGR-11382	<i>Video</i>	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	
363	VNGR-11351	<i>Video</i>	When the video from an endpoint is blocked, inconsistent video resolution settings are implemented.	V4.1	
364	VNGR-11341	<i>Interoperability</i>	During H.320 calls, Lip Sync issues occur when content is being sent.	V4.1	
365	VNGR-11324	<i>General</i>	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	
366	VNGR-10922	<i>General</i>	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	
367	VNGR-10239	<i>Video</i>	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	
368	VNGR-10162	<i>Interoperability</i>	An HDX 2.5.0.2-3395 endpoint cannot control a Sony XG80 endpoint using FECC.	V7.2	
369	VNGR-10104	<i>LPR</i>	When an H.323 HDX endpoint sends Content, the endpoint disables the LPR.	V4.0.1	
370	VNGR-9909	<i>Interoperability</i>	When dialing out to a Tandberg MXP ISDN endpoint, the IVR slide is not displayed, although the IVR message is played.	V4.0.0	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>371</b>	VNGR-9844	<i>Interoperability</i>	During an H.320 call, Tandberg 6000 B10 endpoint does not receive content from an HDX9004.	V7.1	
<b>372</b>	VNGR-9843	<i>Interoperability</i>	During an H.323 call, Tandberg 6000 B10 endpoint receives corrupted H239 content from an HDX.	V7.1	
<b>373</b>	VNGR-9834	<i>IVR</i>	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	
<b>374</b>	VNGR-9830	<i>Interoperability</i>	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.
<b>375</b>	VNGR-9829	<i>RMX Web Client</i>	Occasionally, during an ongoing conference, when selecting the Hardware Monitor menu the message "No connection with Switch" appears.	V4.0.0	
<b>376</b>	VNGR-9809	<i>IVR</i>	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	
<b>377</b>	VNGR-9803	<i>General</i>	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	
<b>378</b>	VNGR-9740	<i>Upgrade Process</i>	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).
<b>379</b>	VNGR-9729	<i>General</i>	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.
<b>380</b>	VNGR-9677	<i>Interoperability</i>	When switching Content sending from an HDX9004 to Aethra X7 and back, Content is not received by Aethra X7.	V4.0.0	
<b>381</b>	VNGR-9565	<i>Upgrade Process</i>	When downgrading from version 4.0 to version 3.0, the MPM card does revert to normal.	V4.0.0	
<b>382</b>	VNGR-9340	<i>CDR</i>	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
383	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	
384	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	
385	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	
386	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
387	VNGR-7734	IP	Static Routes table in IP Network Service does not function.	V3.0.0	
388	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	
389	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	
390	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.
391	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.
392	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	
393	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	
394	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	

**Table 1-7** Known Limitations Version 7.6.1

#	Key	Category	Description	Detected in Version	Workaround
<b>395</b>	VNGR-4652	<i>Interoperability</i>	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.
<b>396</b>	VNGR-4405	<i>ISDN</i>	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	
<b>397</b>	VNGR-3977	<i>Interoperability</i>	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.
<b>398</b>	VNGR-3824	<i>General</i>	The Click & View menu doesn't appear in 64 Kbps calls.	V1.1.0	Use the RMX Web Client.
<b>399</b>	VNGR-3276	<i>SIP</i>	SIP participants cannot connect to a conference when the conference name contains blank spaces.	V1.1.0	
<b>400</b>	VNGR-3089	<i>HD</i>	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
<b>401</b>	VNGR-3011	<i>CDR</i>	The Encryption field is missing from the CDR file.	V1.1.0	
<b>402</b>	VNGR-2473	<i>RMX Web Client</i>	Sometimes when installing the RMX Web Client, Windows Explorer >Internet Options> Security Settings must be set to Medium or less.	V1.1.0	

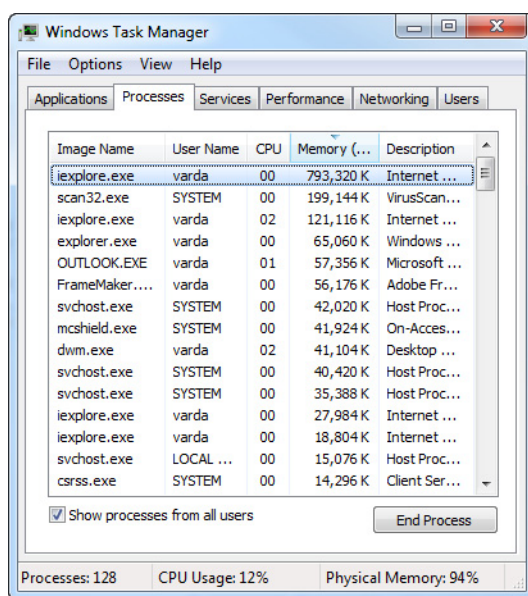
# Troubleshooting Instructions

Close all the Internet Explorer sessions and perform the following procedure.

## 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.

- 1 Start the **Task Manager** and click the **Processes** tab.
- 2 Select an **iexplore** process and click the **End Process** button.



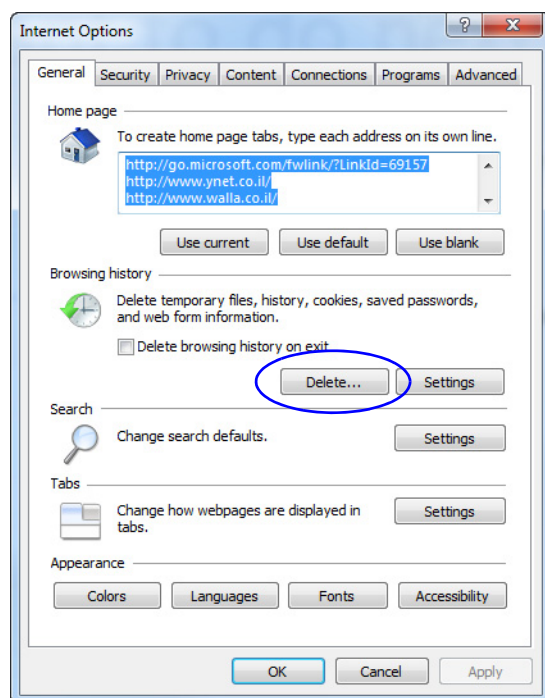
- 3 Repeat this process for all **iexplore** processes that are currently active.
- 4 Close the *Windows Task Manager* dialog box.
- 5 Open the Internet Explorer and connect to the RMX.

If the problem persists, continue with the next step.

## Procedure 2: Deleting the Temporary Internet Files, RMX Cookie and RMX Object

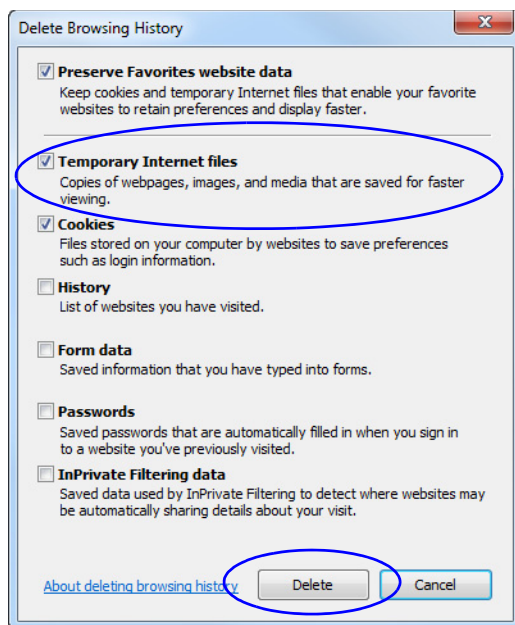
To delete the Temporary files:

- 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.

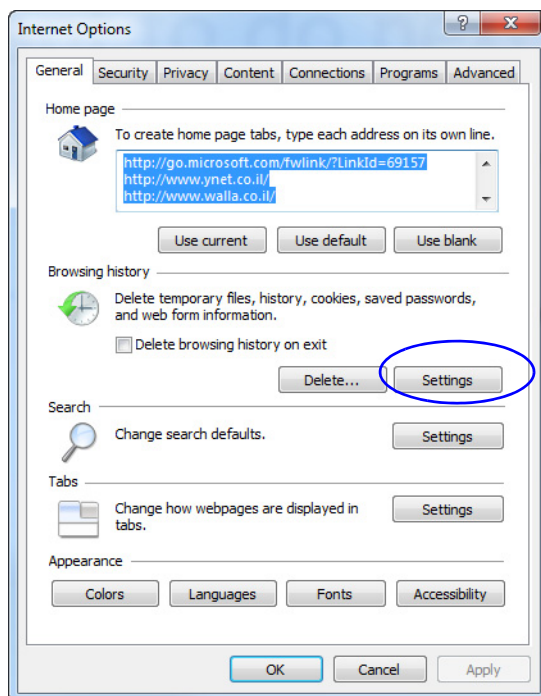


The *Delete Browsing History* dialog box opens.

- 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.



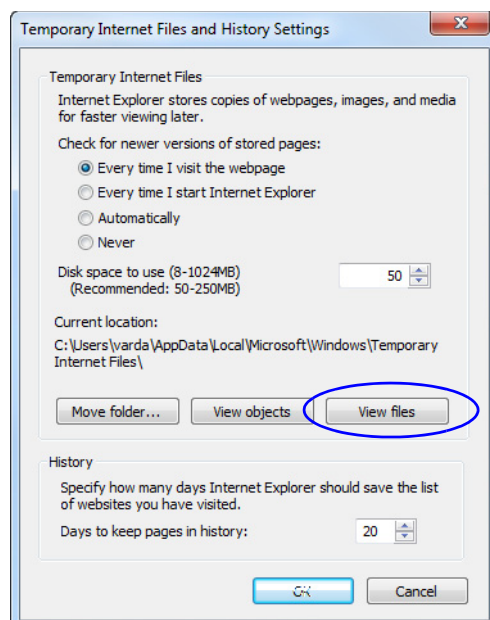
- 4 Click the **Delete** button.
  - 5 When the process is complete, the system return to the *Internet Options* dialog box.
- To delete the RMX Cookie:**
- 6 In the *Internet Options* dialog box - *Browsing History* pane, click the **Settings** button.





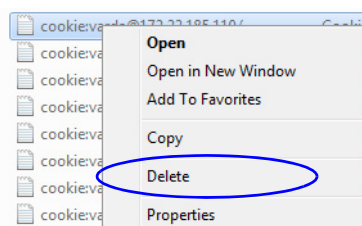
The *Temporary Internet Files and History Settings* dialog box opens.

- 7 Click the **View files** button.



The Windows Explorer screen opens, listing Windows *Temporary Internet Files*.

- 8 Browse to the RMX cookie.  
The cookie is listed in the format: **cookie:user name@RMX IP address**. For example: **cookie:valerie@172.22.189.110**.
- 9 Right-click the RMX cookie and click **Delete**.

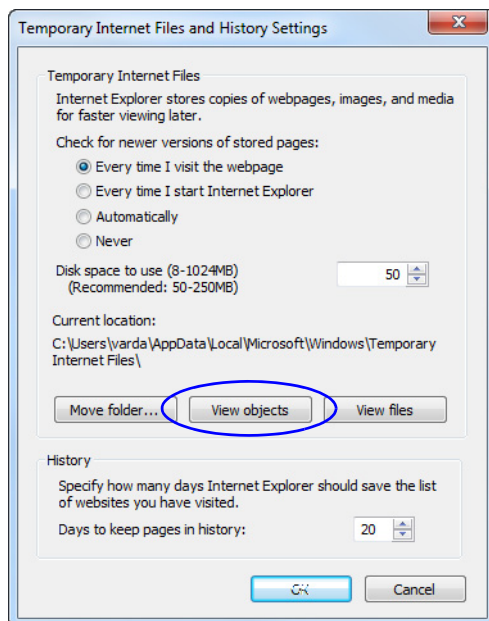


The system prompts for confirmation.

- 10 Click **Yes**.  
The cookie is deleted.
- 11 Close the Windows Explorer screen.

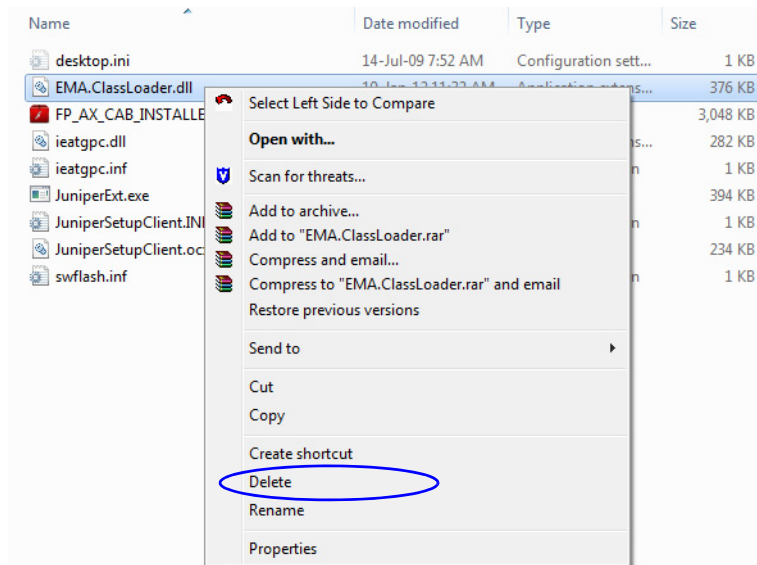
### To delete the RMX ActiveX Object:

- 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 system.

If the problem persists, continue with the next step.

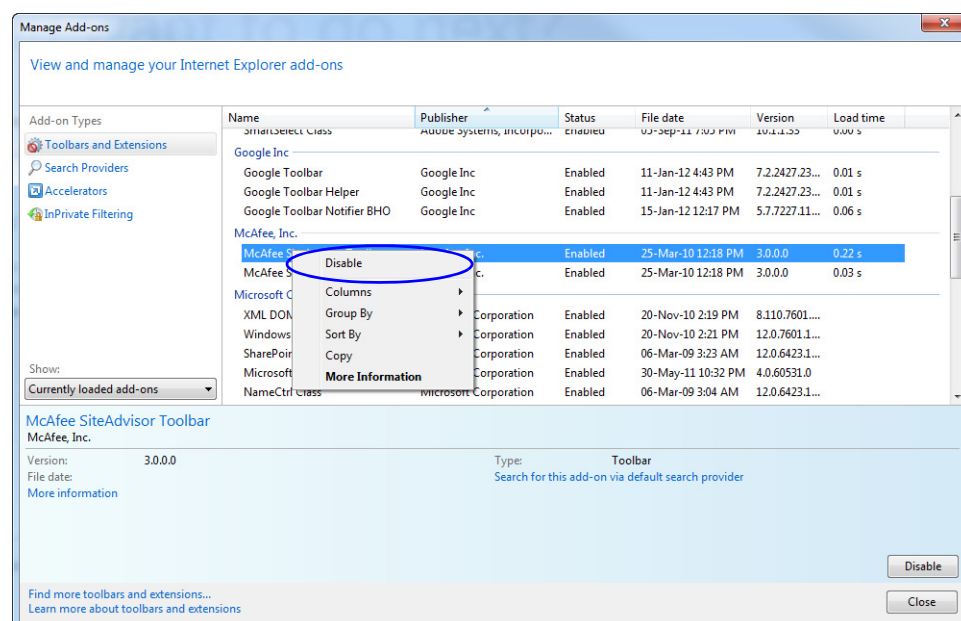
### Procedure 3: Managing Add-ons Collisions

In some cases, a previously installed add-ons, such as anti virus programs can prevent the installation of a new add on. In some cases, disabling these add-ons is 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 system.

