



Polycom[®] RMX[®] 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.

© 2010 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.

Table of Contents

Version 6.0 - New Features List	1
Version 6.0 - Changes to Existing Features	3
Version 6.0- Upgrade Package Contents	5
Where to Get the Latest Product Information	5
Version 6.0 - Interoperability Tables.....	6
Devices	6
RMX Web Client	8
Windows 7™ Security Settings	9
Internet Explorer 8 Configuration	11
Polycom Solution Support	13
Version 6.0 - Upgrade Procedure.....	14
Upgrading to Version 6.0	14
Upgrading from Version 5.x to Version 6.0 (RMX 2000)	14
Upgrading from Version 3.x/4.x to Version 6.0 (RMX 2000)	16
Additional/Optional System Updates After Upgrading	18
IVR Services	18
Gathering Settings	19
Version 6.0 Detailed Description	20
Polycom Conferencing for Microsoft Outlook®	20
Setting up the Calendaring Solution	21
Option 1 - Using default Exchange Server settings	22
Option 2 - Using an alternate Primary SMTP Mailbox	23
Option 3 - Using modified Exchange Server settings	24
Calendaring Guidelines	25
Creating and Connecting to a Conference	27
Creating a Conference	27
Connecting to a Conference	29
Gathering Phase	30
Gathering Phase Guidelines	30
Gathering Phase Duration	31
Enabling the Gathering Phase Display	32
Monitoring Gathering-enabled Conferences	35
Auto Brightness	36
Guidelines	36
Audio Clarity	37
Guidelines	37
Packet Loss Concealment (PLC) for Audio	38
Guidelines	38
Siren 22 and G.719 Audio Algorithm Support	39
Guidelines	39
Mono	39
Stereo	40
Monitoring Participant Audio Properties	40
Microsoft Environment - Creating and Exporting the Security Certificate to the RMX Workstation	42

Creating the Certificate Request	42
Installing the Certificate	44
Detailed Description - Changes to Existing Features	46
PSTN Dial-in Using GK Prefix	46
Enabling PSTN dial-in using GK prefix	46
RMX Resource Management by CMA and DMA	47
Guidelines	47
Recording Link Layout	48
Immersive Telepresence (ITP) Enhancements	49
Changes to the New Profile Dialog Box	49
Automatic detection of Immersive Telepresence (ITP) Sites	49
Retrieving the Telepresence Layout Mode	50
Monitoring Telepresence Mode	51
Monitoring Ongoing Conferences	51
Monitoring Participant Properties	51
Striping Options	52
Horizontal Striping	52
Asymmetric Letter box Cropping	52
Gathering Phase with ITP Room Systems	52
All layouts available to all participants	52
Aspect ratio for standard endpoints	52
Video Fade is enabled for all Telepresence conferences	52
Setting the RMX as a Voice Gateway in Microsoft OCS R2 2007 Environment	53
Setting the Numerical Dialing into RMX Meeting Rooms	53
Optional. Removing the RMX from the Host Authorization List	54
Configuring the RMX as a Routable Gateway	54
Establishing a Voice Route to the RMX "Voice" Gateway	55
Configuring Office Communicator Users for Enterprise Voice	58
Starting a Conferencing Call from the MOC	61
Corrections and Known Limitations	62
Corrections Between Version 5.0 and Version 6.0	62
Version 6.0 System Limitations	70

Version 6.0 - New Features List

The following table lists the new features in Version 6.0 (RMX 2000 and RMX 4000).

Table 1 New Features List - RMX 2000 and RMX 4000

	Category	Feature Name	Description	Card Configuration Mode
1	Conferencing Mode	Polycom Conferencing for Microsoft Outlook	<i>Polycom Conferencing for Microsoft Outlook</i> is an add-in that enables users to easily organize and invite attendees to Video meetings via Microsoft Outlook®. When scheduling a Polycom Meeting via Outlook, Video Meeting information is added to the meeting invitation. Attendees call the meeting at the scheduled Start Time using the link or the dial-in number provided in the meeting invitation.	MPM MPM+
2	Conferencing Mode	Gathering Slide	Once connected to the conference, a special slide, the Gathering Slide, is displayed to connected participants until the conference starts. The Gathering Slide displays live video along with information taken from the meeting invitation.	MPM MPM+
3	Video	Auto Brightness	Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.	MPM+
4	Audio	Audio Clarity	Audio Clarity improves received audio from participants connected via ISDN/ PSTN using the following low bandwidth (8kHz) audio algorithms: G.729a and G.711.	MPM+
5	Audio	Packet Loss Concealment (PLC)	Packet Loss Concealment (PLC) for Siren audio algorithms improves received audio when packet loss occurs in the network. The following audio algorithms are supported: <ul style="list-style-type: none"> • Siren 7 (mono) • Siren 14 (mono/stereo) • Siren 22 (mono/stereo) • G.719 	MPM+
6	Audio	Siren 22 Audio Algorithm	Polycom's proprietary Siren 22 Audio Algorithm is supported for participants connecting with Polycom endpoints. Both Mono and Stereo are supported.	MPM+

Table 1 *New Features List - RMX 2000 and RMX 4000 (Continued)*

	Category	Feature Name	Description	Card Configuration Mode
7	Audio	Siren 14 - Stereo	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).	MPM+
8	General	Recording/ IVR Service	Recording of conferences can be controlled via the corresponding buttons on the HDX remote control. Cosequentially, the DTMF codes of the Recording actions defined in the default IVR service shipped with new RMX system were changed. For a list of changes, see “ <i>Version 6.0 - Changes to Existing Features</i> ” on page 3 and “ <i>Additional/Optional System Updates After Upgrading</i> ” on page 18.	MPM MPM+
9	Partners	Microsoft Environment	When working in Microsoft R1 and R2 environment, an additional secured and standard method of certificate installation in the IP Network Service - SIP Server called CSR can be used to install the required certificate.	MPM MPM+

Version 6.0 - Changes to Existing Features

The following table lists the changes to existing features in Version 6.0.

Table 2 Feature Changes List

	Category	Feature Name	Description
1	CMA/DMA	RMX Resource Management by CMA and DMA	In version 6.0, following a request by the CMA and DMA, the RMX will send updates on resource usage to both CMA and DMA, with each application updating its own resource usage for the RMX. This provides better management of the RMX resources by CMA and DMA.
2	General	Recording	When the video layout of the conference is set to Auto Layout, the recording of the conference will now include all the conference participants (in previous versions, not all participants were recorded).
3	General	Recording Link	The layout of the Recording Link can be changed, selecting a <i>Personal</i> layout as for any participant in the conference, allowing the RMX user to customize the recorded layout. The Recording Link Layout can be changed during an ongoing conference.
4	General	IVR Service	The DTMF Codes of the Roll Call actions defined in the default IVR Services shipped with new RMX systems were changed as follows: <ul style="list-style-type: none"> • Enable Roll Call: old: *32 new: *42 • Disable Roll Call: old: #32 new: #42 • Roll Call Review Names: old: *33 new: *43 • Roll Call Stop Review: old: #33 new: #43
5	General	IVR Service	The DTMF Codes of the Recording actions defined in the default IVR Services shipped with new RMX systems were changed as follows: <ul style="list-style-type: none"> • Start/Resume Recording: old: *73 new: *3 • Stop Recording: old: *74 new: *2 • Pause Recording: old: *75 new: *1

Table 2 *Feature Changes List (Continued)*

	Category	Feature Name	Description
6	Video	Telepresence Mode	Control and monitoring of <i>Immersive Telepresence (ITP)</i> features have been enhanced with: <ul style="list-style-type: none"> • Automatic detection of <i>ITP</i> sites. • Retrieval of <i>Telepresence Layout Mode</i>. • Control of <i>Cropping</i> and <i>Striping</i> options. • Enhanced <i>Layout</i> control.
7	Partners	Microsoft Environment	The RMX can be configured as a Voice Gateway in the OCS environment, enabling dialing in to meeting rooms using numbers instead of or in addition to SIP URI addresses which are long strings.

Version 6.0- Upgrade Package Contents

Version 6.0 upgrade package must be downloaded from the *Polycom Resource Center* and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Documentation
 - RMX 2000/4000 Version 6.0 Release Notes
 - RMX 2000/4000 Getting Started Guide
 - RMX 2000/4000 Administrator's Guide
 - RMX 2000 Hardware Guide
 - RMX 4000 Hardware Guide
 - RMX 2000 Quick Installation Booklet
 - RMX 4000 Quick Installation Booklet
 - Installation Quick Start Guide for RMX 2000
 - Installation Quick Start Guide for RMX 4000
 - RMX Open Source Third Party Licenses
- External DB Tools Version 4.0.2
 - RMX System External Database API Programmer's Guide
 - Sample Scripts
- RMX XML API Kit Version 6.0
 - RMX System XML API Version 6.0 Release Notes
 - RMX System XML API Overview
 - RMX 2000 XML API Schema Reference Guide (version 3.0)
 - MGC to RMX XML API Conferencing Comparison
 - Polycom XML Tracer User's Guide
 - XML Schemas
 - Polycom XML Tracer application
- Translations of RMX 2000 Version 5.0 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 www.polycom.com/support.

Version 6.0 - Interoperability Tables

Devices

The following table lists the devices and versions with which RMX Version 6.0 was tested. Supported versions include also previous versions.

Table 3 Version 6.0.x Device Interoperability Table

Device	Version
Gatekeepers/Proxies	
<i>Polycom CMA</i>	5.0 build 41
<i>Polycom PathNavigator</i>	7.0.12
<i>Polycom SE200</i>	3.00.07.ER001
<i>Cisco gatekeeper</i>	12.3
<i>Radvision ECS gatekeeper</i>	3.5.2.5
<i>Iptel proxy</i>	0.9.6
<i>Microsoft OCS</i>	R1 / R2
Recorder	
<i>Polycom RSS 2000</i>	4.0.0.001 360
<i>Polycom RSS 4000</i>	6.0.0.001 22237
MCUs, Call Managers Network Devices and Add ins	
<i>Polycom MGC 25/50/100 and MGC+50/100</i>	8.0.2 and 9.0.3
<i>RMX 1000</i>	2.1
<i>Polycom DMA 7000</i>	2.0.0 build 11
<i>Avaya CM</i>	5.2
<i>Avaya ACM</i>	943
<i>Avaya IP Softphone R6.0</i>	SP1
<i>Cisco Call Manager</i>	4.1
<i>Tandberg MCU</i>	D3.11
<i>Tandberg MPS</i>	J3.3
<i>Polycom VBP 5300LF-S25</i>	9.1.5.1
<i>Polycom Conferencing Add in for Microsoft Outlook</i>	0.9.1 build 4
Endpoints	
<i>Polycom HDX Family</i>	2.5.0.6 / 2.5.0.7 Beta
<i>Polycom HDX Durango</i>	2.6.0.4659

Table 3 Version 6.0.x Device Interoperability Table (Continued)

Device	Version
<i>Polycom VSX product line</i>	9.0.5.1
<i>Polycom Viewstation</i>	7.5.4
<i>Polycom CMAD</i>	5.0.0.0143
<i>Polycom QDX6000</i>	4.0
<i>Polycom VVX1500</i>	3.2.2.0191
<i>Polycom ViaVideo PVX</i>	8.0.4
<i>Polycom VS 512</i>	7.5.4
<i>Polycom VSSP 128/384</i>	7.5.4
<i>Polycom VS EX</i>	6.0.5
<i>Polycom VS 4000</i>	6.0.5
<i>Polycom VS FX</i>	6.0.5
<i>Polycom V700 and Polycom V500</i>	9.0.5.1
<i>Polycom iPower 9000</i>	6.2.1208
<i>Soundstation IP3000</i>	2.8
<i>Aethra X3</i>	11.3.23
<i>Aethra X7</i>	12.1.7
<i>Aethra VegaStar Gold</i>	6.0.49
<i>Avaya IP Softphone R6</i>	6.01.48
<i>Avaya 1XC</i>	R1.020-SP2-1696
<i>LifeSize</i>	4.2.0.17
<i>LifeSize Room and Express</i>	4.2.0.17
<i>VVX1500</i>	3.1.2.0256
<i>DST B5</i>	2.0
<i>DST K60</i>	2.0.1
<i>DST K80</i>	4.0
<i>Sony PCS -XG80</i>	2.0.4
<i>Sony PCS -1</i>	3.42
<i>Sony PCS -G50</i>	2.70
<i>Sony PCS -TL50</i>	2.42
<i>Tandberg 150 MXP</i>	F8.1
<i>Tandberg MXP Product line</i>	F8.1
<i>Tandberg Classic E-Series</i>	E5.3 PAL
<i>Tandberg 880 E</i>	F8.1

Table 3 Version 6.0.x Device Interoperability Table (Continued)

Device	Version
Microsoft OC client R2	3.5.6907.0



Nortel environment is supported only with RMX 2.0.2 Nortel designated version. This version is only supported on RMX A/B/C- type chassis with MPM cards only and no MPM+ cards.

RMX Web Client

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

Table 4 Version 6.0 Environment Interoperability Table

Web Browser	Operating System
Internet Explorer 6	Windows XP™
Internet Explorer 7	Windows XP™ Windows Vista™
Internet Explorer 8	Windows XP™ Windows Vista™ (32 bit) Windows 7™ (32 bit)

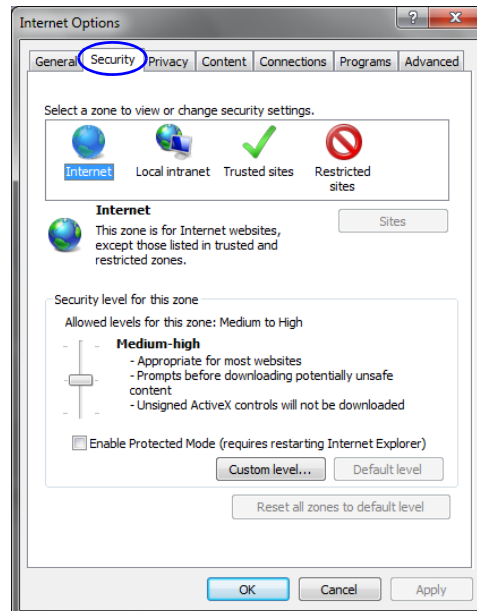
Windows 7™ Security Settings

If *Windows7* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 6.0* software to the workstation.

To disable Protected Mode:

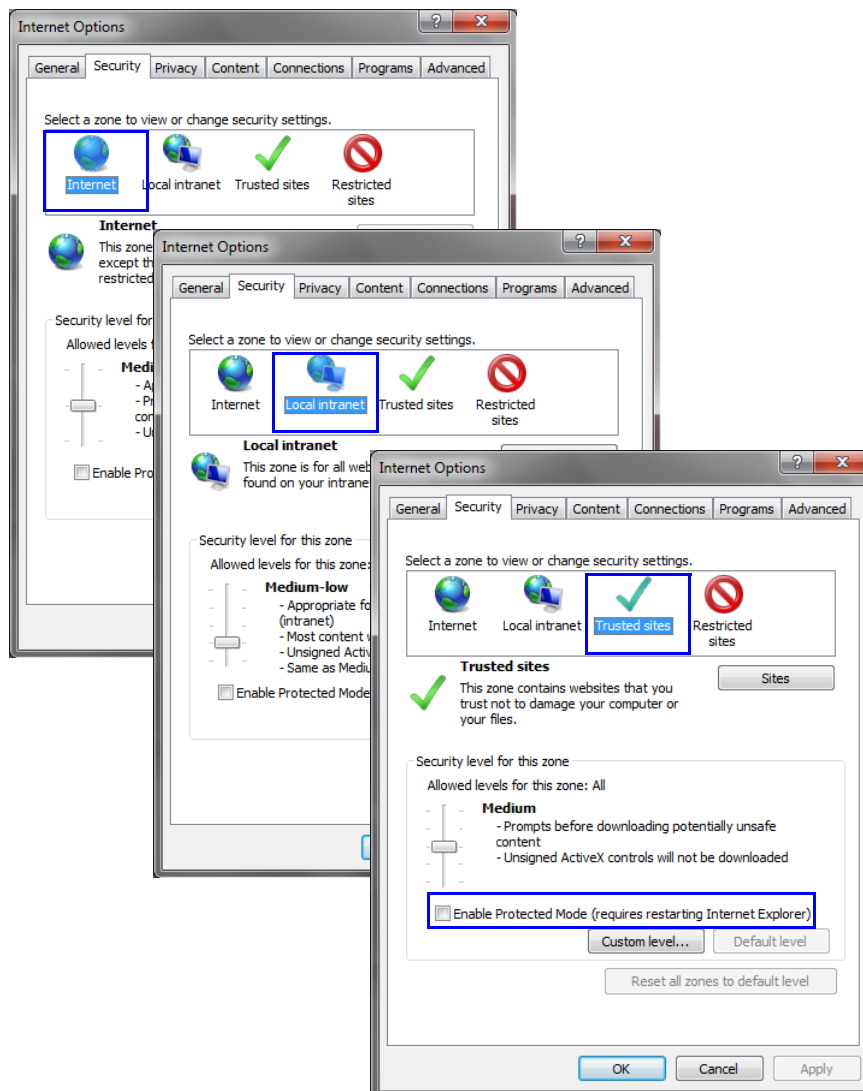
- 1 In the *Internet Options* dialog box, click the **Security** tab.

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*

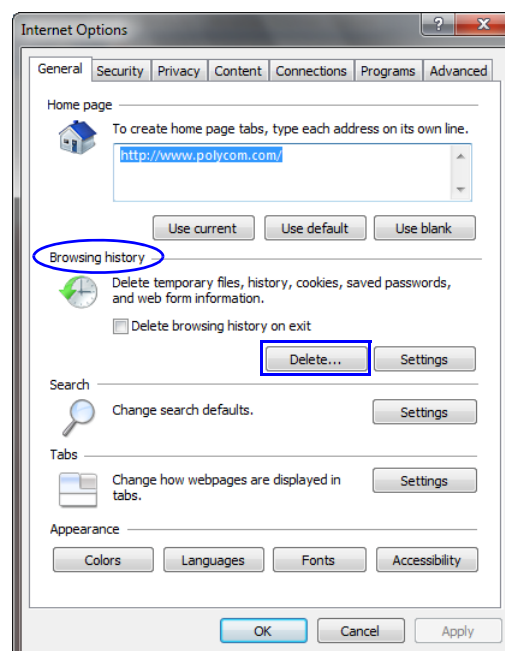
Internet Explorer 8 Configuration

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:

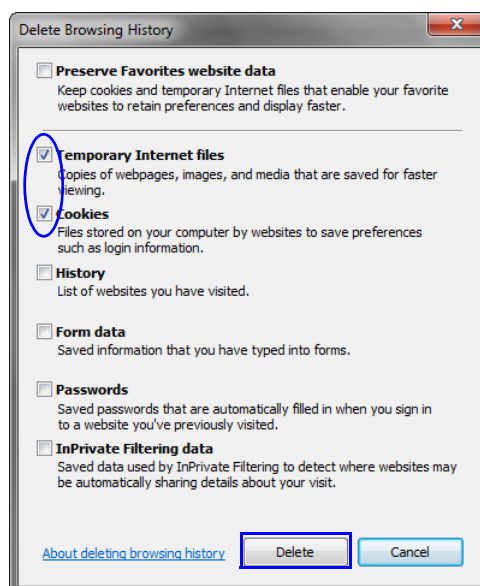
- 1 Close **all** browsers running on the workstation.
- 2 Use the *Windows Task Manager* to verify that no *iexplore.exe* processes are running on the workstation. If any processes are found, use the **End Task** button to end them.
- 3 Open *Internet Explorer* but do **not** connect to the RMX.
- 4 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.



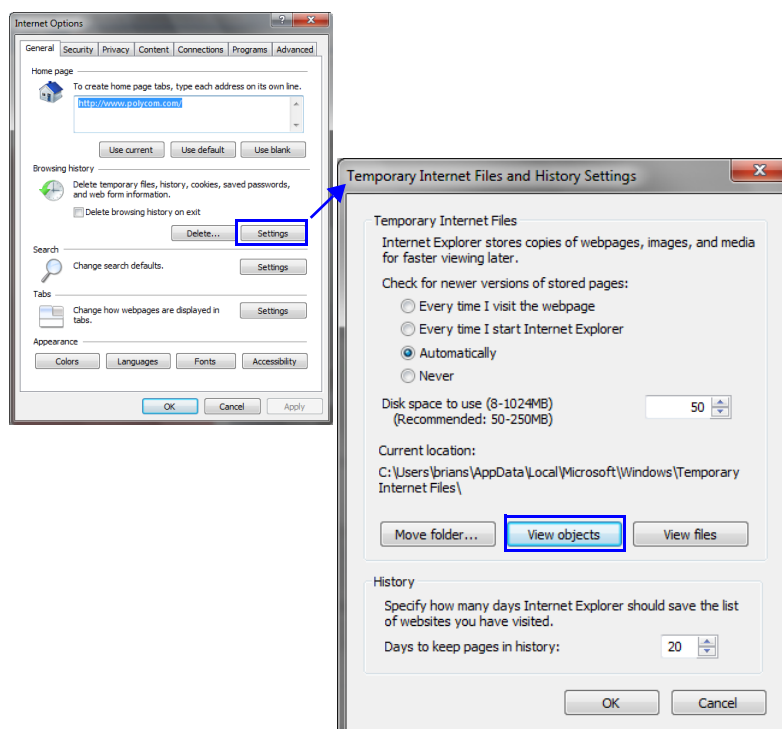
6 Select the **Temporary Internet files** and **Cookies** check boxes.

7 Click the **Delete** button.

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

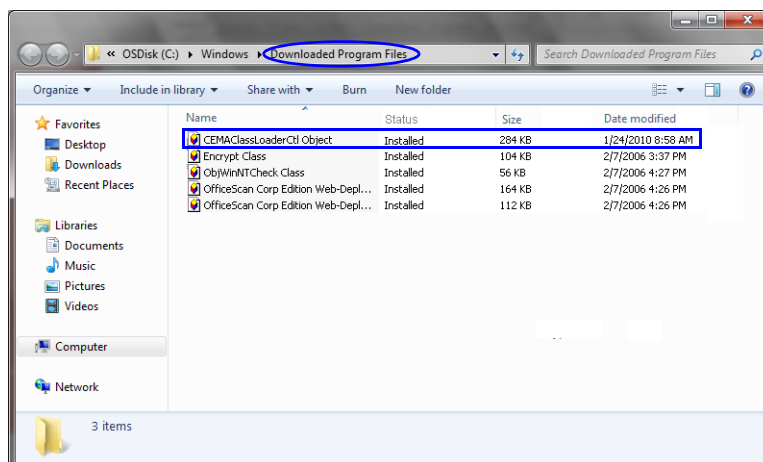
9 In the *Internet Options* dialog box, click the **Settings** button.

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 *CEMAClassLoaderCtrl Object* file
- 12 Press the **Delete** key on the workstation.
- 13 Close the *Downloaded Program Files* folder and the *Temporary Internet Files and History Settings* dialog box.
- 14 In the *Internet Options* dialog box, click the **OK** button to save the changes and close the dialog box.

Polycom Solution Support

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

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

Version 6.0 - Upgrade Procedure

Upgrading to Version 6.0

Upgrading from Version 5.x to Version 6.0 (RMX 2000)

- 1 Download the required software Version 6.0 from the *Polycom Resource Center* web site.



If *Windows 7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 6.0* software to the workstation.
For more information see "*Windows 7™ Security Settings*" on page 9.

- 2 Backup the configuration file. For more information, see the *RMX 2000/4000 Administrator's Guide*, "*Software Management*" on page 18-88.
- 3 Install MCU Software Version 6.0.
On the *RMX* menu, click **Administration > Software Management > Software Download**.
- 4 Browse to the *Install Path*, selecting the **Version 6.0xx.bin** file in the folder where Version 6.0 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.
- 5 Click **OK** in the new activation key message box.
- 6 Click **Close** in the *Install Software* dialog box.
- 7 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 **OK**.
- 9 When prompted whether to reset the *RMX*, click **Yes** to reset the *RMX*.
- 10 When prompted to wait while the *RMX* resets, click **OK** to reset the *RMX*.

The upgrade procedure takes approximately 30 minutes.
Connection to the *RMX* is terminated and you are prompted to reopen the browser.



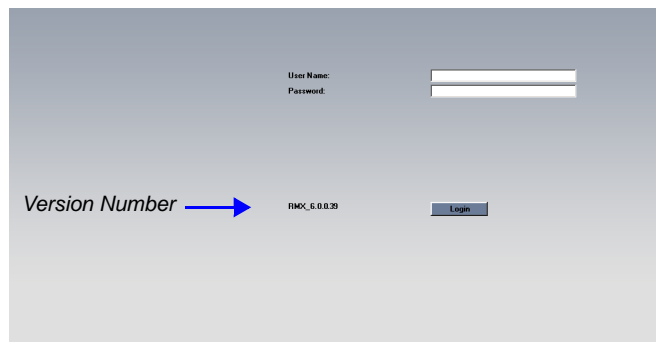
- 11 After approximately 30 minutes close and reopen the browser.
- 12 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RMX*.
The browser displays a message indicating that it cannot display the requested page.
- 13 Refresh the browser 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.*



- 14 **Optional.** Close and reopen the browser.
- 15 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 6.x.x.x.



- 16 In the *RMX Web Client - Welcome* screen, enter your *Username* 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.



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.



To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

Upgrading from Version 3.x/4.x to Version 6.0 (RMX 2000)



When upgrading from version 3.x and 4.x, it is essential that you upgrade directly to version 6.0. Do not perform any intermediate upgrade

- 1 Download the required software Version 6.0 from the *Polycom Resource Center* web site.
- 2 Obtain the Version 6.0 *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 [2-15](#).
- 3 Backup the configuration file. For more information, see the *RMX Administrator's Guide*, "Banner Display and Customization" on page [18-84](#).
- 4 Install MCU Software Version 6.0.
On the RMX menu, click **Administration > Software Management > Software Download**.
- 5 Browse to the *Install Path*, selecting the **Version 6.0xx.bin** file in the folder where Version 6.0 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 Click **Close** to close the *Install Software* dialog box.
- 7 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 **OK**.
- 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.

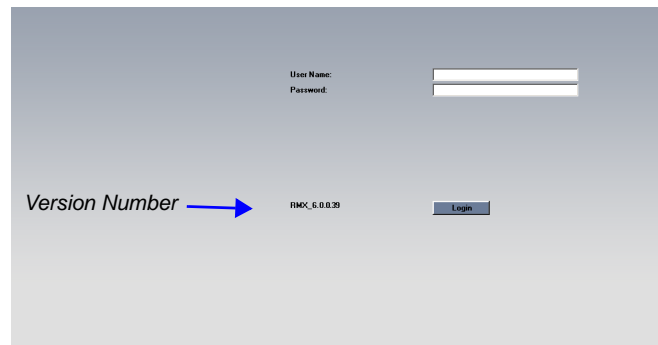
The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP*.



Sometimes when upgrading from version 4.x to version 6.0 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.

- 10 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 6.0.



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



- If upgrading from version 4.x, after software installation, the MCU is in the last *Card Configuration Mode* that was set for the system before the software upgrade. For more information on the Card Configuration Modes, see the RMX 2000 Hardware Guide, "*MPM and MPM+ Configuration Modes*" on page [1-20](#).
- If upgrading from version 2.x or 3.x, after software installation, the MCU is in **MPM Card Configuration Mode**. For details on upgrading to MPM+, see the *RMX 2000 MPM to MPM+ Migration Procedure* document.

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.



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 the POLYCOM User is renamed or a new Administrator User is created and the default User is deleted.



To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

- 12 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 [18](#).



To upgrade from Version 2.x to Version 6.0, you must first upgrade to version 4.1.1 and then upgrade to version 6.0. If after the installation of version 4.1.1 the MCU reset fails, turn the system power off and on again.



If the upgrade process fails, please contact Polycom support.

Additional/Optional System Updates After Upgrading

IVR Services

When upgrading from version 4.0 and earlier, Operator Assistance and the Gateway calls options require that the IVR Service includes specific (new) DTMF Codes and voice messages that 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.



Changes to the DTMF code numbers do not require a new IVR service to be defined.

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.

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 5 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

- 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 [14-9](#).

Gathering Settings

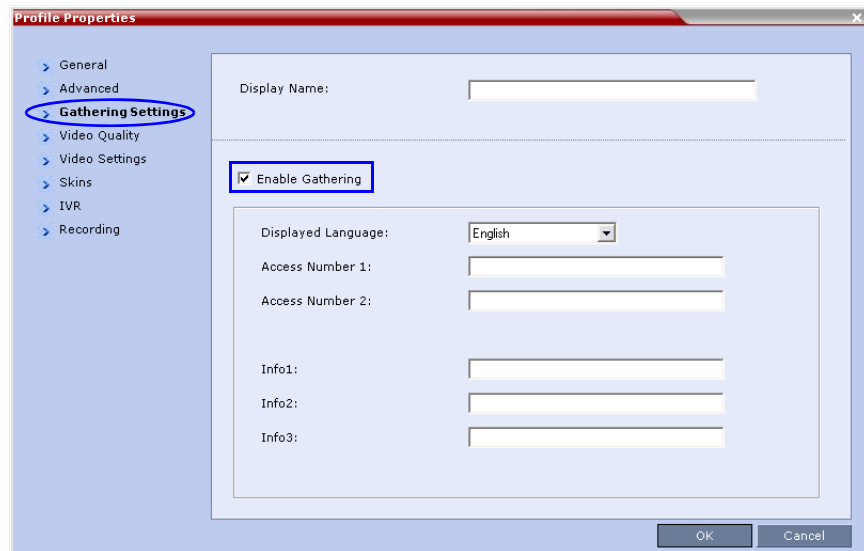
When upgrading from earlier versions, the *Enable Gathering* check box in the *Profile Properties - Gathering Settings* dialog box is not selected by default for existing *Profiles*.

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 "*Gathering Phase*" on page [1-30](#).

Version 6.0 Detailed Description

Polycom Conferencing for Microsoft Outlook®

Polycom Conferencing for Microsoft Outlook is an add-in that enables users to easily organize and invite attendees to *Video Enabled* meetings via Microsoft Outlook®.

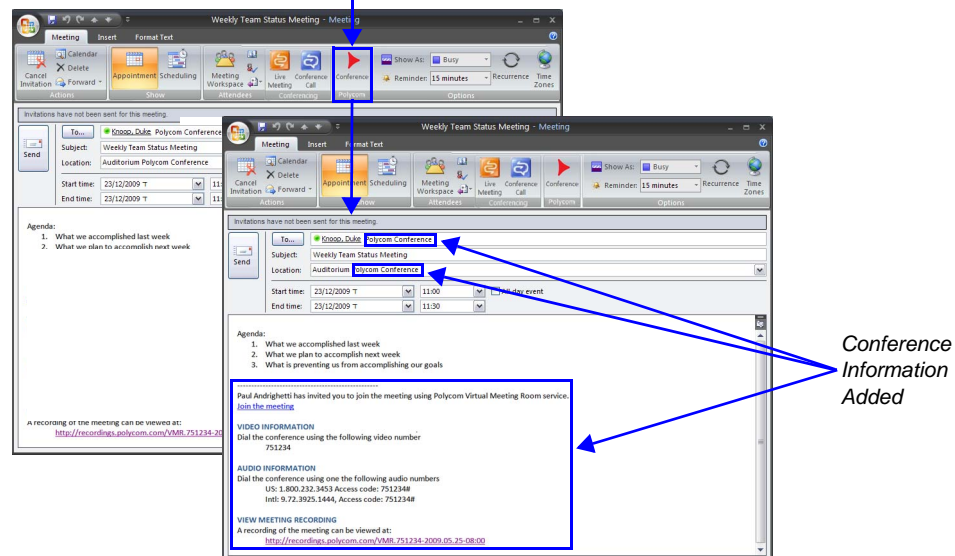
Polycom Conferencing for Microsoft Outlook is implemented by installing the *Polycom Conferencing Add-in for Microsoft Outlook* on the *Microsoft Exchange Server*® and *Microsoft Outlook*® e-mail clients. It enables meetings to be scheduled with video endpoints from within *Outlook*. The add-in also adds a *Polycom Conference* button in the *Meeting* tab of the *Microsoft Outlook* e-mail client ribbon.

The meeting organizer clicks the **Polycom Conference** button to add *Conference Information* to the meeting invitation.

Attendees call the meeting at the scheduled *Start Time* using the link or the dial-in number provided in the meeting invitation.

A *Gathering Slide* is displayed to connected participants until the conference starts.

Polycom Conference Button



Gathering Slide:
Displays Meeting
Information Until
Conference Starts



The *Gathering Slide* displays live video along with information taken from the meeting invitation such as the subject, meeting organizer, duration, dial-in numbers etc. At the end of the *Gathering Phase*, the conference layout is displayed.

For more information see “*Gathering Phase*” on page 1.

Setting up the Calendaring Solution

The following steps are performed to set up the Calendaring solution:

- A The administrator installs the *Polycom Conferencing Add-in for Microsoft* for *Microsoft Outlook* e-mail clients. For more information, see the *Deploying Visual Communications Administration Guide*.
- B The administrator creates an *Microsoft Outlook* e-mail-account for the RMX. If included in the solution, *Polycom DMA system (DMA)* and calendaring-enabled endpoints share this e-mail account. *Deploying Visual Communications Administration Guide*.
- C The administrator configures the RMX for *Calendaring* using the *Exchange Integration Configuration* dialog box, providing it with the *Microsoft Exchange* Server Name, User Name and Password and optional Primary SMTP Mail box information needed to access the e-mail account.

To configure the RMX’s *Exchange Integration Configuration*:

- 1 On the RMX menu, click **Setup > Exchange Integration Configuration**.

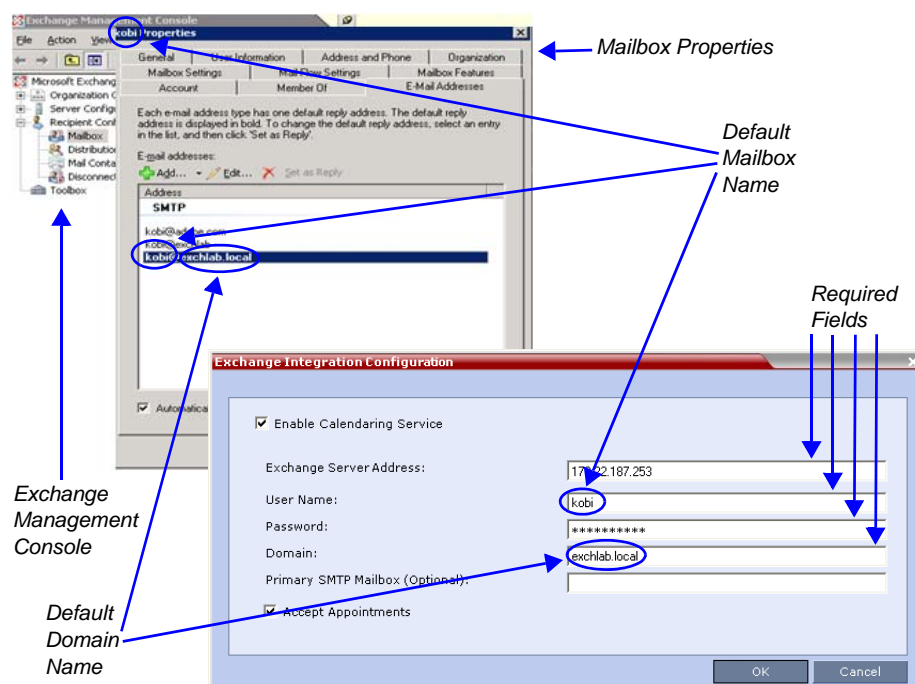
The *Exchange Integration Configuration* dialog box is displayed.



There are three options that can be used to configure the *Exchange Integration Configuration*. The option you choose will depend on the configuration of the mailbox in the *Exchange Server* and the configuration of the *Exchange Server* itself.

- **Option 1** - Use this option if the *Exchange Server* settings have been left at their default values.
- **Option 2** - Use this option if the *Primary SMTP Mailbox* is not the default mailbox.
- **Option 3** - Use this option if the *Exchange Server* settings have been modified by the administrator.

Option 1 - Using default Exchange Server settings



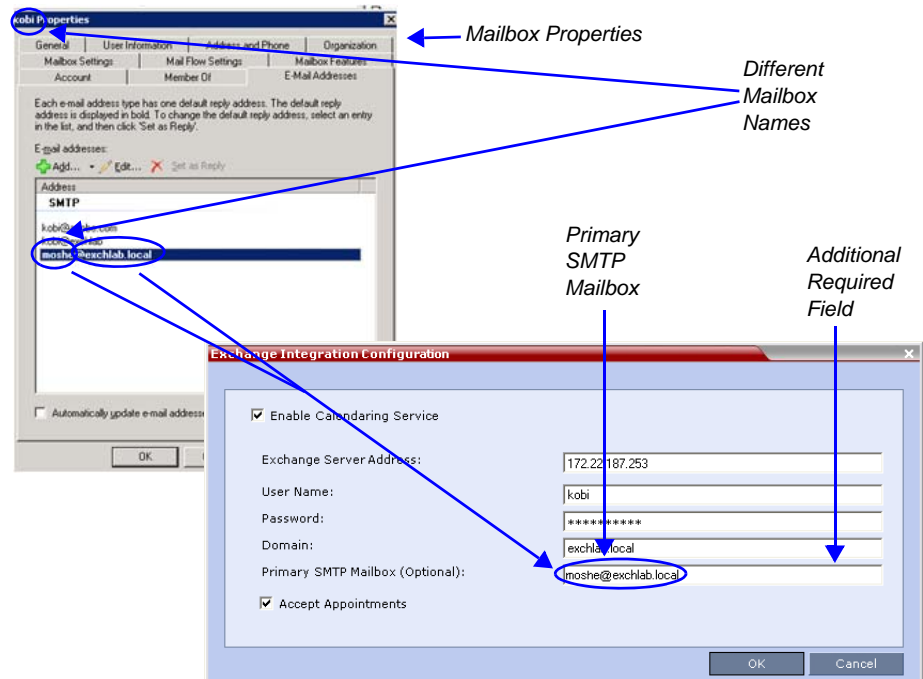
- a Define the following fields:

Table 6 Exchange Integration Configuration - Option 1

Field	Description
<i>Enable Calendaring Service</i>	Select or clear this check box to enable or disable the Calendaring Service using the Polycom Add-in for Microsoft Outlook. When this check box is cleared all fields in the dialog box are disabled.
<i>Exchange Server Address</i>	Enter the IP address of the Exchange Server.
<i>User Name</i>	Enter the User Name of the RMX, as registered in the Microsoft Exchange Server, that the RMX uses to login to its e-mail account. Field length: Up to 80 characters.
<i>Password</i>	Enter the Password the RMX uses to login to its e-mail account as registered in the Microsoft Exchange Server. Field length: Up to 80 characters.
<i>Domain</i>	Enter the name of the network domain where the RMX is installed as defined in the Microsoft Exchange Server.
<i>Primary SMTP Mailbox (Optional)</i>	This field is left empty.
<i>Accept Appointments</i>	Select this check box to enable the RMX to send replies to meeting invitations. Clear this check box when the RMX is part of a Unified Conferencing solution that includes a DMA, as the DMA will send a reply to the meeting invitation.

- b Click the **OK** button.

Option 2 - Using an alternate Primary SMTP Mailbox



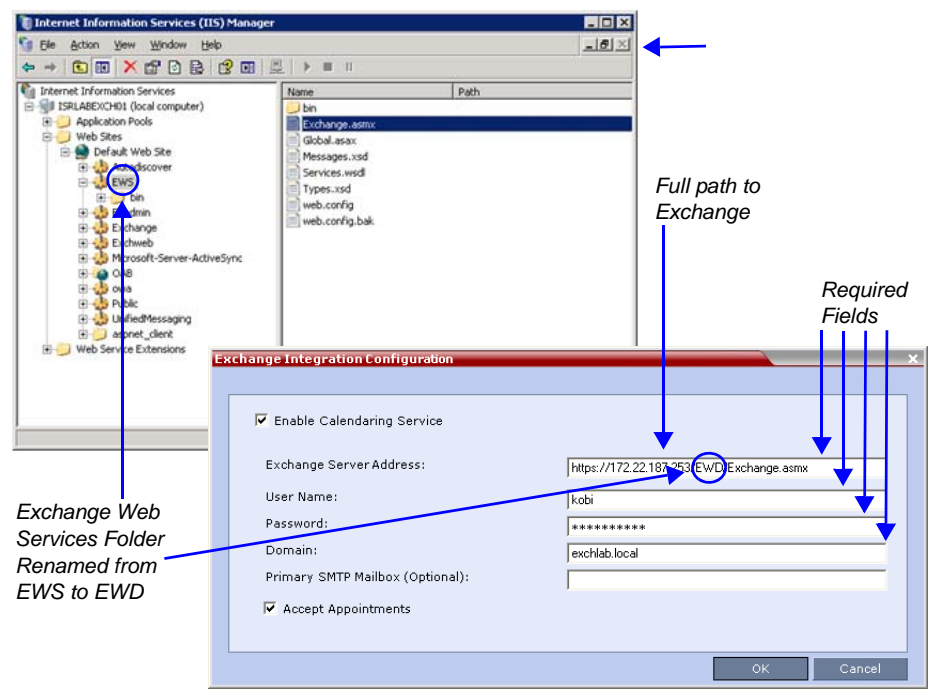
- a Define the following fields:

Table 7 Exchange Integration Configuration - Option 2

Field	Description
Enable Calendaring Service	These fields are defined as for Option 1 above.
Exchange Server Address	
User Name	
Password	
Domain	
Accept Appointments	
Primary SMTP Mailbox (Optional)	Enter the name of the SMTP Mailbox in the Microsoft Exchange Server to be monitored by the RMX. Note: Although several mailboxes can be assigned to each user in the Microsoft Exchange Server, only the Primary SMTP Mailbox is monitored. The Primary SMTP Mailbox name does not have to contain either the RMX's User Name or Domain name.

- b Click the OK button.

Option 3 - Using modified Exchange Server settings



- a Define the following fields:

Table 8 Exchange Integration Configuration - Option 3

Field	Description
Exchange Server Address	<p>If Exchange Server settings have been modified, enter the full path to the Microsoft Exchange Server where the RMX's Microsoft Outlook e-mail account is registered, for example if the EWS folder has been renamed <i>EWD</i>:</p> <p>https://labexch01/EWD/Exchange.asmx</p> <p>Note: If a server name is entered, the RMX and the Microsoft Exchange Server must be registered to the same Domain. (The Domain name entered in this dialog box must match the Local Domain Name entry in the Management Network - DNS Properties dialog box.)</p> <p>For more information see the RMX 2000/4000 Administrator's Guide,"<i>Modifying the Management Network</i>" on page 13-3.</p> <p>Field length: Up to 80 characters.</p>

Table 8 Exchange Integration Configuration (Continued)- Option 3

Field	Description
<i>Enable Calendaring Service</i>	These fields are defined as for Option 1 above.
<i>User Name</i>	
<i>Password</i>	
<i>Domain</i>	
<i>Primary SMTP Mailbox (Optional)</i>	
<i>Accept Appointments</i>	

- b Click the **OK** button.

If applicable, *RSS*, *VMC*, *DMA* and calendaring-enabled endpoints are configured with the *Exchange Server Name*, *User Names* and *Passwords* needed to access their accounts. *Deploying Visual Communications Administration Guide*.

- 2 The administrator configures the RMX to have a default *Ad-hoc Entry Queue* service enabled. If *ISDN/PSTN* participants are included, up to two *ISDN/PSTN* dial-in numbers must be configured for the *Ad Hoc Entry Queue*. For more information see the *RMX 2000/4000 Administrator's Guide*, "Defining a *New Entry Queue*" on page 4-4.

Calendaring Guidelines

- The RMX must have its *MCU* prefix registered in the gatekeeper. For more information see the *RMX 2000/4000 Administrator's Guide*, "Modifying the *Default IP Network Service*" on page 12-13.
- The RMX must be configured as a *Static Route*. For more information see the *RMX 2000/4000 Administrator's Guide*, "Modifying the *Default IP Network Service*" on page 12-13.
- The RMX's *Default Entry Queue* must be configured as an *Ad Hoc Entry Queue* and must be designated as the *Transit Entry Queue*. For more information see the *RMX 2000/4000 Administrator's Guide*, "Entry Queues" on page 4-1.
- The meeting organizer can enable recording and/or streaming of the meeting.
- If meeting is to be recorded, the *Ad Hoc Entry Queue* must have recording enabled in its *Profile*. For more information see the *RMX 2000/4000 Administrator's Guide*, "Defining *Profiles*" on page 1-9.
- Meetings can be single instance or have multiple occurrences.
- Attendees that do not have video devices may be invited to the meeting.
- Attendees using e-mail applications that use the *iCalender* format may be invited to meetings via the *Calendaring Service*.

- Meeting invitations sent by *Polycom Conferencing for Microsoft Outlook* can be in a different language to the *RMX Web Client*. The following languages are supported:
 - English
 - French
 - German
 - International Spanish
 - Korean
 - Japanese
 - Simplified Chinese
- RMX resource management is the responsibility of the system administrator:
 - Conferences initiated by Polycom Conferencing for Microsoft Outlook are ad hoc and therefore resources are not reserved in advance.
 - Polycom Conferencing for Microsoft Outlook Add-in assumes that sufficient resources are available and does not check resource availability. Sufficient resources are therefore not guaranteed.
 - A meeting invitation that is automatically accepted by the RMX is not guaranteed availability of resources.
 - If the RMX runs out of resources, attendees will not be able to connect to their conferences.
- By using DMA to load-balance resources between several RMXs, resource capacity can be increased, alleviating resource availability problems.

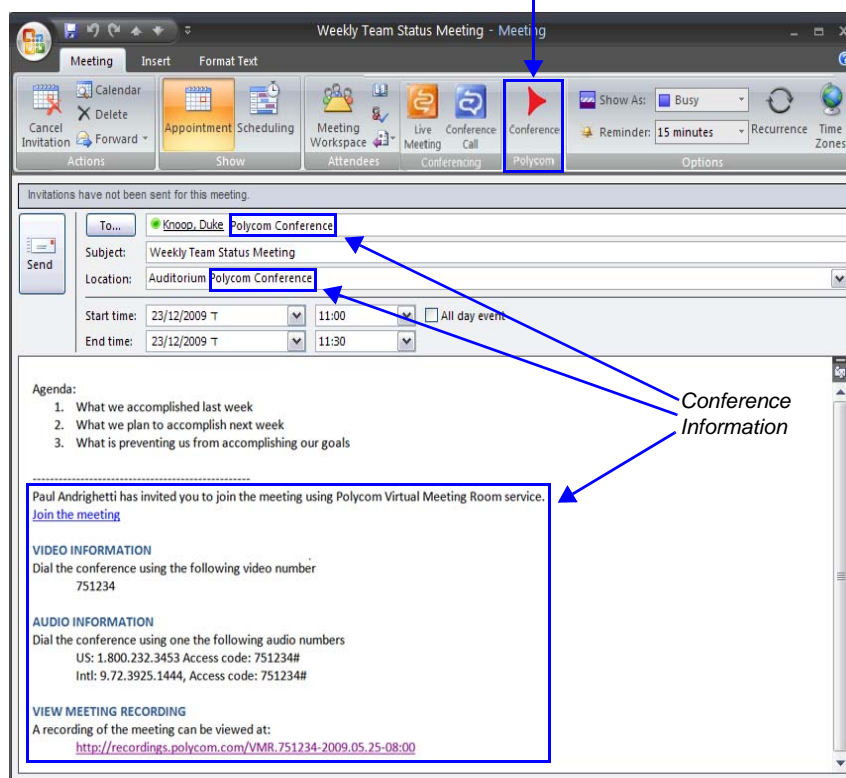
Creating and Connecting to a Conference

Creating a Conference

Meetings are organized using the *Microsoft Outlook* client in the normal manner.

If the meeting organizer decides that video participants are to be included in a multipoint video conference, he/she clicks the **Polycom Conference** button. *Conference Information* such as the *Meeting ID* and connection information is automatically added to the existing appointment information.

Polycom Conference Button



The meeting organizer can add a meeting agenda or personal text to the invitation before it is sent. The meeting organizer can update or cancel the video enabled meeting in the same manner as for any other meeting.

When the meeting organizer sends the meeting invitation a meeting record is saved in the *Microsoft Exchange Server*, the *RMX*, *DMA*, *RSS* and calendaring-enabled endpoints. *RMXs*, *DMA* and calendaring-enabled endpoints poll the *Microsoft Exchange Server* to retrieve new meeting records and updates to existing meeting records.

Table 4 summarizes the *RMX's* usage of *Microsoft Outlook* data fields included in the meeting invitation.

Table 9 Microsoft Outlook Field Usage

Microsoft Outlook Field	Usage by the RMX / DMA	
	Conference / Meeting Room	Gathering Slide
<i>Subject</i>	Display Name of Conference / Meeting Room.	Meeting Name.

Table 9 *Microsoft Outlook Field Usage*

Microsoft Outlook Field	Usage by the RMX / DMA	
	Conference / Meeting Room	Gathering Slide
<i>Start/End Time</i>	Used to calculate the Conference's Duration.	
<i>Record</i>	Enable Recording in the Conference or Meeting Room Profile.	Display Recording option.
<i>Video Access Number</i>	<p>Comprised of: <MCU Prefix in Gatekeeper> <Conference Numeric ID>.</p> <p>Note: It is important that <i>MCU Prefix in Gatekeeper</i> field in the RMX's <i>IP Network Service - Gatekeeper</i> tab and the <i>Dial-in prefix</i> field in the <i>Polycom Conferencing Add-in for Microsoft Outlook - Video Network</i> tab contain the same prefix information.</p> <p>If Recording and Streaming are enabled in the Conference Profile, this number is used as part of the recording file name.</p>	Displayed as the IP dial in number in the Access Number section of the Gathering Slide.
<i>Audio Access Number</i>	ISDN/PSTN dial-in number. Up to two numbers are supported.	Displayed as the ISDN/ PSTN dial-in number in the Access Number section of the Gathering Slide.
<i>Streaming recording link</i>	<p>Enables the recording of the conference to the Polycom RSS using the recording link.</p> <p>Enables streaming of the recording of the conference from the Polycom RSS.</p>	If recording is enabled, a REC indicator is displayed in the top left corner of the slide.

Connecting to a Conference

Participants can connect to the conference in the following ways:

- Participants with *Polycom CMA Desktop™* or a *Microsoft Office Communicator* client running on their PCs can click on a link in the meeting invitation to connect to the meeting.
- Participants with a *HDX* or a room system will receive a prompt from the endpoint's calendaring system along with a button that can be clicked in order to connect.
Participants with endpoints that are not calendaring-enabled can connect to the meeting by dialing the meeting number manually.
- Participants outside the office or using *PSTN* or mobile phones, can use the dial in number in the meeting invitation to manually dial in to the meeting.

RMX Standalone Deployment

When using a single *RMX* in a standalone deployment, connection is via an *Ad Hoc Entry Queue*. The meeting is started when the first participant connects to the *RMX*.

When the first participant connects, a conference is created and named according to the information contained in the dial string. Subsequent participants connecting with the same dial string are routed from the *Ad Hoc Entry Queue* to the conference.

After the conference has been created the *Conference Name*, *Organizer*, *Time*, *Duration* and *Password* (if enabled) are retrieved from the conference parameters for display during the *Gathering Phase*.

RMX and Polycom DMA System Deployment

In a *DMA* deployment a *Virtual Meeting Room* is activated when the first participant connects to the *DMA*. *DMA* receives the dial string to activate a *Virtual Meeting Room* on the *RMX*.

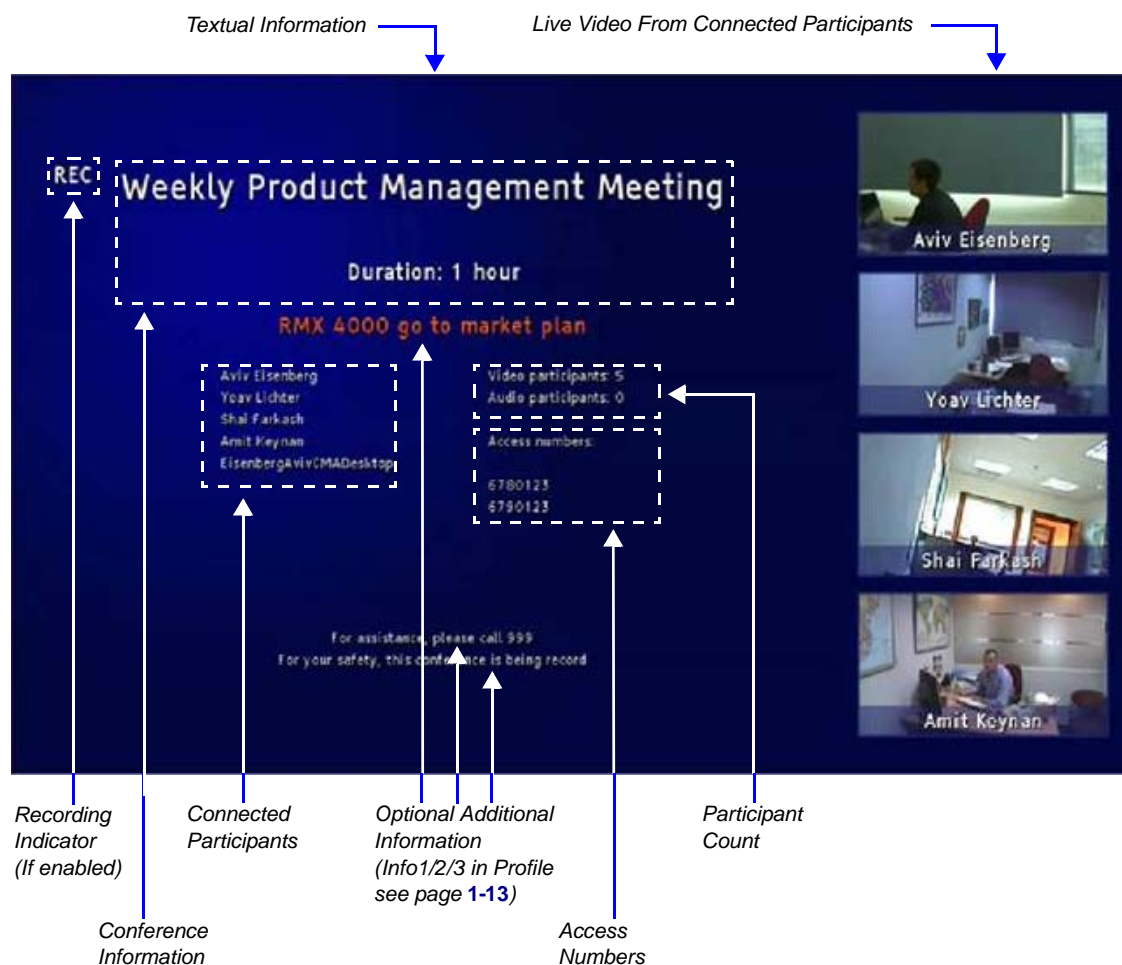
DMA uses the *Meeting ID* contained in the dial-in string to access meeting information stored in the *Exchange Server* database.

When the meeting information is found on the *Exchange Server*, the *Conference Name*, *Organizer*, *Time*, *Duration* and *Password* (if enabled) are retrieved from the *Exchange Server* database for display during the *Gathering Phase*.

Gathering Phase

The *Gathering Phase* of a conference is the time period during which participants are connecting to a conference. During the *Gathering Phase*, a mix of live video from connected endpoints is combined with both static and variable textual information about the conference into a slide which is displayed on all connected endpoints. All connected participants are kept informed about the current conference status including names of connected participants, participant count, participant type (video/audio) etc.

During the *Gathering Phase*, the audio of all participants can be heard, and the video of active speakers is displayed in the video windows as they begin talking.

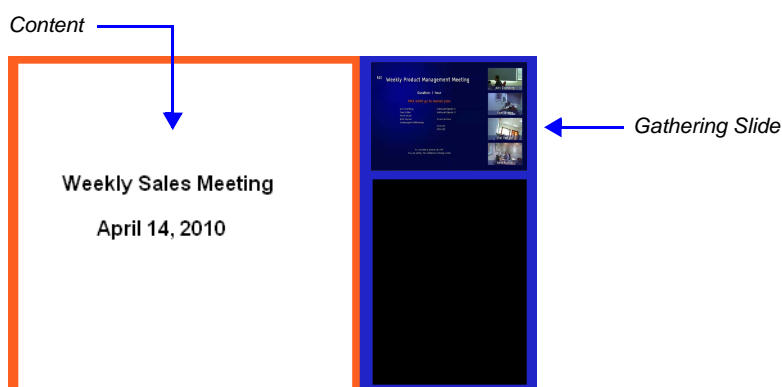


Gathering Phase Guidelines

- The *Gathering Phase* slide can be displayed at any time during the conference by entering the *Show Participants DTMF* code, *88.
- The *Gathering Phase* is not supported in *Video Switching Conferences*.
- The names of the first eight participants to connect are displayed. If eight or more participants connect, the 8th row displays "...".
- **Static text** in the *Gathering Phase* slide such as the field headings: *Organizer, Duration, Video/Audio Participants, Access Number, IP* are always displayed in the language as configured in the *Polycom Virtual Meeting Rooms Add-in for Microsoft*

Outlook. The following languages are supported:

- English
- French
- German
- International Spanish
- Korean
- Japanese
- Simplified Chinese
- **Dynamic text** in the *Gathering Phase* slide such as the meeting name, participants names, access numbers and the additional information entered in the *Info1/2/3* fields of the *Gathering Settings* tab of the conference *Profile* are displayed in the language of the meeting invitation.
- The language of a *Gathering Phase* slide of a conference configured to include a *Gathering Phase* that is not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* is configured by the administrator. Using the *RMX Web Client*, the administrator selects the language for the *Gathering Phase* slide. The language selected can be different to that of the *RMX Web Client* used by the administrator to perform the configuration.
- *Content* can be sent during the *Gathering Phase*. The content is displayed in the large video window of the participant's layout while the *Gathering* slide is displayed in a smaller video window in the layout.



Gathering Phase Duration

The duration of the *Gathering Phase* can be customized by the administrator so that it is long enough to be viewed by most connected participants yet short enough so as not to over extend into the scheduled conferencing time.

The *Gathering Phase* duration is configured for the *RMX*, by the following *System Flags* in *system.cfg* using the *Setup > System Configuration* menu:

- **CONF_GATHERING_DURATION_SECONDS**

Range: 0 - 3600 seconds

Default: 180 seconds

The *Gathering Phase* duration of the conference is measured from the scheduled start time of the conference.

Example: If the value of the flag is set to **180**, the *Gathering* slide is displayed for three minutes to all participants starting at the conference *Start Time*, and ending three minutes after the conference *Start Time*.

For participants who connect before *Start Time*, the *Gathering* slide is displayed from the time of connection until the end of the *Gathering* duration period.

- **PARTY_GATHERING_DURATION_SECONDS**

Range: 0 - 3600 seconds

Default: 15 seconds

The value of this flag determines the duration of the display of the *Gathering* slide for participants that connect to the conference after the conference *Start Time*.

Participants connecting to the conference very close to of the end of the *Gathering Phase* (when there are fewer seconds left to the end of the *Gathering Phase* than specified by the value of the flag) have the *Gathering* slide displayed for the time specified by the value of the flag.

Example: If the value of the flag is set to **15**, the *Gathering Phase* slide is displayed to the participant for 15 seconds.

Enabling the Gathering Phase Display

The *Gathering Phase* is enabled for per conference in the *Conference Profile*. The profile also includes the dial-in numbers and the optional additional information to display on the slide.

Conferences that are configured to include a *Gathering Phase* that are not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* need the following information to be entered via the *New Profile* or *Profile Properties – Gathering Settings* dialog box:

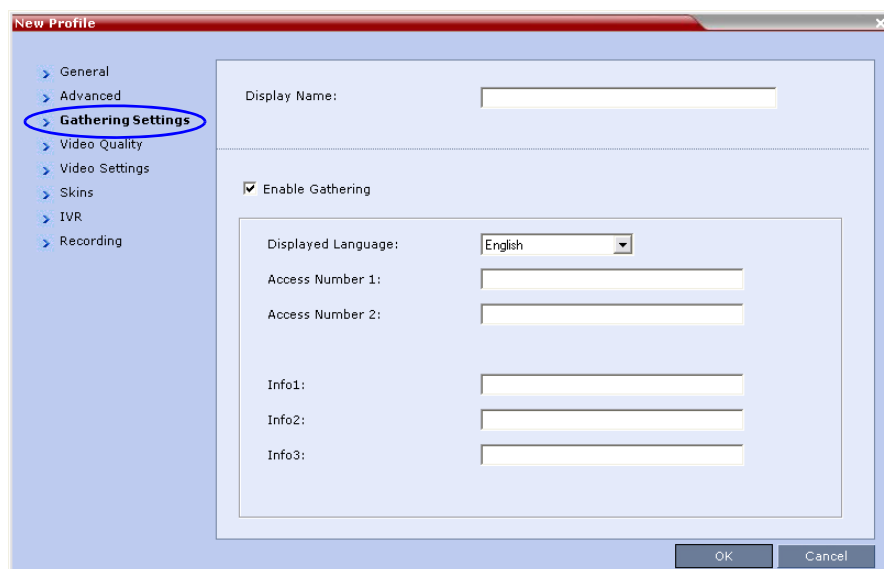
- *Display Name* (Optional, the *Meeting Name* is used if left blank.)
- *Displayed Language*
- *Access Number 1 / 2* (Optional.)
- *Additional Information* (Optional free text)
 - *Info 1*
 - *Info 2*
 - *Info 3*

Conferences launched by the *Polycom Conferencing Add-in for Microsoft Outlook* receive this information from the meeting invitation.

To enable the Gathering Phase:

- 1 In the *RMX Management* pane, click **Conference Profiles**.
- 2 In the *Conference Profiles* pane, click the **New Profile** button or double-click the entry of an existing profile to be modified.

- 3 Click the **Gathering Settings** tab.




- 4 Define the following fields:

Table 10 Profile - Gathering Settings

Field	Description
<i>Display Name</i>	This field is defined when the <i>Profile</i> is created. For more information see the <i>RMX 2000/4000 Administrator's Guide</i> , "Defining Profiles" on page 1-9.
<i>Enable Gathering</i>	Select this check box to enable the <i>Gathering Phase</i> feature. Default: Selected.
Displayed Language	Select the <i>Gathering Phase</i> slide language: <i>Gathering Phase</i> slide field headings are displayed in the language selected. The <i>Gathering Phase</i> slide can be in a different language to the <i>RMX Web Client</i> . Default: English Note: When working with the <i>Polycom Conferencing Add-in for Microsoft Outlook</i> , the language selected should match the language selected for the conference in the <i>Polycom Conferencing Add-in for Microsoft Outlook</i> to ensure that the <i>Gathering Phase</i> slide displays correctly.
<i>Access Number 1</i>	Enter the ISDN or PSTN number(s) to call to connect to the conference. Note: The numbers entered must be verified as the actual Access Numbers.
<i>Access Number 2</i>	

Table 10 Profile - Gathering Settings

Field	Description
Info 1	<p>Optionally, enter any additional information to be displayed during the Gathering Phase.</p> <p>These fields are not limited in the RMX Web Client but only 96 characters can be displayed in the Gathering Slide on a 16:9 monitor.</p> <p>If the Gathering slide is displayed on a 4:3 endpoint: the slide is cropped on both sides:</p> <ul style="list-style-type: none"> The left most characters of the information fields will not be displayed. The live video is cropped on the right side of the display. <div data-bbox="702 694 1394 985">  </div>
Info 2	
Info 3	

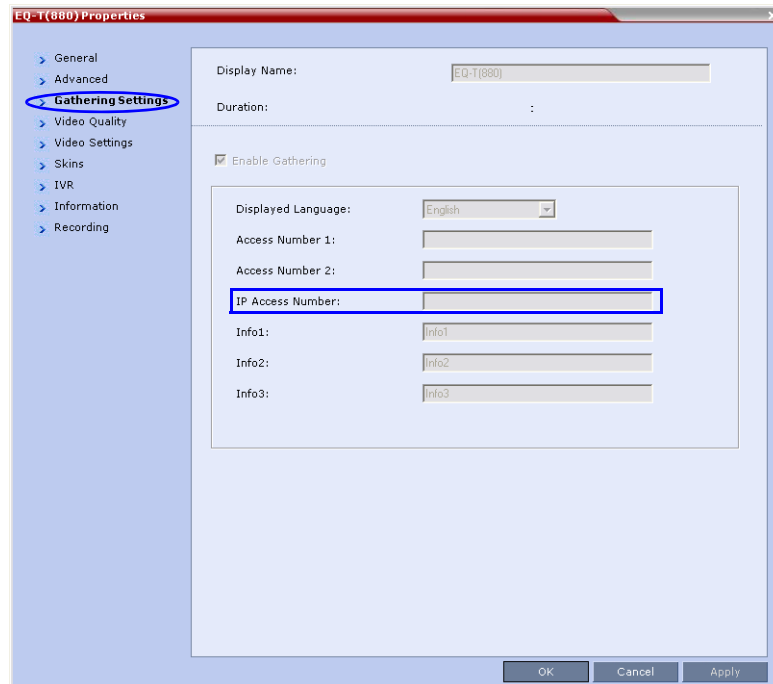
5 Click OK.

Monitoring Gathering-enabled Conferences

Conferences launched by the *Polycom Conferencing Add-in for Microsoft Outlook* are monitored in the same manner as all other conferences.

In the gathering settings tab, an additional field, *IP Access Number*, is displayed in addition to the ISDN/PSTN access numbers, *Access Number 1* and *Access Number 2* which were entered when defining the conference *Profile*.

The *IP Access Number* is made up of the *Conference ID* generated by the *Polycom Conferencing Add-in for Microsoft Outlook* and the gatekeeper prefix.



The screenshot shows the 'EQ-T(880) Properties' dialog box with the 'Gathering Settings' tab selected. The 'Gathering Settings' tab is highlighted with a blue circle. The 'IP Access Number' field is highlighted with a blue rectangle. The dialog box contains the following fields and options:

- Display Name: EQ-T(880)
- Duration: :
- ☒ Enable Gathering
- Displayed Language: English (dropdown menu)
- Access Number 1:
- Access Number 2:
- IP Access Number:
- Info1: info1
- Info2: info2
- Info3: info3

At the bottom of the dialog box are the buttons: OK, Cancel, and Apply.

Auto Brightness

Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.

Guidelines

- *Auto Brightness* is supported with MPM+ cards only.
- *Auto Brightness* only increases brightness and does not darken video windows.
- *Auto Brightness* is enabled by the **SET_AUTO_BRIGHTNESS** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.

Possible Values: ON / OFF

Default: OFF

Audio Clarity

Audio Clarity improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.

The enhancement is applied to the following low bandwidth (4kHz) audio algorithms:

- G.729a
- G.711

Guidelines

- *Audio Clarity* is supported with MPM+ cards only.
- *Audio Clarity* is enabled by the **SET_AUDIO_CLARITY** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.

Possible Values: ON / OFF

Default: OFF

Packet Loss Concealment (PLC) for Audio

Packet Loss Concealment (PLC) for *Siren* audio algorithms improves received audio when packet loss occurs in the network.

The following audio algorithms are supported:

- Siren 7 (mono)
- Siren 14 (mono/stereo)
- Siren 22 (mono/stereo)

Guidelines

- *PLC for Audio* is supported with MPM+ cards only.
- The speaker's endpoint must use a *Siren* algorithm for audio compression.
- *PLC* is enabled by the **SET_AUDIO_PLC** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.

Possible Values: ON / OFF

Default: ON

Siren 22 and G.719 Audio Algorithm Support

Polycom's proprietary *Siren 22* and industry standard *G.719* audio algorithms are supported for participants connecting with *Polycom* endpoints.

The *Siren 22* Audio Algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications. *Siren 22* requires dramatically less computing power and has much lower latency than alternative wideband audio technologies.

Guidelines

- *Siren 22*, *G.719* and *Siren 22Stereo* are supported with *MPM+* cards only.
- *Siren 22* and *G.719* are supported in both mono and stereo.
- Stereo is supported in *H.323* calls only.
- *Siren 22* is supported by Polycom HDX endpoints, version 2.0 and later.

Mono

The *Siren 22* and *G.719* mono audio algorithms are supported at the following bit rates:

Table 11 *Siren22 and G.719 Mono vs Bitrate*

Audio Algorithm	Minimum Bitrate (kb)
Siren22 64k	384
<i>Siren22 48K</i>	
<i>Siren22_32k</i>	
G.719_64k	
G.719_48k	
G.719_32k	
<i>Siren22_48K</i>	256
<i>Siren22_32k</i>	
G.719_48k	
G.719_32k	
<i>Siren22_32k</i>	128
G.719_32k	

Stereo

The *Siren 22Stereo* and *G.719Stereo* audio algorithms are supported at the following bit rates.

Table 12 *Siren22Stereo and G.719Stereo vs Bitrate*

Audio Algorithm	Minimum Bitrate (kb)
<i>Siren22Stereo_128k</i>	1024
<i>Siren22Stereo_96k</i>	
<i>Siren22Stereo_64k</i>	
<i>G.719Stereo_128k</i>	
<i>G.719Stereo_96k</i>	
<i>G.719Stereo_64k</i>	
<i>Siren22Stereo_96k</i>	512
<i>Siren22Stereo_64k</i>	
<i>G.719Stereo_96k</i>	
<i>G.719Stereo_64k</i>	
<i>Siren22Stereo_64k</i>	384
<i>G.719Stereo_64k</i>	

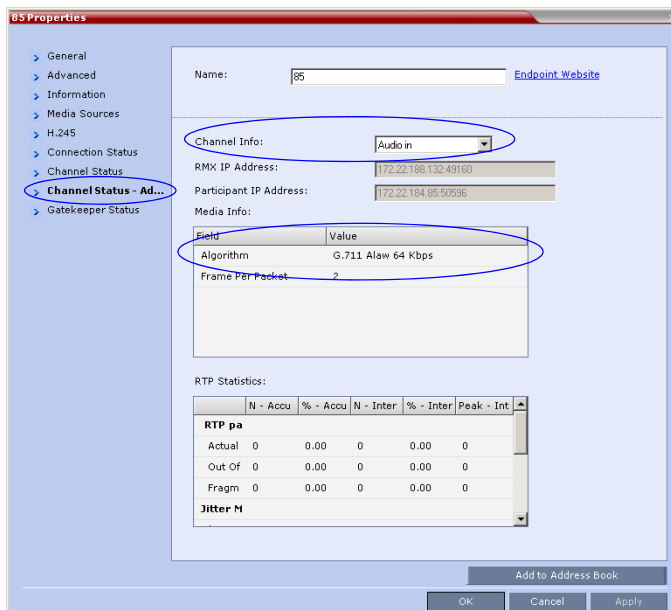
Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the Participant Properties - Channel Status dialog box.

To view the participant's properties during a conference:

- 1 In the *Participants* list, right click the desired participant and select **Participant Properties**.
- 2 Click the **Channel Status - Advanced** tab.
The *Participant Properties - Channel Status - Advanced* dialog box is displayed.

- 3 In the *Channel Info* field, select **Audio In** or **Audio Out** to display the audio parameters.



85 Properties

- General
- Advanced
- Information
- Media Sources
- H.245
- Connection Status
- Channel Status
- Channel Status - Ad...**
- Gatekeeper Status

Name: 85 [Endpoint Website](#)

Channel Info: Audio In

RMX IP Address: 172.22.188.132:49160

Participant IP Address: 172.22.184.85:50596

Media Info:

Field	Value
Algorithm	G.711 Alaw 64 Kbps
Frame Per Packet	2

RTP Statistics:

	N - Accu	% - Accu	N - Inter	% - Inter	Peak - Int
RTP pa					
Actual	0	0.00	0	0.00	0
Out Of	0	0.00	0	0.00	0
Fragm	0	0.00	0	0.00	0
Jitter M					

Add to Address Book

OK Cancel Apply

- 4 Click the **OK** button.

Microsoft Environment - Creating and Exporting the Security Certificate to the RMX Workstation





When working in Microsoft R1 and R2 environment or when encryption of SIP signaling is used, the SIP server and the RMX *Transport Type* must be set to TLS and a certificate must be created and sent to the RMX.

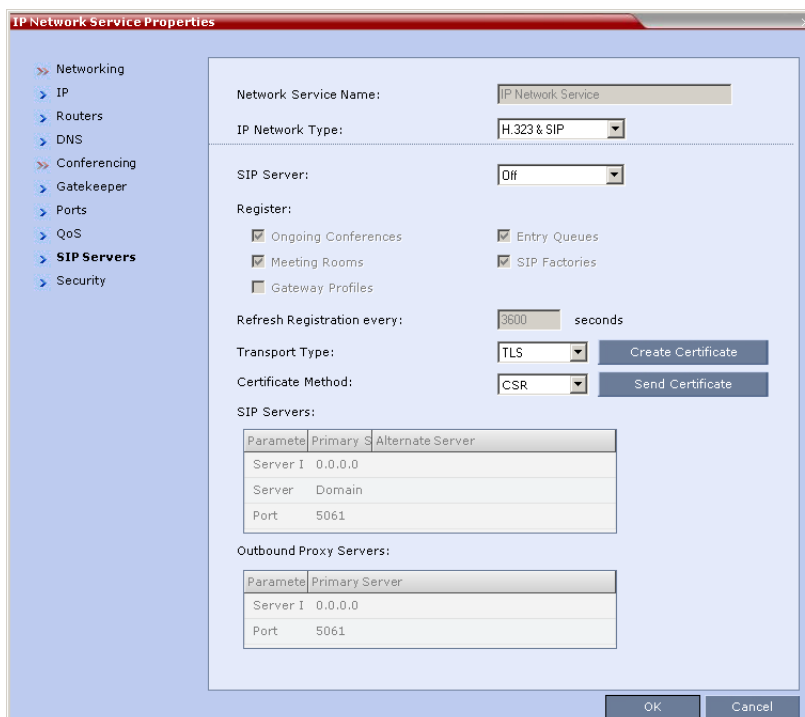
An additional secured and standard method of certificate installation called CSR can be used to install the required certificate.

The CSR method consists of the following steps:

- Creating the certificate request (in the *Default IP Network Service - SIP Server* dialog box).
- Sending the certificate request to a Certificate Authority.
- Receiving the certificate from the Certificate Authority.
- Installing the certificate in the RMX (in the *Default IP Network Service - SIP Server* dialog box).

Creating the Certificate Request

- 1 In the *RMX Management* pane, click **IP Network Services** ().
- 2 In the *Network* list pane, double-click the **Default IP Service** (, , or ) entry. The *Default IP Service - Networking IP* dialog box opens.
- 3 Click the **SIP Servers** tab.



The screenshot shows the 'IP Network Service Properties' dialog box with the 'SIP Servers' tab selected. The left pane shows a tree view with 'SIP Servers' highlighted. The main area contains the following fields and controls:

- Network Service Name:** IP Network Service
- IP Network Type:** H.323 & SIP
- SIP Server:** Off
- Register:**
 - ☒ Ongoing Conferences
 - ☒ Meeting Rooms
 - ☐ Gateway Profiles
 - ☒ Entry Queues
 - ☒ SIP Factories
- Refresh Registration every:** 3600 seconds
- Transport Type:** TLS
- Certificate Method:** CSR
- SIP Servers:**

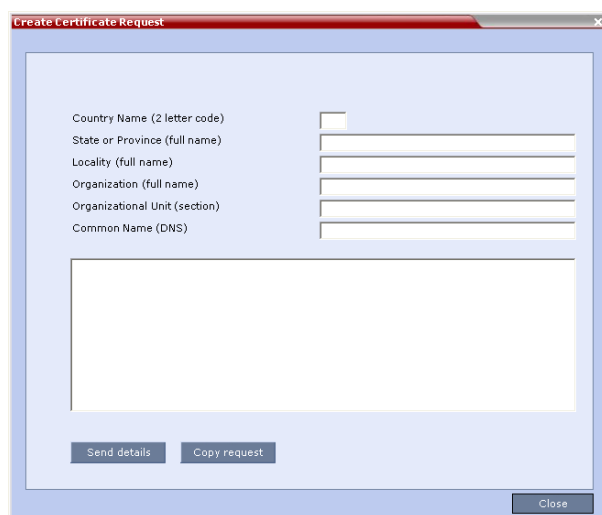
Parameter	Primary	Alternate Server
Server 1	0.0.0.0	
Server	Domain	
Port	5061	
- Outbound Proxy Servers:**

Parameter	Primary Server
Server 1	0.0.0.0
Port	5061

Buttons: Create Certificate, Send Certificate, OK, Cancel.

- 4 Make sure that the *Registration* options (*Ongoing Conferences*, *Meeting Rooms*, *Gateway Profiles*, *Entry Queues* and *SIP factories*) are not selected (check boxes are cleared).

- 5 Make sure that the IP address of the Office Communications Server 2007 is specified and the *Server Domain Name* is the same as defined in the OCS and in the *Management Network* for the DNS.
- 6 If not selected by default, change the *Transport Type* to **TLS**.
The *Create Certificate* and *Send Certificate* buttons are enabled.
- 7 If not selected by default, change the *Certificate Method* to **CSR**.
- 8 Click the **Create Certificate** button.
The *Create Certificate Request* dialog box is displayed.



- 9 Enter information in all the following fields:

Table 13 *Create Certificate Request*

Field	Description
Country Name	Enter any 2 letter code for the country name.
<i>State or Province</i>	Enter the full name of the state or province.
<i>Locality</i>	Enter the full name of the town/city/location.
<i>Organization</i>	Enter the full name of your organization for which the certificate will be issued.
<i>Organizational Unit</i>	Enter the full name of the unit (group or division) for which the certificate will be issued.
<i>Common Name (DNS/ IP)</i>	Enter the <i>DNS MCU Host Name</i> . This <i>MCU Host Name</i> must also be configured in the <i>Management Network Properties</i> dialog box.

- 10 Click **Send Details**.

The RMX creates a *New Certificate Request* and returns it to the *Create Certificate Request* dialog box along with the information the user submitted.

Create Certificate Request

Country Name (2 letter code)	<input type="text" value="PL"/>
State or Province (full name)	<input type="text" value="Tivachet"/>
Locality (full name)	<input type="text" value="Petikoya"/>
Organization (full name)	<input type="text" value="Polycorn"/>
Organizational Unit (section)	<input type="text" value="PD"/>
Common Name (DNS)	<input type="text" value="rmx154"/>

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBKjCB/AIBADBTQswCgYDVQQGEwUJTDJELMAKGAIUECBMCDNUdAxCzAJBgNVBAACT
AJHMRARwGTVDOVQKEwdQEKZQZQ09RMmNMQSwCgYDVQLwEwIjEwNmELMAKGAIUEA
gZWdwDQoJKzZlbnRvbmQAQEBBAQAGPjOAMGAgGAALBzhuzazVgbuwh/LITCqJZ2TG
tJmXdmEtb8Hlx+eRQMvEXasuxugA34/DVJAJMHHbbmcQBjNuairVbaulk.MhgDrp
oIdukBN6nm+5pdv61/gFN7o43qqWEvhDuBchnTAw/R923oz738b/Y9p2b+69rth
eL0ZkQcVBAPs44ajAgMBAAQGAADANBgkqhkiG9w0BAQAFAAOBgQCWiqzGlabeZOEH
qNi6TB2E9cmosZnU1f+UB7IZ2OIloSk+9wwk1pdyXB7F5jdJ1+N/vr6RGhd
XS5yBwmwOFK7IZ2n6VpDoENelFPj9QmsZeWIUZWF0no75JIKZq7XAoy/nib4
JKI/THE9/RAOCtkm7eX4dk2HuTSdq==
-----END NEW CERTIFICATE REQUEST-----
```

- 11 Click **Copy Request** to copy the *New Certificate Request* to the workstation's clipboard.
- 12 Connect to your preferred *Certificate Authority's* website using the web browser.
- 13 Follow the purchasing instructions at the *Certificate Authority's* website. Paste (**Ctrl + V**) the *New Certificate Request* as required by the *Certificate Authority*. The *Certificate Authority* issues the TLS/SSL certificate, and sends the certificate to you by e-mail.



If the process of purchasing the certificate is short, you may leave the *IP Network Service - SIP Servers* dialog box open. Otherwise, close it without saving the changes to the Transport Type and Certificate Method.

Installing the Certificate

To install the certificate:

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



If you have closed the *IP Network Service - SIP Servers* dialog box, repeat steps 1 to 7 in the procedure "Installing the Certificate" on page 1-44.

- 1 Open the *Certificate Authority* email and **Copy (Ctrl + C)** the certificate information from the *Certificate Authority's* e-mail to the clipboard.
- 2 In the *IP Network Service - SIP Servers* dialog box, click the **Send Certificate** button. The *Send Certificate* dialog box opens.

- 3 Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.



- 4 Click the **Send Certificate** button to send the certificate to the RMX.



- 5 Click the **Close** button.
- 6 In the *IP Network Service - SIP Servers* dialog box, complete the SIP Servers definitions.
- 7 Click **OK**.

The MCU validates the certificate.

- If the certificate is not valid, an error message is displayed.
- If the certificate matches the private key, and the task is completed, a confirmation message indicating that the certificate was created successfully is displayed.

- 8 Reset the RMX.



Certificates are deleted when an administrator performs a *Restore Factory Defaults* with the *Comprehensive Restore* option selected.

Version 6.0 Detailed Description - Changes to Existing Features

PSTN Dial-in Using GK Prefix

When connecting to an RMX that is standalone or part of a DMA solution deployment, PSTN participants are prompted by an IVR message requesting the *Destination Conference ID* followed by the # key to be entered using the DTMF input keypad.

Including the *Gatekeeper Prefix* in the DTMF input string enables PSTN participants to use the input string when connecting to an RMX whether the RMX is a standalone MCU or part of a DMA solution deployment.

For more information see the *RMX 2000/4000 Administrator's Guide*, "Gateway Calls" on page 15-1.

Enabling PSTN dial-in using GK prefix

The feature is enabled by the `USE_GK_PREFIX_FOR_PSTN_CALLS` System Flag in `system.cfg` using the **Setup > System Configuration** menu.

Possible Values: YES / NO

Default: NO

Table 14 summarizes the PSTN participant's DTMF input depending on the flag value.

Table 14 PSTN Participant input via DTMF

Configuration	FLAG: USE_GK_PREFIX_FOR_PSTN_CALLS=	
	NO	YES
Standalone RMX Conference ID= 1234	PSTN participant enters: 1234#.	PSTN participant enters: 761234#
RMX with DMA Virtual Meeting Room ID in DMA = 1234 DMA gatekeeper prefix = 76	PSTN participant enters: 761234#	(The <i>Gatekeeper Prefix</i> "76" is automatically removed from the DTMF input string for a standalone RMX.)

RMX Resource Management by CMA and DMA

Currently, when both *CMA* and *DMA* are part of the solution, each application works independently and is unaware of the RMX resources used by the other application.

In version 6.0, following a request by the CMA and DMA, the RMX will send updates on resource usage to both *CMA* and *DMA*, with each application updating its own resource usage for the RMX. This provides better management of the RMX resources by CMA and DMA.

Guidelines

- Resource usage updates from RMX to the CMA and DMA are supported only with RMXs with MPM+ Cards.
- Both Flexible Resource Capacity™ and Fixed Resource Capacity™ modes are supported.
- Following requests sent by CMA and DMA, the RMX will send the number of occupied resources for a conference or total for the MCU, according the Resource capacity mode used by the system.
 - In *Flexible Resource Capacity Mode*, CMA/DMA receive information about how many *Video (CIF)* and *Audio* resources are occupied per conference or MCU according the request type sent by the CMA and DMA.
 - In *Fixed Resource Capacity™ Mode*, CMA/DMA receive information about the number of occupied resources per resource type (Audio only, CIF, SD, HD 720p, HD 1080p) and per conference or MCU according the request type sent by the CMA and DMA.
- Occupied resources are resources that are connected to ongoing conferences. Disconnected endpoints in an ongoing conference are not counted as occupied resources.
- An ongoing conference that does not include participants and the *Send Content to Legacy Endpoints* option is disabled does not occupy resources. If the *Send Content to Legacy Endpoints* option is enabled, the conference occupies one SD resource.
- The RMX is unaware of the resource usage split between the CMA and DMA.

Recording Link Layout





















When the video layout of the conference is set to Auto Layout, the recording of the conference will now include all the conference participants and not n-1 participants as in previous versions.

In the new Auto Layout algorithm, the Recording Link is counted as a “participant” and therefore it is excluded from the layout display used for the recording. The layout used for the other participants will behave as in the “standard” Auto Layout behavior.

The Recording Link Layout can be changed during an ongoing conference in the same manner as for any other conference participant. For more information see the *RMX 2000/4000 Getting Started Guide*, “Personal Layout Control with the RMX Web Client” on page 3-67.

The default settings for Auto Layout for the conference and the Recording Link are summarized in the following table:

Table 15 Recording Link Default Layout Settings (Auto Layout Mode)

Participants	Conference Auto Layout Default Settings	Recording Link Auto Layout Settings
0	Not applicable	Not applicable
1		
2		
3		
4		
5		
6		
7		
8		
9		
10 or more		

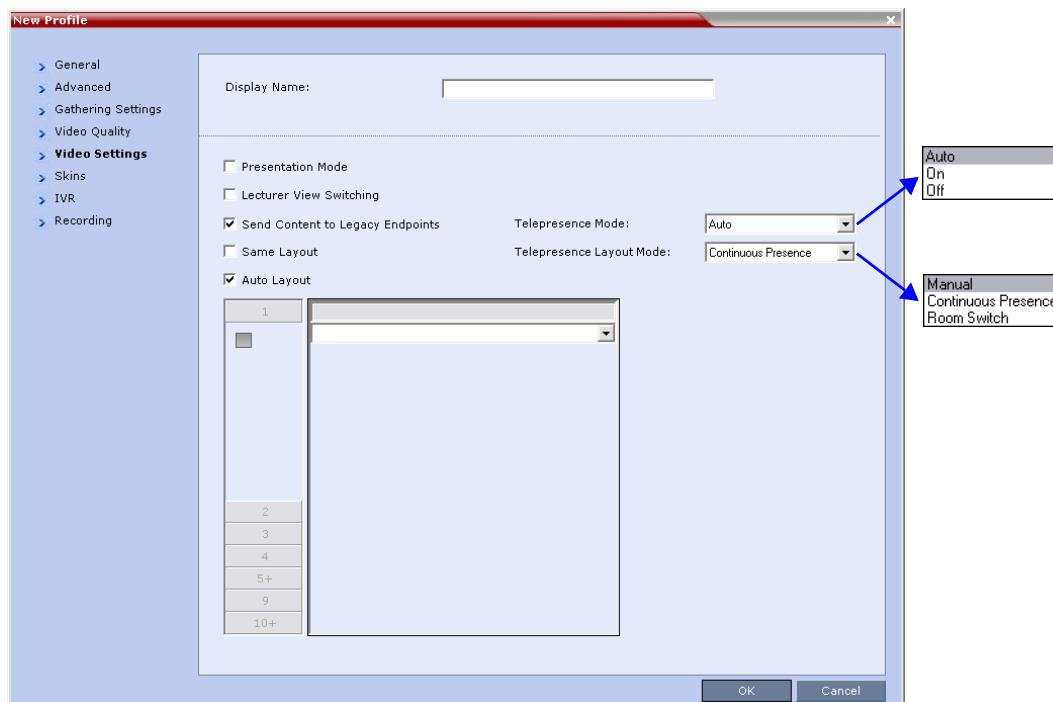
The default settings for Auto Layout of the Recording Link cannot be changed, and the Auto Layout flags do not apply to the Recording Link Auto Layout default settings.

Immersive Telepresence (ITP) Enhancements

Changes to the New Profile Dialog Box

The *New Profile - Video Settings* dialog box has been modified to enable enhanced control of *ITP* features such as:

- Automatic detection of *ITP* sites.
- Retrieval of *Telepresence Layout Mode*.
- *Layout* control.



The *Telepresence Mode* and *Telepresence Layout Mode* fields are only displayed if the *RMX* has a *Telepresence* license installed.

Automatic detection of Immersive Telepresence (ITP) Sites

A *Telepresence Mode* drop-down menu replaces the previous check box in the *New Profile - Video Settings* dialog box containing the following options:

- Off
- Auto (Default)
- On

ITP endpoints are automatically detected. If *ITP* endpoints are detected, *ITP* features are applied and the *RMX* sends conference video with the following options disabled:

- Borders
- Site names
- Speaker indication
- Skins
- Same Layout

- Presentation Mode
- Auto Layout
- Lecture Mode

Table 16 summarizes the *Telepresence Mode* options.

Table 16 *Telepresence Mode Options*

Telepresence Mode	Description
OFF	When OFF is selected, normal conference video is sent by the RMX.
AUTO (Default)	When AUTO is selected and any ITP endpoints are detected, ITP features are applied to the conference video for all participants. When AUTO is selected, the ITP features are dynamic. If all ITP endpoints disconnect from the conference, normal conference video is resumed for all participants. ITP features are resumed for all participants should an ITP endpoint re-connects to the conference.
ON	ITP features are applied to the conference video for all participants regardless of whether there are <i>ITP</i> endpoints connected or not.

Retrieving the Telepresence Layout Mode

A new field, *Telepresence Layout Mode*, has been added to the *New Profile – Video Settings* dialog box, enabling *VNOC* operators and *Polycom Multi Layout Applications* to retrieve *Telepresence Layout Mode* information from the RMX.

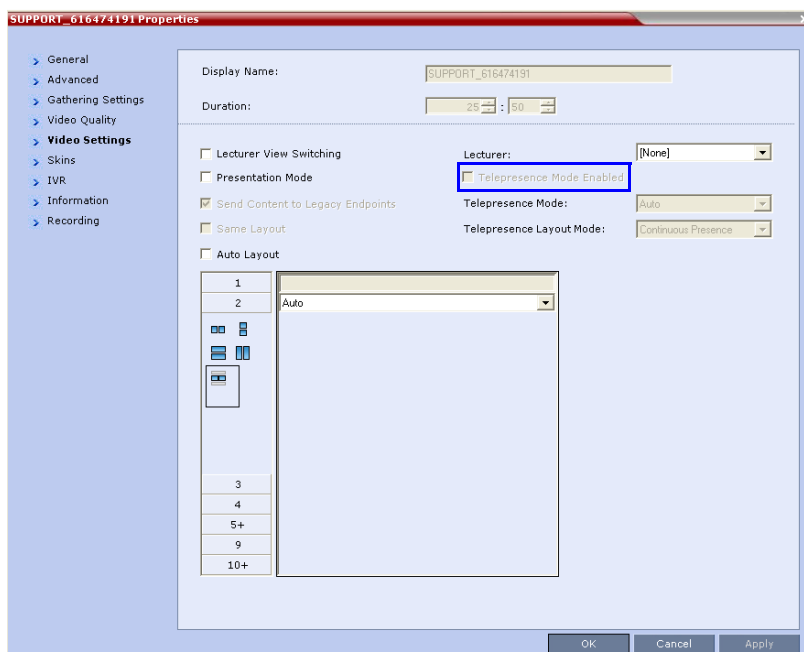
The following modes can be selected:

- *Manual*
- *Continuous presence* - Room Continuous Presence (Default)
- *Room Switch* - Voice Activated Room Switching

Monitoring Telepresence Mode

Monitoring Ongoing Conferences

A additional status indicator, *Telepresence Mode Enabled*, is displayed in the *Conference Properties - Video Settings* tab when monitoring ongoing conferences.

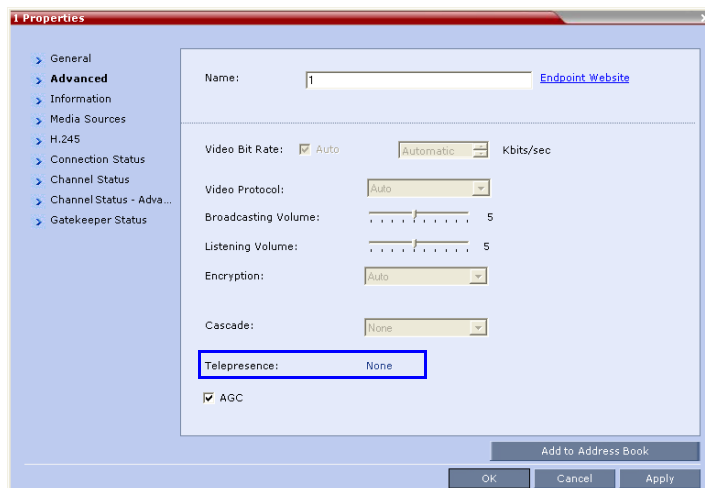


The *Telepresence Mode Enabled*, *Telepresence Mode* and *Telepresence Layout Mode* fields are only displayed if the RMX has a Telepresence license installed.

If *Telepresence Mode* is enabled, a check mark is displayed in the check box. The field description and the check box are grayed as this a status indicator and cannot be used to enable or disable *Telepresence Mode*.

Monitoring Participant Properties

A additional status indicator, *Telepresence*, is displayed in the *Participant Properties - Advanced* tab when monitoring conference participants.



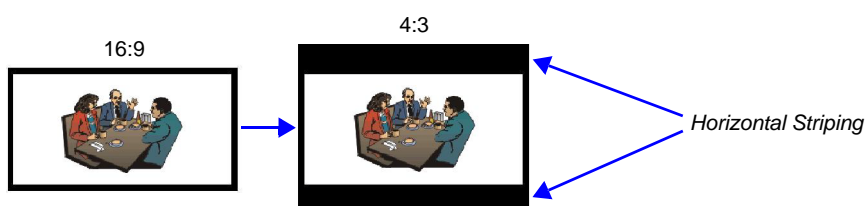
The *Telepresence* mode of the participant is indicated:

- *RPX* - the participant's endpoint is transmitting 4:3 video format.
- *TPX* - the participant's endpoint is transmitting 16:9 video format.
- *None*.

Striping Options

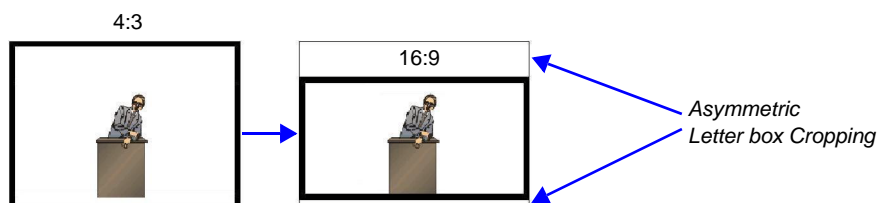
Horizontal Striping

Horizontal Striping is used by the RMX in order to prevent cropping and preserve the aspect ratio of video for all *Telepresence Modes*.



Asymmetric Letter box Cropping

Asymmetric Letter box Cropping is used by the RMX in order to preserve the aspect ratio of video for all *Telepresence Modes*.



Gathering Phase with ITP Room Systems

When a conference is configured to include a *Gathering Phase*, only one endpoint name is displayed for the *ITP* room in the connected participant list of the *Gathering* slide. The *ITP* room endpoint with the suffix "1" in its name receives the *Gathering* slide.

All layouts available to all participants

In previous versions, additional layouts were available only to *TPX* endpoints. In this version all layouts are available to all endpoints on both conference layout and *Personal Layout* levels.

Aspect ratio for standard endpoints

Standard endpoints (non-*ITP*) receive video from the RMX with the same aspect ratio as that which they transmitted to the RMX.

Video Fade is enabled for all Telepresence conferences

Video Fade, disabled for *Telepresence* conferences in previous versions, is enabled for all *Telepresence* conferences.

Setting the RMX as a Voice Gateway in Microsoft OCS R2 2007 Environment

The RMX can be configured as a Voice Gateway in the OCS environment, enabling dialing in to meeting rooms using numbers instead of or in addition to SIP URI addresses which are long strings.

In such configuration, HDX or MOC users dial a number rather than a full SIP URI, simplifying the dialing, which is especially beneficial with the HDX remote control.

Such configuration also enables a common dialing plan for meeting rooms across OCS and H.323 infrastructures. In an integrated environment that also includes Microsoft Exchange Server and Polycom Conferencing Add-in for Microsoft Outlook, a single number can be inserted into a calendar invitation and it will be valid for OC client endpoints and H323 endpoints.

This dialog method can be configured in parallel to the matching URI dialing method (using Static Routes).

Setting the Numerical Dialing into RMX Meeting Rooms

The following processes are required to set up the numerical dialing into RMX Meeting Rooms in the OCS infrastructure:

OCS side:

- Configuring the RMX as a Routable Gateway - The RMX (or DMA) must be set as a trusted voice gateway in the OCS infrastructure. This does not restrict RMX to just voice operation, rather it means that the RMX (or DMA) can be set as a destination for a voice route using the OCS management console. Setting the RMX as a trusted voice gateway also enables it to be used as a trusted gateway for static routes using URI matching.
- Establishing a Voice Route to the RMX "Voice" Gateway - The Voice Route to the RMX (or DMA) must be configured in the OCS infrastructure.



If the RMX was previously defined as a Trusted Host for matching URI dialing method, this definition must be removed before configuring the RMX as a voice gateway. It will be defined as trusted host as part of the voice gateway configuration. For more details, see "Optional. Removing the RMX from the Host Authorization List".

- Configure Office Communicator Users for Enterprise Voice.

RMX side:

The following tasks are detailed in *RMX 2000/4000 Administrator's Guide*, "Configuring the RMX 2000/4000 for Microsoft OCS 2007 Integration" on page [H-24](#).

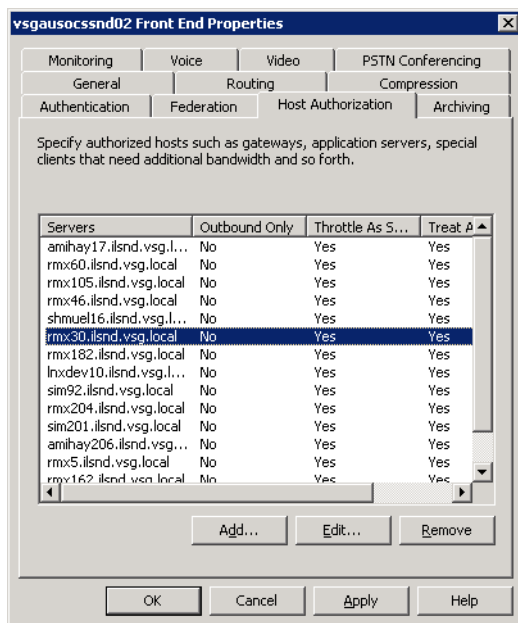
- 9 Modify the Management Network Service to include the DNS server and set the Transport Type to TLS.
- 10 Create the security certificate (using one of the two available methods)
- 11 Define a SIP Network Service in the RMX and install the TLS certificate.
- 12 Modify and add the required system flags in the RMX System Configuration.
- 13 **Optional.** Defining additional Entry Queues and Meeting Rooms in the RMX environment. For details see the *RMX 2000/4000 Administrator's Guide*.

Optional. Removing the RMX from the Host Authorization List

If you have defined the RMX as Trusted Host to enable dialing using the Static Routes and you want to use numerical dialing in addition or instead of SIP URI dialing, you need to remove the current definition of the RMX and redefine it as a voice gateway.

To remove the definition of the RMX as trusted host from the Front End Properties:

- 1 In the OCS application, display the *Front End Properties* (right-click the Front End and select Properties).
- 2 Click the **Host Authorization** tab.
- 3 In the *Trusted Hosts* list, click the RMX entry and then click the **Remove** button.



- 4 Click **OK**.

Configuring the RMX as a Routable Gateway

The RMX must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the RMX to just voice operation, rather it means that the RMX can be set as a destination for a voice route in the Office Communications Server infrastructure.

The Office Communications Server infrastructure uses the WMI class `MSFT_SIPTrustedAddInServiceSetting` to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers, but in this case, the RMX is set as a voice gateway by creating a new instance of the class `MSFT_SIPTrustedAddInServiceSetting`.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to accomplish this.

To set up the RMX/DMA as a Voice Gateway:

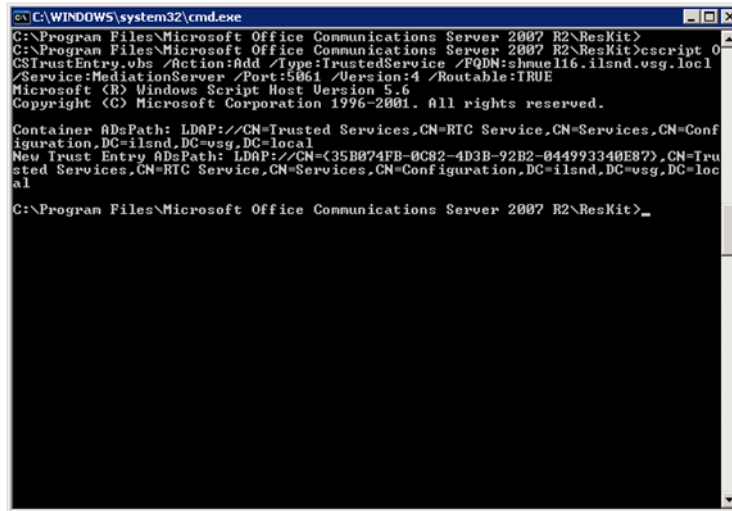
- 1 Download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:
<http://www.microsoft.com/downloads/details.aspx?familyid=9E79A236-C0DF-4A72-ABA6-9A9602A93ED0&displaylang=en>

- 2 Open a command prompt and navigate to where you installed the resource kit. For example, C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\.

- 3 Run the following command:

```
cscript OCSTrustEntry.vbs /action:add /type:trustedservice/  
fqdn:<your FQDN> /service:MediationServer /port:5061/  
version:4 /routable:TRUE
```

Where <your FQDN> is the FQDN of your RMX system. The script automatically generates the GUID discover the proper Active Directory container to store the object.



```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit>
C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit>cscript OCSTrustEntry.vbs /action:add /type:TrustedService /fqdn:shmael16.ilsnd.vsg.local /service:MediationServer /port:5061 /version:4 /routable:TRUE
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Container ADSPath: LDAP://CN=Trusted Services,CN=RTC Service,CN=Services,CN=Configuration,DC=ilsnd,DC=vsg,DC=local
New Trust Entry ADSPath: LDAP://CN={35B074FB-0C82-4D3B-92B2-044993340E87},CN=Trusted Services,CN=RTC Service,CN=Services,CN=Configuration,DC=ilsnd,DC=vsg,DC=local

C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit>_
```

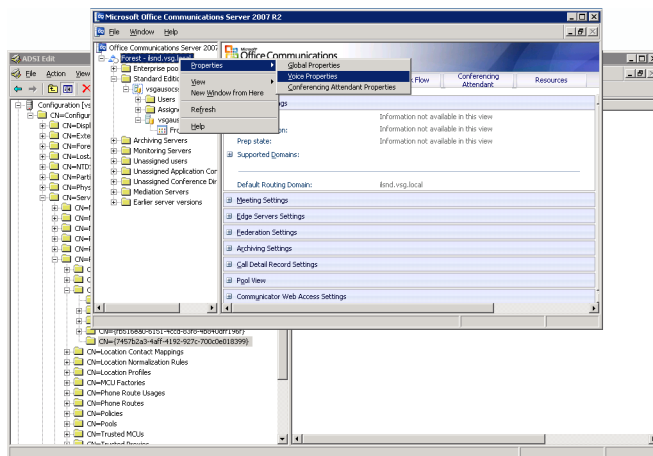
Your RMX system is now established as a trusted gateway by all Office Communications Server pools in the domain. It appears in the list of voice gateways when you establish a voice route.

Establishing a Voice Route to the RMX “Voice” Gateway

The OCS infrastructure enables you to establish a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers which match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers which start with “11” will be routed to RMX11 (DNS name rmx11.r13.vsg.local2).

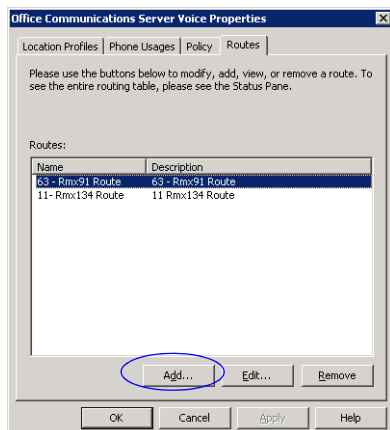
To establish the voice route:

- 1 Open the OCS R2 management Console and right click on **Forest** and then click **Properties > Voice Properties**.



The *Office Communications Server Voice Properties* dialog box opens.

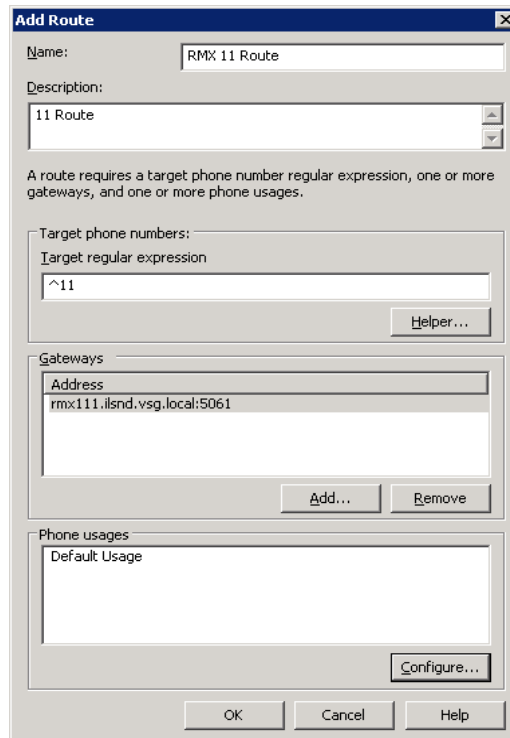
- 2 Click the **Routes** tab.
- Office Communications Server Voice Properties - Routes* dialog box opens.
- 3 Click the **Add** button.



The *Add Route* dialog box opens.

- 4 In the *Name* field, enter a name that will identify this voice route.
- 5 Optional. In the *Description* field, enter a description.

- 6 In the *Target Regular Expression* field enter ^ and the MCU prefix as defined in the gatekeeper. This prefix is also defined in the *RMX IP Network Service*.



Add Route

Name: RMX 11 Route

Description: 11 Route

A route requires a target phone number regular expression, one or more gateways, and one or more phone usages.

Target phone numbers:
Target regular expression: ^11

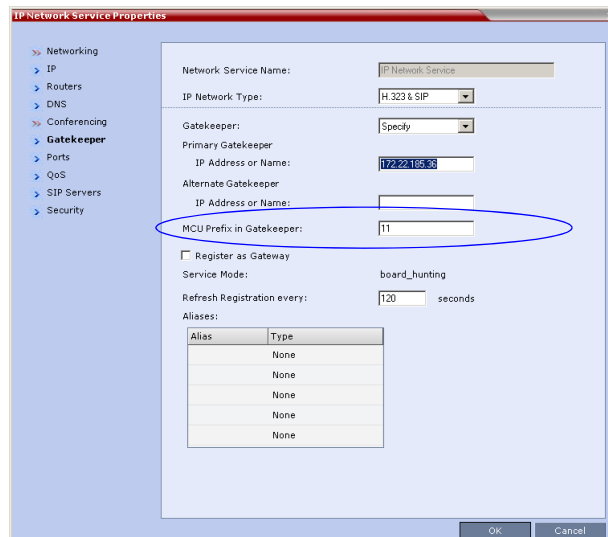
Gateways:
Address: rmx111.ilsnd.vsg.local:5061

Phone usages:
Default Usage

Buttons: OK, Cancel, Help

For example, if 11 is the RMX prefix defined in gatekeeper, enter ^11. The circumflex expression "^11" causes this route to be applied to all numbers starting with "11".

If you have not defined such a prefix in the IP Network Service in the RMX configuration, you can add it later, using value entered here.



IP Network Service Properties

Networking > IP > Routers > DNS > Conferencing > **Gatekeeper** > Ports > QoS > SIP Servers > Security

Network Service Name: IP Network Service

IP Network Type: H.323 & SIP

Gatekeeper: Specify

Primary Gatekeeper:
IP Address or Name: 172.22.105.89

Alternate Gatekeeper:
IP Address or Name:

MCU Prefix in Gatekeeper: 11

☐ Register as Gateway

Service Mode: board_hunting

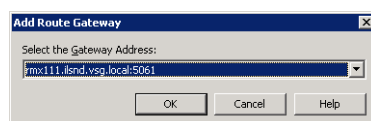
Refresh Registration every: 120 seconds

Aliases:

Alias	Type
	None
	None
	None
	None
	None

Buttons: OK, Cancel

- 7 In the *Gateways - Addresses* box, click the **Add** button. The *Add Route Gateway* dialog box opens.



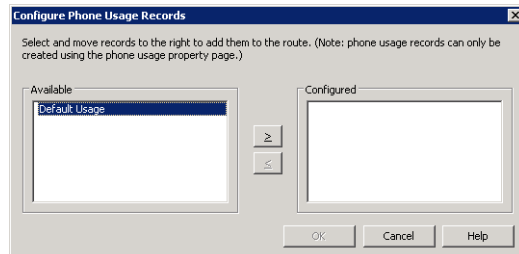
Add Route Gateway

Select the Gateway Address:

rmx111.ilsnd.vsg.local:5061

Buttons: OK, Cancel, Help

- 8 Select the RMX gateway address that was set up in “Configuring the RMX as a Routable Gateway” in step 14 that appears in the drop down list of gateways.
- 9 Click **OK** to save the address and return to the *Add Route* dialog box.
- 10 In the *Phone Usage* box, click the **Configure** button.
The *Configure Phone Usage Records* dialog box opens.
- 11 In the *Available* box, click **Default Usage** and then click the > button.



The *Default Usage* option appears in the *Configured* box.

- 12 Click **OK**.
- 13 In the *Add Route* dialog box, click **OK** to save the new route.

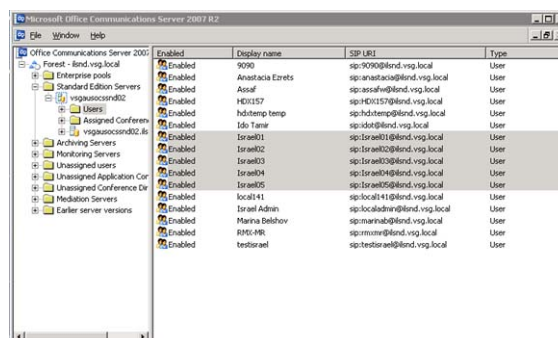
Configuring Office Communicator Users for Enterprise Voice

Each of the endpoints in the OCS environment must be set to use the voice route.

The setting is done in the Office Communications Server management console for all required users (endpoints) simultaneously or in the Active Directory for each of the Users (endpoints).

To Configure Office Communicator Users for Enterprise Voice in the Office Communications Server management console:

- 1 Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.
- 2 Expand the Enterprise pool or Standard Edition server node where your users reside.
- 3 Expand the pool or server where your users reside, and then click the **Users** node.
- 4 In the right pane, right-click one or more users whom you want to configure, and then select **Configure users**.



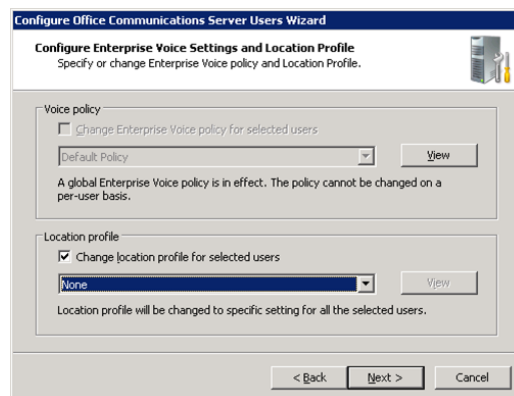
The *Welcome to the Configure Users Wizard* opens.

- 5 On the *Welcome to the Configure Users Wizard* dialog box, click **Next**.
- 6 On the *Configure User Settings* dialog box, click **Next**.
- 7 On the *Configure Meeting Settings* dialog box, click **Next**.

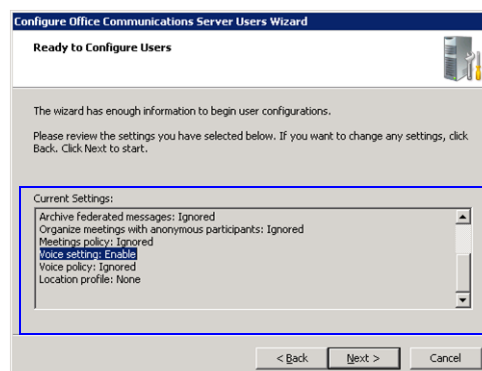
- 8 On the *Configure User Settings specify meeting policy* dialog box, click **Next**.
- 9 On the *Configure Enterprise Voice* dialog box, select **Change Enterprise Voice Settings for selected users**, and then click **Enable Enterprise Voice**. Click **Next**.



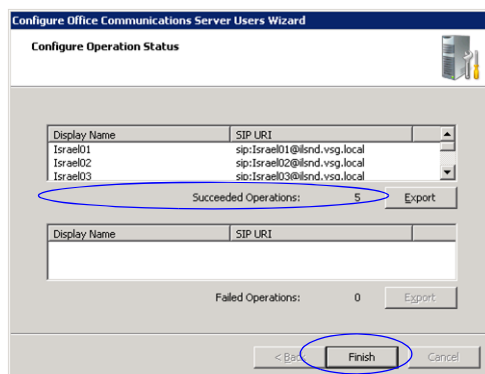
- 10 On the *Configure Enterprise Voice Settings and Location Profile* dialog box, select **Change Enterprise Voice Policy for selected users**.
- 11 Select an Enterprise Voice policy from the list.



- 12 Select **Change location profile** for selected users.
- 13 Select a location profile from the list, and then click **Next**.
- 14 On the *Ready to Configure Users* dialog box, review the settings, and then click **Next**.

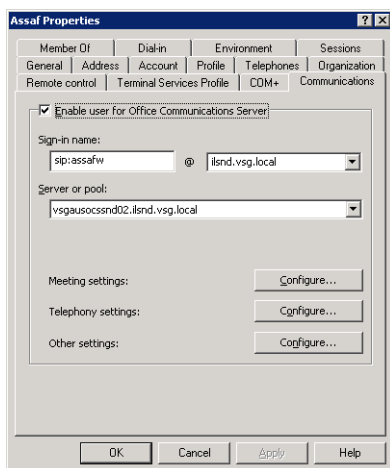


- 15 On the *Configure Operation Status* dialog box, verify that the operation succeeded, and then click **Finish**.



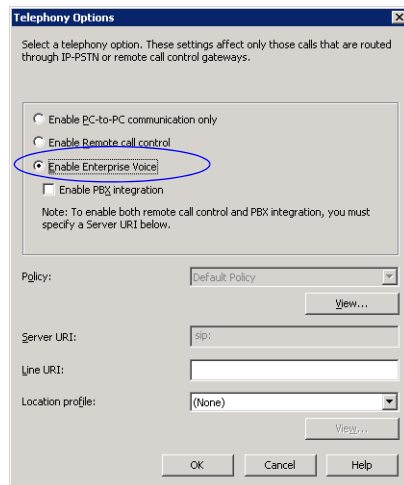
To Configure Office Communicator Users for Enterprise Voice in the in the Active Directory:

- 1 Open the *Active Directory* and navigate to the endpoint whose properties require changing.
- 2 Right-click the endpoint and select **Properties**.
The *Properties* dialog box opens.
- 3 Click the **Communications** tab.



- 4 Click the **Telephony Settings - Configure** button.
The *Telephony Options* dialog box opens.

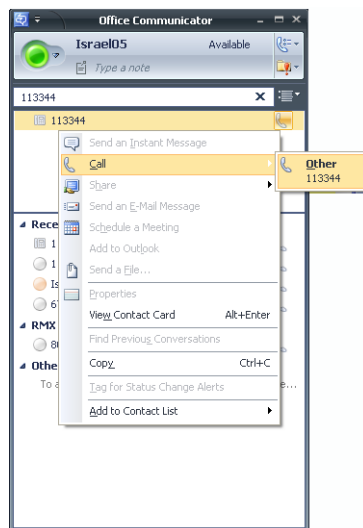
- 5 Select the **Enable Enterprise Voice** option.



- 6 Click **OK** to return to the *Properties - Communications* dialog box.
- 7 Click **OK**.

Starting a Conferencing Call from the MOC

- 1 In the Office Communicator application, enter the number to dial, for example, 113344. This number is composed of the RMX Prefix in the Gatekeeper (for example, 11) and the Meeting Room ID, as defined on the RMX (for example, 3344).



- 2 Click **Call**, and then click **Other**.
The call is routed to the Meeting Room on the RMX, and the caller that initiated the call connects as the conference chairperson.
- 3 The MOC User can then add video to the call, by selecting **Add Video** in the *Office Communicator* window.

Corrections and Known Limitations

Corrections Between Version 5.0 and Version 6.0

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
1	<i>Calendaring</i>	VNGR-13703	No Active Alarm or error message when defining incorrect parameters of the Exchange server on the RMX.	V6.0	
2	<i>CDR</i>	VNGR-11586	Wrong GMT Offset in RMX CDR file. It does not include the minutes.	V4.0.1	
3	<i>CDR</i>	VNGR-11691	Wrong GMT Offset in RMX CDR file. It does not include the minutes.	V4.0.1	
4	<i>Content</i>	VNGR-12225	In a conference running at a line rate of 768 Kbps with HDX endpoints connected and Content that is set to Graphics is sent or VSX endpoint connects the line rate decrease to 512 Kbps and does not increase back to 768 Kbps when Content is halted or the VSX endpoint disconnects.	V5.0.0	
5	<i>Content</i>	VNGR-12342	When adding two or more Legacy endpoints to an ongoing conference, ViewStation endpoints do not revert back to Conference Layout after content sharing is halted.	V4.1	
6	<i>Content</i>	VNGR-13465	An assert occurs when sending Content from a VSX 3000 endpoint to a conference that includes a recording link and MOC (SIP URI), HDX SIP, VSX 3000 H323 are connecting to it.	V6.0	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
7	Content	VNGR-14791	Artifacts can be seen around the layout lines and site names when endpoints (HDX 8000,HDX 9004,HDX 4000.CMAD,PSTN) connect to a conference running on an RMX in MPM mode, at a line rate of 512 Kbps and Content is sent to all endpoints.	V6.0	
8	Encryption	VNGR-12212	FX ISDN endpoints cannot connect to encrypted conferences.	V5.0.0	
9	Gateway	VNGR-12018	When an endpoint connects through MGC Gateway, the layout is automatically defined as 1x1 'Personal' layout instead of applying the conference layout.	V5.0.0	
10	General	VNGR-10100	When the RMX is set to Flexible Allocation Mode and more than 14 endpoints are connected to a single MPM+80 card in line rates above 2Mbps, video artifacts may appear.	V4.0.1	Change the resource Allocation Mode to Fixed Mode.
11	General	VNGR-10341	When the "\$" sign is included in the User password logged into RMX Ver 3.0 or 4.0, access to Hardware Monitor is denied and an error message is displayed.	V4.0.0	
12	General	VNGR-10366	After deleting an ISDN/ PSTN Network Service, text that appears in the message alert is inconsistent.	V4.1	
13	General	VNGR-10884	When the Resource Capacity Mode is set to Flexible and the Port Configuration slider is moved, an incorrect message displays, requesting that the RMX be reset.	V4.1	Ignore the message.

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
14	General	VNGR-11970	A Power OFF error message appears on the MPM+ cards on an RMX that has been running 20 conferences at a line rate of 1472 Kbps with four HD720p dial-in participants in each conference when terminating all the conferences after 90 minutes and restarting them immediately.	V5.0.0	
15	General	VNGR-12241	Sometimes, after 8 hours or more of conferencing at line rates of 4Mbps in a highly loaded MCU, the video processing unit fails.	V5.0.0	
16	Hardware	VNGR-12059	After upgrading to build version 5.0.0.21, the temperature on the card reached Major and required attention.	V5.0.0	
17	Interoperability	VNGR-10880	VSX6000/VSX3000 endpoints receive incorrect protocol and format in a encrypted conference with LPR enabled.	V4.0.1	
18	Interoperability	VNGR-11412	In a CP Conference with the Video Quality set to Sharpness, VSX6000 and V500 H.323 endpoints encounter video stills.	V4.1	
19	Interoperability	VNGR-11508	When endpoints connect to a conference running on the RMX through the DMA, the endpoints will see full screen (1x1) layout and not the conference layout.	V4.1	
20	Interoperability	VNGR-11753	Picture is horizontally stretched on the ISDN endpoint behind Codian ISDN Gateway, despite changing video display settings on the endpoint.	V4.1	
21	Interoperability	VNGR-11854	When Ipower v6.2.0.1208 connects to RMX V.4.1 with Siren 14 or G722.1, the audio is garbled / chopped.	V4.0.1	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
22	Interoperability	VNGR-11881	Garbled audio is heard or audio is muted altogether when dialing from PVX to other endpoints via RMX version 4.1.	V4.1	
23	Interoperability	VNGR-11882	A PVX endpoint sometimes cannot receive H.239 content from an RMX 2000.	V5.0.0	
24	Interoperability	VNGR-11959	When the RMX is used as a gateway to route audio calls to the DMA that run conferences on RMX with a version earlier than 4.1.1, the audio endpoints fail to connect to these conferences.	V4.1.1	Use RMX version 4.1.1 or later.
25	Interoperability	VNGR-11962	A loud buzzing noise occurs when a Tandberg MXP endpoint connects to a conference using ISDN with AES encryption set to Auto.	V5.0.0	
26	Interoperability	VNGR-12069	In a conference running at a line rate of 1920Kbps, with LPR and AES enabled, H.320 Tandberg MXP dial-in participants cannot connect and an assert appears.	V5.0.0	
27	Interoperability	VNGR-9928	When sending content from CMAD in a 384Kbps call, changes in the video image are observed.	V3.0.0	
28	IP	VNGR-12255	Occasionally, problems are encountered with the Gatekeeper and memory. The process recovers seamlessly without effecting the overall experience.	V5.0.0	
29	ISDN	VNGR-11392	No Voice Activated Switching when an ISDN Video participant is connected to a conference running on RMX version 4.0.	V4.0.0	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
30	ISDN	VNGR-11672	Sony PCS-1600s endpoint cannot connect using ISDN lines.	V4.1	Set the flag ISDN_LEGACY_EP_CLOSE_CONTENT_FORCE_H263 to Yes
31	IVR	VNGR-10824	In a SIP CP conference with a line rate of 2 Mb, HDX 8006 endpoints cannot view the IVR slide.	V4.1	
32	IVR	VNGR-11773	On rare occasions, the IVR audio message may be played at a higher speed than normal.	V4.1.1	
33	IVR	VNGR-12021	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	
34	IVR	VNGR-9191	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	
35	IVR-RMX 4000	VNGR-12283	On the RMX 4000, when dialing from ISDN endpoint to GW, the IVR Welcome message is cut off.	V5.0.0	
36	IVR-RMX 4000	VNGR-12508	When an endpoint connects to a Meeting Room on the RMX4000, the RMX2000 Welcome slide is displayed.	V5.0.0	
37	LPR	VNGR-11020	Reduced video quality may be observed when using LPR with HD720p. When packet loss is detected by the LPR mechanism, the LPR lowers the call bit rate to keep the video quality of the call. When excessive packet loss exists, the call rate may drop down to 128K, using HD 720p under these conditions will result in a reduced video image quality.	V4.1	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
38	Multilingual	VNGR-12096	After selecting French or Japanese and logging out of the Web Client, when repeating the Log-in/out process the UI appears in English.	V5.0.0	
39	Multilingual	VNGR-12425	After creating a new gateway, using the Japanese RMX Web Client, the pop-up message has the wrong description.	V5.0.0	
40	Multilingual	VNGR-12426	In the Japanese RMX Web Client, the New Profile > Advanced tab several field names are not translated.	V5.0.0	
41	Multilingual	VNGR-12427	In the New Reservation dialog box, several translations are missing in Japanese.	V5.0.0	
42	Multilingual	VNGR-12453	After deleting a conference, a confirmations message appears in English instead of Japanese.	V5.0.0	
43	Recording	VNGR-11664	Recording links on RMX 4.0 do not support AES encryption, although the RSS v4.0 and above have an AES encryption option.	V4.0.2	
44	Reservations	VNGR-11635	When the duration of an ongoing conference with an ISDN dial in number is set to one minute and auto-extend is enabled, the RMX may not detect a conflict in ISDN dial-in number when placing a reservation on the RMX with an identical ISDN number. In case of a dial-in number conflict, incoming calls are routed to the ongoing conference and not to the reserved meeting.	V4.1	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
45	<i>RMX 4000</i>	VNGR-12298	When viewing the RTM LAN properties of RMX 4000 in the Hardware Monitor, no data is displayed.	V5.0.0	
46	<i>RMX Manager</i>	VNGR-12195	On Vista Operating Systems, when accessing the RMX Web Client and clicking Install RMX Manager, no installation is implemented.	V5.0.0	
47	<i>RMX Manager</i>	VNGR-14452	When using RMX Manager V5.1 and V6.0 to manage several RMXs and swapping between RMXs, the Gatekeeper Prefix displayed on the main screen is not updated according to the selected RMX.	V5.0.1	
48	<i>SIP</i>	VNGR-11971	When trying to connect SIP participants via an external API application, when the URI and IP address fields are switched (the IP address is left empty and the URI is set to the IP address), the endpoint will disconnect.	V5.0.0	Set the IP address correctly.
49	<i>SIP</i>	VNGR-12017	Occasionally, when a dial-in SIP participant accesses the Entry Queue, the participant connection fails even though the participant entered the correct conference ID.	V5.0.0	
50	<i>Upgrade Process</i>	VNGR-12389	When upgrading the RMX2000 from V4.1 to V5.0.0.23 after the software was uploaded an error message "Version download failed" appears.	V5.0.0	
51	<i>Upgrade Process</i>	VNGR-14404	Loss of Connection to the Management Network and H323 Signaling Ports occurs immediately after upgrading RMX 4000 to version 5.0.1.23.	V5.0.1	

Table 17 Corrections between Version 5.0 and Version 6.0

No	Category	Key	Description	Detected in Version	Workaround
52	Video	VNGR-11257	When connecting a VSX3000 endpoint to a CP conference at a line rate of 4M and video quality set to Sharpness, video quality of the connected participants is affected.	V4.1	
53	Video	VNGR-11541	When the VVX1500 is forced to H.263 in SIP calls, the endpoint cannot receive video from the RMX.	V4.1	Do not force the VVX1500 to H.263.
54	Video	VNGR-11609	Incorrect video aspect ratio in full screen in mixed resolution conference running at a line rate of 384 Kbps and to which	4.1	
55	Video	VNGR-11680	Site names disappear from layout 4x4 or 1+10.	V4.1	
56	Video	VNGR-11697	Several HDX endpoints connected to a conference running on RMX version 4.1 at 1Mb at a lower resolution (4SIF instead of 720p).	V4.1	Disconnect and connect the endpoint.
57	Video	VNGR-12217	In a conference running at line rate of 4Mb and resolution of HD1080p, some HDX endpoints (H.323 & SIP) encounter video problems due to a DSP failure.	V5.0.0	
58	Video	VNGR-13311	When a VSX7000 IP endpoint joins a conference running at a line rate of 384 Kbps set to Sharpness with VSX6000, V500 and VSX7000 IP endpoints connected, the video resolution changes to 4CIF.	V4.1	

Version 6.0 System Limitations

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
1	Audio	VNGR-14578	On an RMX with a license for 800 audio only participants, a disconnection cause always occurs after connecting the 767th participant.	V6.0	
2	Audio	VNGR-14687	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	
3	Audio	VNGR-14858	When the first participant connects to a conference running at a line rate of 384Kbps, the music the single party hears (music on hold) has periodic cuts for 1-2 second.	V6.0	
4	Calendaring	VNGR-13350	When resetting the RMX after defining the Exchange Integration Configuration parameters, a software assert appears in the Faults List.	V6.0	
5	Calendaring	VNGR-13686	On the RMX 4000 in a 1080p H.323 Video Switching conference with a line rate of 6Mb, the IVR welcome screen can freeze on the HDX8006 and HDX 9006 endpoints.	V5.0.0 and V6.0	
6	Calendaring	VNGR-13810	In version 6.0, in the Conference Profiles list, the default Event Mode (COP) profile is not used, and should not be listed.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
7	Calendaring	VNGR-14393	After scheduling a VC2W2 conference with a long subject title, the subject title overlaps the 'REC' sign on the endpoint.	V6.0	
8	Calendaring	VNGR-14670	When a conference set up in Calendaring becomes ongoing, an active alarm appears: "MFA error".	V6.0	
9	Calendaring	VNGR-14709	With VC2W2Calendaring, when the Exchange server is down no active alert appears in RMX Manager, the RMX status appears in normal.	V6.0	
10	Cascading	VNGR-11953	When connecting to a cascaded CP conference with a 768Kpbs line rate and the video quality set to Sharpness, HDX endpoints experience bad video quality.	V5.0.0	
11	CDR	VNGR-11746	GMT Time Offset is written to the unformatted CDR as 0.	V4.1	
12	CDR	VNGR-1569	When the conference termination time is changed, the CDR is not updated.	V1.0.0	
13	CDR	VNGR-3011	The Encryption field is missing from the CDR file.	V1.1.0	
14	CDR	VNGR-9340	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	
15	CMA	VNGR-11543	When creating a conference using the CMA, the Conference Management UI displays the participants as disconnected, even though they are connected.	V4.1	
16	CMA	VNGR-12432	5000 version 4.01.04 ER11 does not support RMX4000 version 5.0x yet. Conference on Demand does not work.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
17	Content	VNGR-11491	In a conference with a line rate of 384Kbps, when H.323 participant connect to the conference using FECC, incorrect data is displayed in the Participant Properties - FECC and Content channels of the RMX Web Client. The information is updated correctly once the participant is fully connected.	V4.1	
18	Content	VNGR-12348	Rarely, when Content is sent from an ISDN HDX 9002 - Release - 2.5.0.6-3955 that is connected at a line rate of 256Kbps other participants cannot view the Content.	V5.0.0	Reset the HDX.
19	Content	VNGR-14420	Content sent by legacy endpoints disappears from layout when Click&View is initiated. Content display resumes when a different layout is selected.	V6.0	
20	Diagnostics	VNGR-14428	Components experiencing failure are not displayed in red, when running Hardware Diagnostic tests on RMX 4000.	V6.0	
21	Encryption	VNGR-11401	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	V4.1	
22	Encryption	VNGR-12202	Rarely, in an encrypted conference, H.323 encrypted dial-in and dial-out participants cannot connect and an assert appears (File:EncryptionKeyServer Manager.cpp).	V5.0.0	
23	Encryption	VNGR-14840	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	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
24	Encryption	VNGR-9568	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	V4.0.0	
25	Gateway	VNGR-10863	When deleting the default Gateway Profile and then displaying the properties of an ISDN/PSTN Network Service, an error message appears.	V4.1	
26	Gateway	VNGR-10999	When dialing from H.323 to ISDN using the Gateway IVR method and the string [Bridge prefix][GW profile], after entering the number of the destination ISDN endpoint, the connection indication on the endpoint screen pops up with each connection update.	V4.1	
27	Gateway	VNGR-14672	When a Gateway call is placed through the RMX 4000 to various HDX8006 endpoints, SIP endpoints connected using G.722.1C while the H.323 endpoints connected using Siren22.	V6.0	
28	General	VNGR-10922	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	
29	General	VNGR-10967	Mute incoming participants function (DTMF*86) is not applied to ISDN participants who dial in directly to the conference.	V4.1	Connect via an Entry Queue, to apply the Mute.

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
30	General	VNGR-11064	When moving several participants using multiple selection from one conference to another conference whose maximum number of participants is exceeded by at least one of the moved participants, this participant cannot connect to the conference but is also disconnected from his/her source conference.	V4.1	
31	General	VNGR-11324	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	
32	General	VNGR-11383	When updating the Profile assigned to a Conference Template, changes are not applied when the conference becomes ongoing.	V4.1	
33	General	VNGR-11422	When the RMX is set to Flexible Allocation Mode and more than 14 endpoints are connected to a single MPM+80 card in line rates above 2Mbps, video artifacts may appear.	V4.1	Change the resource Allocation Mode to Fixed Mode.
34	General	VNGR-11741	RMX Web Client users can drag participants to each other's Operator conferences. When using the menu options to try and move participants to the Operator conference, the behavior is correct and the participants cannot be moved to each other's Operator conferences.	V4.1	
35	General	VNGR-11840	MCMS Version is listed as 0.0.0.0 in the Faults List Description field.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
36	General	VNGR-11883	After software upgrade, it is necessary to close and reopen Internet explorer.	V5.0.0	
37	General	VNGR-11926	Rarely, during a web browser connection, a Microsoft .NET framework message may appear.	V5.0.0	Reopen the Internet Explorer.
38	General	VNGR-11987	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.
39	General	VNGR-12001	Rarely, during a web browser connection, a Microsoft .NET framework message may appear.	V5.0.0	Reopen the Internet Explorer.
40	General	VNGR-12033	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	
41	General	VNGR-12056	The title RMX 2000 appears instead of RMX 4000 in the error message dialog box that opens when trying to export an empty address book.	V5.0.0	
42	General	VNGR-12100	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.
43	General	VNGR-12155	When trying to connect an endpoint after hot swapping an RTM ISDN card the endpoint may not connect and the following disconnection description is displayed: Internal Problem - 65022.	V5.0.0	
44	General	VNGR-12173	Dial-out prefixes are not sortable in the ISDN Services dialog box.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
45	General	VNGR-12235	RMX Menu > Help > About RMX contains no information.	V5.0.0	
46	General	VNGR-12240	Endpoints are disconnected after extended time period (8 hrs +) when all MPM+ resources are used. Error message is displayed: "Unit not responding".	V5.0.0	
47	General	VNGR-12245	In a conference where the participant becomes the chairperson and then switches between a secure or unsecure conference using DTMF (*71/#71) codes, the chairperson hears a cut message.	V5.0.0	
48	General	VNGR-12449	In English and Japanese RMX Web Clients, the "Terminal Viewer" fails to open. When using Administration > Turn On SSH and Administration > Tools > Terminal commands, a message, "Failed to open Terminal Viewer" is displayed.	V5.0.0	Make sure that SSH is turned on.
49	General	VNGR-13962	On RMX 2000, HDX endpoints configured for audio only and SIP attempting to connect to a conference at any line rate with defined dial-in and audio only, receive an incorrect reason for connection termination. Reason for termination is incorrectly reported as being due to gatekeeper problems while the real reason is due to resources deficiency.	V6.0	
50	General	VNGR-13965	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 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
51	General	VNGR-14016	Logger Mode drop-down menu overflows Shelf Management Administration Tool dialog box. The dialog box cannot be resized.	V6.0	
52	General	VNGR-14062	On a fully loaded RMX 4000, endpoint may disconnects with Call Disconnection Cause stated as "MCU internal problem - 11122".	V6.0	
53	General	VNGR-14151	A Shelf Voltage problem is always displayed in the System Alerts pane regardless of the actual status.	V6.0	
54	General	VNGR-14152	Major Active Alarm for Shelf Voltage problem is reported with wrong Card ID. Card ID is reported as 0 instead of 2.	V6.0	
55	General	VNGR-14159	Operator assistance function is blocked when the TelePresence mode is enabled.	V6.0	
56	General	VNGR-14276	When the MCU is in startup mode, the upgrade status bar does not appear.	V6.0	
57	General	VNGR-14465	When the securing / unsecuring the conference using DTMF code *71, the text indication appears twice on screen.	V6.0	
58	General	VNGR-14595	In a CP conference with a 512Kbps line rate, when changing the layout with Click&View, the line rate dropped from 30 fps to 10 fps.	V6.0	
59	General	VNGR-14600	When attempting to retrieve large auditor logs, the following message appears: "Error in retrieving auditor file".	V6.0	
60	General	VNGR-14621	Occasionally, the RMX manager application freezes when connected to 10 RMX's.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
61	General	VNGR-14667	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	
62	General	VNGR-14688	When a conference is deleted in the RMX Manager, conference participants are not deleted in the participants list.	V6.0	
63	General	VNGR-14698	When endpoints disconnect, RMX takes a long time to detect the disconnections. In RMX Manager endpoints appear connected to the meeting room disconnection.	V6.0	
64	General	VNGR-14722	A 128Kbps conference with CP, Auto layout and Sharpness enabled, the conference connects four H.323 endpoints one after the other. After connecting the 4th HDX, the endpoint disconnected.	V6.0	
65	General	VNGR-14725	A 384Kbps conference with CP, Auto layout and Sharpness/Clarity and Gathering enabled, the conference connects a variety of endpoints, LifeSize, Tandberg & HDX9004 show a "Window Shades" pattern during the gathering slide phase.	V6.0	
66	General	VNGR-14767	H.323 party disconnect due to MCU Internal Problem 32212.	V6.0	
67	General	VNGR-3824	The Click & View menu doesn't appear in 64 Kbps calls.	V1.1.0	Use the RMX Web Client.

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
68	General	VNGR-9729	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.
69	General	VNGR-9803	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	
70	H.323	VNGR-11810	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	
71	Hardware	VNGR-9571	In D-type chassis, when hot-swapping an MPM card, unit failure may occur.	V4.0.0	Reset the MCU
72	HD	VNGR-11429	In conference running at a line rate of 1920 Kbps and the Video set to Sharpness & Auto Layout, Aethra X7 H.323 endpoints receive 1024x576 instead of 720p HD.	V4.1	
73	HD	VNGR-3089	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
74	Interoperability	VNGR-10162	An HDX 2.5.0.2-3395 endpoint cannot control a Sony XG80 endpoint using FECC.	V4.0.1	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
75	Interoperability	VNGR-10849	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	(1) Upgrade to HDX software version 2.5.0.5 (2) Use conference line rates below 256 or above 768 Kbps. (3) Disable the IVR Welcome slide and avoid using a 1x1 Video Layout.
76	Interoperability	VNGR-10989	In a ISDN dial-in conference with a line rate of 384 Kbps, Tandberg MXP ISDN endpoints cannot view content.	V4.1	
77	Interoperability	VNGR-11341	During H.320 calls, Lip Sync issues occur when content is being sent.	V4.1	
78	Interoperability	VNGR-11406	In a conference running at a line rate of 1920 Kbps and is set to Auto Layout, Tandberg 1700 and Edge95 MXP H.323 endpoints receive 1024x576 instead of 720p HD format.	V4.1	
79	Interoperability	VNGR-11421	Sony PCS-XG80 endpoints are unable to send H.239 Content in H.323 encrypted calls on the RMX.	V4.1	
80	Interoperability	VNGR-11425	When Tandberg MXP sends Content using H.323, ISDN endpoints cannot view Content.	V4.1	
81	Interoperability	VNGR-11463	In a conference running at a line rate of 128 Kbps that includes Content sent by H.323 endpoint, Lifesize ISDN endpoints cannot view the Content.	V4.1	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
82	Interoperability	VNGR-11464	The RMX does not open the audio channel when connecting a DST K60 endpoint in a conference with a line rate of 384 Kbps.	V4.1	
83	Interoperability	VNGR-11480	Legacy endpoints occasionally cannot switch from 1x1 to 7+1 video layouts when Content is started.	V4.1	
84	Interoperability	VNGR-11489	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	
85	Interoperability	VNGR-11492	Legacy endpoints occasionally cannot switch from 1x1 to 7+1 video layouts when Content is started.	V4.1	
86	Interoperability	VNGR-11512	In a conference running at a line rate of 1920 Kbps, when the RMX dials out to a Sony XG80, the HD video may display fragmentation or artifacts.	V4.1	
87	Interoperability	VNGR-11523	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	
88	Interoperability	VNGR-11563	Legacy endpoints occasionally cannot switch to Content when Content switched from H,264 to H.263.	V4.1	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
89	Interoperability	VNGR-11724	H.239 Content sometimes cannot be seen on PVX endpoint (Version 8.5.0.4) when connected to the RMX, using H.264 protocol. The PVX endpoint is shown as 'connected with problem'.	V4.1	
90	Interoperability	VNGR-11767	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	
91	Interoperability	VNGR-11798	When Tandberg C20 endpoint sends Content, the far end indicates that Content is being received but received Content is black.	V5.0.0	
92	Interoperability	VNGR-11830	Sony XG80 endpoint cannot send Content in H.323 384 Kbps call.	V6.0	
93	Interoperability	VNGR-11920	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	
94	Interoperability	VNGR-11963	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	
95	Interoperability	VNGR-12177	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	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
96	Interoperability	VNGR-12178	In a conference with AES, LPR and Video Clarity enabled, H.320 HDX8006/ HDX9004 endpoints send Content in H.263 only.	V5.0.0	
97	Interoperability	VNGR-12214	Sony PCS-G50 ISDN endpoints cannot view video when connected to encrypted conferences.	V6.0	
98	Interoperability	VNGR-12266	Tandberg MXP endpoint receives ghosted video from HDX9004 endpoint during H.323 conference.	V5.0.0	
99	Interoperability	VNGR-12273	IVR welcome message is not clear on an Ipower v6.2.0.1208 endpoint connecting to RMX with Siren 14 or G722.1	V5.0.0	
100	Interoperability	VNGR-12355	DST K60 endpoint receives tiled video from HDX9004 endpoint during H.323 conference.	V5.0.0	Set the system flag SEND_WIDE_RES_TO_IP to NO to force the system to send 4CIF.
101	Interoperability	VNGR-12369	Tandberg C20 endpoint periodically displays fast updates in HD1080p conferences.	V5.0.0	
102	Interoperability	VNGR-12372	Tandberg 6000 E and B series, H.320 endpoints do not connect to conferences when encryption is enabled.	V5.0.0	
103	Interoperability	VNGR-12373	HDX endpoint connected via H.320 does not receive Content from Tandberg MXP endpoint connected via H.323.	V5.0.0	
104	Interoperability	VNGR-12559	VSX5000 endpoint freezes followed by disconnection of all VSX endpoints.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
105	Interoperability	VNGR-13685	Video display freezes on the HDX9006 endpoint when connected to a Video Switching conference running on the RMX 4000 at a line rate of 6Mb and a resolution of 1080p via H.323 connection.	V5.0.0 and V6.0	
106	Interoperability	VNGR-14047	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	
107	Interoperability	VNGR-14221	PVX endpoint connects partially to conference when Video Quality is set to "Sharpness" and Content Protocol setting is "Up to H.264".	V6.0	
108	Interoperability	VNGR-14779	Sony XG80 SIP endpoint receives but does not transmit video to 720p VSHD conference on RMX 2000 with MPM card(s).	V6.0	
109	Interoperability	VNGR-14780	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	
110	Interoperability	VNGR-3977	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.

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
111	Interoperability	VNGR-4652	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.
112	Interoperability	VNGR-6902	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.
113	Interoperability	VNGR-7597	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
114	Interoperability	VNGR-7598	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
115	Interoperability	VNGR-8605	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	
116	Interoperability	VNGR-9015	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	
117	Interoperability	VNGR-9425	HDX8000 (Release - 2.0.3.1-2729) and VSX3000 (9.0.1-18.07.2008) endpoints connect at a higher line rate than the conference line rate.	V4.0.0	
118	Interoperability	VNGR-9677	When switching Content sending from an HDX9004 to Aethra X7 and back, Content is not received by Aethra X7.	V4.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
119	Interoperability	VNGR-9816	When dialing out to VSX6000A SIP endpoint from a CP conference at line rate of 1920Kbps, it connects as Secondary.	V4.0.0	
120	Interoperability	VNGR-9830	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.
121	Interoperability	VNGR-9909	When dialing out to a Tandberg MXP ISDN endpoint, the IVR slide is not displayed, although the IVR message is played.	V4.0.0	
122	IP	VNGR-12053	When changing the IP configuration mode from IPv4 to or from IPv6 Auto/Manual, the system does not reset.	V5.0.0	
123	IP	VNGR-12288	Static Route malfunctions and returns with an incorrect IP address.	V5.0.0	
124	IP	VNGR-14109	When the RMX Card Configuration Mode is changed from MPM+ to MPM, IPv6 is still selected in the IP Network Services, although it is not supported in the MPM mode.	V6.0	
125	IP	VNGR-14111	IPv6 can be set in the IP Network Services in RMX configured to MPM Card Configuration Mode although IPv6 is not supported in this Card Configuration Mode.	V6.0	
126	IP	VNGR-14376	SSH cannot be activated when IPv6 is selected. Login via Putty or wincp is not possible.	V6.0	
127	IP	VNGR-14705	14 H.323 HDX endpoints are connected and disconnected from the conference, some of the reconnecting endpoints do not reconnect.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
128	IP	VNGR-7734	Static Routes table in IP Network Service does not function.	V3.0.0	
129	ISDN	VNGR-11872	The following assert occurs when encrypted ISDN endpoints connected with a "Connected with Problem" status. Segment.cpp, Line:650, Code:127.; ASSERT:"	V5.0.0	
130	ISDN	VNGR-11908	ISDN endpoints do not display the IVR slide.	V5.0.0	
131	ISDN	VNGR-12007	Occasionally, when ISDN participants connect to a conference with line rate 384kbs, multiple asserts appear in the log file.	V5.0.0	
132	ISDN	VNGR-12011	Occasionally, an ISDN participant fails to connect to the conference due to the following error - "MCU internal problem - 50020".	V5.0.0	
133	ISDN	VNGR-12034	In a conference running at a line rate of 384 Kbps, H.320 encrypted participant cannot connect and an assert appears.	V5.0.0	
134	ISDN	VNGR-12370	Removing the main or backup PRI clock source causes disconnection of all connected IP and ISDN participants.	V5.0.0	
135	ISDN	VNGR-14133	Green artifacts appear on the Welcome IVR slide displayed on ISDN endpoints when connected at 1472kbps.	V6.0	
136	ISDN	VNGR-14263	Tandberg 6000 E and B series endpoints cannot connect in H.320 encrypted conferences.	V6.0	
137	ISDN	VNGR-14374	After sending Content in 2Mb encrypted conference, ISDN Endpoints video freezes.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
138	ISDN	VNGR-14772	ISDN (H.320) endpoints fail to connect to RMX 4000 running conference using 384Kb, LPR, AES, Sharpness, Video Clarity, Auto Layout. In Participant Properties - Connection Status, Call Disconnection Cause is given as "the encryption setup process did not end on time - 0".	V6.0	
139	ISDN	VNGR-4405	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	
140	IVR	VNGR-10054	Customized CIF slide is not displayed on the HDX screen when connecting to a 1080p High Definition Video Switching conference.	V4.0.1	
141	IVR	VNGR-11531	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	
142	IVR	VNGR-11712	The Welcome slide is not displayed when a dial-out SIP endpoint connects at a line rate of 768 Kbps, using H261 video protocol.	V4.1.1	
143	IVR	VNGR-12031	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	
144	IVR	VNGR-12116	When a single participant enters a conference that is running at a line rate of 2Mb, the participant does not hear music.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
145	IVR	VNGR-9809	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	
146	IVR	VNGR-9834	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	
147	IVR-RMX 4000	VNGR-12284	On the RMX 4000, when dialing from ISDN endpoint to GW, video artifacts appear in the IVR slide.	V5.0.0	
148	LPR	VNGR-10104	When an H.323 HDX endpoint sends Content, the endpoint disables the LPR.	V4.0.1	
149	Multilingual	VNGR-14331	Incorrect Japanese translation in RMX manager - "Normal" has two different translations in several locations.	V6.0	
150	Multilingual	VNGR-14332	The stop monitoring option (in right click on MCU) in the RMX manager is not translated to Japanese. VNGBE-851	V6.0	
151	Multilingual	VNGR-14333	Translation of the Exchange Integration Configuration dialog box is missing.	V6.0	
152	Multilingual	VNGR-14335	Several fields in the Conference Profile dialog box have not been translated.	V6.0	
153	Multilingual	VNGR-14336	Translations of some of the fields in the New Conference dialog box are missing.	V6.0	
154	Multilingual	VNGR-14338	Translation of the entries Copy Conference and past Conference in the Conference right-click menu is missing.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
155	Multilingual	VNGR-14340	The following alarm is not translated to Japanese: "SIP and ISDN protocol cannot be selected for dial-out in the Gateway Profile because SIP and ISDN Network are not configured".	V6.0	
156	Multilingual	VNGR-14348	SIP calls in both HDX and VSX systems do not connect to their specified line rates. For example; 384kbps connect at 368kbps and 512kbps calls connected at 496kbps.	V6.0	
157	Multilingual	VNGR-14567	Translation of some of the fields in the Upgrade windows and dialog box are missing.	V6.0	
158	Multilingual	VNGR-14800	The translation of the Create Certificate button in the IP Network Service - SIP Server tab is missing.	V6.0	
159	Multilingual	VNGR-5151	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	
160	Multilingual	VNGR-5310	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	
161	Partners - Microsoft	VNGR-13314	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	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
162	<i>Partners - Microsoft</i>	VNGR-14199	When a Microsoft Office Communicator client disconnects from a conference (from the endpoint side) the Disconnection Cause is "Party hung up" instead of "Closed normally".	V6.0	
163	<i>RMX 4000</i>	VNGR-14386	Display information for Slot 5, FSM (Fabric Switch Module), in the RMX 4000 Hardware Monitor is incomplete.	V5.1	
164	<i>RMX Manager</i>	VNGR-13893	When RMX's are located outside a V2IU network, connecting to the RMX Manager is impossible.	V6.0	
165	<i>RMX Manager</i>	VNGR-14175	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	
166	<i>RMX Manager</i>	VNGR-14774	After restart following MCU State: MAJOR, MCU State: MAJOR is still displayed by RMX Manager although Hardware Monitor list all component in Normal state.	V6.0	
167	<i>RMX Manager</i>	VNGR-14808	In the RMX Manager, when right-clicking the empty Conferences pane (no ongoing conferences), the Copy Conference option is enabled although there is no conference to copy.	V6.0	
168	<i>RMX Manager</i>	VNGR-14814	In the RMX Manager application, the MCU State (shown on the right bottom corner of the screen) is not updated when the MCU status changes from Major to Normal.	V6.0	Close and reopen the RMX Manager to update the MCU State.
169	<i>RMX Web Client</i>	VNGR-12172	In the RMX Web Client, the main window opens up as full screen and cannot be resized.	V5.0.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
170	<i>RMX Web Client</i>	VNGR-12176	In the RMX Web Client when viewing the Conference Properties - General, the keyboard Tab button does not move the cursor to the next field.	V5.0.0	Keep pressing the Tab button.
171	<i>RMX Web Client</i>	VNGR-12257	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	
172	<i>RMX Web Client</i>	VNGR-14373	Cropped words: "Participants" in System Information box; "Notification" in Notification Settings dialog box.	V6.0	
173	<i>RMX Web Client</i>	VNGR-14750	Login button is not wide enough to accommodate certain languages. "Install RMX Manager" link is displayed in English.	V6.0	
174	<i>RMX Web Client</i>	VNGR-14778	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	
175	<i>RMX Web Client</i>	VNGR-14809	The option View> Group by MCU does not work in the RMX Web Client (Internet Explorer).	V6.0	Use the RMX Manager application.
176	<i>RMX Web Client</i>	VNGR-14833	On RMXs upgraded to Version 6.0, the "Enable Gathering" check box (Profile > Gathering Settings) is not checked by default in existing Profiles.	V6.0	In the Conference Profiles list, double -click the Profile icon. Select the Profile to be modified and then click Profile Properties > Gathering Settings. Select the Enable Gathering check box.

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
177	<i>RMX Web Client</i>	VNGR-2473	Sometimes when installing the RMX Web Client, Windows Explorer >Internet Options> Security Settings must be set to Medium or less.	V1.1.0	
178	<i>RMX Web Client</i>	VNGR-7557	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.
179	<i>RMX Web Client</i>	VNGR-9829	Occasionally, during an ongoing conference, when selecting the Hardware Monitor menu the message "No connection with Switch" appears.	V4.0.0	
180	<i>Security</i>	VNGR-14603	Cannot open SSH on an RMX system with IPV6 and IPV4 configuration.	V6.0	
181	<i>SIP</i>	VNGR-11923	The maximum number of Meeting Rooms, Entry Queues, SIP Factories and on-going conferences that can be registered to the Proxy, is limited to 100.	V5.0.0	
182	<i>SIP</i>	VNGR-11949	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	
183	<i>SIP</i>	VNGR-12006	With SIP defined and undefined dial-in participants you cannot change the layout type from "conference layout" to "personal layout".	V5.0.0	
184	<i>SIP</i>	VNGR-14266	A Tandberg Edge95 MXP endpoint does not transmit video in SIP calls at line rates above 768kbps.	V6.0	
185	<i>SIP</i>	VNGR-14353	HDX9004 endpoints with ver. 2.6.0-4717 during a SIP call transmits siren22 at 32kbps and receives siren22 at 64kbps.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
186	SIP	VNGR-14385	IPv6 SIP dial out to HDX endpoint fails with disconnection cause "SIP time out".	V6.0	Reset of endpoint results in successful connection.
187	SIP	VNGR-14396	During a SIP CP 4 MB conference, when an Aethra X7 connects, video does not transmits and the IVR Welcome screen remains displayed.	V6.0	
188	SIP	VNGR-14681	When configuring a SIP Server in the Fast Configuration Wizard, and an incorrect Domain Name is set, there is no error notification.	V6.0	
189	SIP	VNGR-3276	SIP participants cannot connect to a conference when the conference name contains blank spaces.	V1.1.0	
190	Software Version	VNGR-8259	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
191	Software Version	VNGR-9228	When trying to restore last version, after upgrading from version 3 to version 4, the RMX prompts for an activation key.	V4.0.0	
192	Unified Communication Solution	VNGR-13729	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 and an error message (assert) is displayed in the RMX Management application.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
193	Upgrade Process	VNGR-14554	The RMX Manager disconnects after updating a software version with a new Activation key. After reconnecting to the RMX Manager, an active alarm appears with message that new version is installed and that the activation key was successfully installed.	V6.0	
194	Upgrade Process	VNGR-14720	After software Upgrade is completed, an Active Alarm "Connection to Exchange Server failed" appears in the Alarms List on the RMX4000.	V6.0	
195	Upgrade Process	VNGR-14764	Cannot create conference until the system is restarted following cancelled upgrade to incorrect version.	V6.0	
196	Upgrade Process	VNGR-14844	The Faults List is empty when upgrading the RMX 2000 from V5.01 build 24 to v6.0 build 86.	V6.0	
197	Upgrade Process	VNGR-9565	When downgrading from version 4.0 to version 3.0, the MPM card does revert to normal.	V4.0.0	
198	Upgrade Process	VNGR-9740	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	Switch the MCU off and then switch it on ("hardware" reset).
199	Video	VNGR-10239	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	
200	Video	VNGR-11123	When the Closed Caption text is very long the text is split and may be displayed incorrectly.	V4.1	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
201	Video	VNGR-11351	When the video from an endpoint is blocked, inconsistent video resolution settings are implemented.	V4.1	
202	Video	VNGR-11382	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	
203	Video	VNGR-11843	In a 2 Mb Video Switched conference with 10 or more H.323 endpoints connected, random video refreshes may occur.	V5.0.0	
204	Video	VNGR-11965	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	
205	Video	VNGR-14124	On rare occasions in 2Mbps ISDN calls, ISDN participants connected without their endpoints sending video for a few seconds.	V6.0	
206	Video	VNGR-14158	In a conference with Classic Skin selected, the site name for CIF participants is displayed as half white and half yellow.	V6.0	
207	Video	VNGR-14516	In a VC2W2 conference with Gathering, when the endpoint connects using CMAD, horizontal colored artifacts are viewed on the gathering slide.	V6.0	
208	Video	VNGR-14628	On the RMX4000 during a 4 Mb CP conference with Sharpness enabled, when connecting 18 HDXs with a 10+ layout, sometimes HDXs display flashing video on the border layout.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
209	Video	VNGR-14673	In a 4MB Immersive Telepresence conference with Sharpness enabled, cracking and popping sounds are heard.	V6.0	
210	Video	VNGR-14694	When Gathering is enabled, the Immersive Telepresence systems are displayed as separate video participants and not as an Immersive Telepresence room/suite.	V6.0	
211	Video	VNGR-14696	When placing a call from the HDX8006 (2.5.0.8) to the other endpoints using ISDN with a Gateway, when selecting Single Layout video freezes.	V6.0	
212	Video	VNGR-14726	A 384Kbps conference with CP, Auto layout, Sharpness and Presentation mode enabled, the conference dials out and connect to H.323 LifeSize and the H.320 HDX endpoints. The HDX endpoint sends content, the LifeSize endpoint views black video.	V6.0	
213	Video	VNGR-14731	A 1920Kbps conference with CP, LPR, Sharpness and Layout is set to 1+5, the conference dials out to SIP Sony and H.323 LifeSize3 endpoints. After some time the video on the Sony monitor (from LifeSize) shows predator (divergence) patterns and colored pixels.	V6.0	
214	Video	VNGR-14738	In a 4MB HD 1080p conference with Encryption, Content, LPR and Sharpness enabled, after connecting to the conference some endpoints viewed pixels and mosaic video.	V6.0	

Table 18 Version 6.0 System Limitations

No.	Category	Key	Description	Detected in Version	Workaround
215	Video	VNGR-14745	On a 4 MB 1080p Video Switching conference with 15 1080p video endpoints, corrupted was video sent from the Tandberg C20 endpoint.	V6.0	
216	Video	VNGR-14787	Video endpoints using the H.264 video protocol may sometimes display video artifacts when connected in a noisy network that is experiencing packet loss.	V6.0	To avoid the problem, set system flag H264_MB_INTRA_REFRESH to YES.
217	Video	VNGR-14837	Gathering slide info is cut off for dial-out VSX and CMAD MAC endpoints that receive video at a resolution of 480x352. The gathering screen displays correctly on the HDX endpoints	V6.0	
218	Video	VNGR-14860	Artifacts are displayed on the HDX (v2.6) screen when connected to a HD Video Switching conference running on RMX 4000 at a line rate of Kbps.	V6.0	