



▶ Polycom RMX™  
1500/2000/4000  
Deployment Guide for  
Maximum Security Environments



### Trademark Information

Polycom®, the Polycom “Triangles” logo, and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

### Patent Information

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



This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 7.6 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

© 2011 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

<b>First Time Installation and Configuration . . . . .</b>	<b>1-1</b>
Workstation Requirements .....	1-1
RMX Hardware .....	1-2
Installation and Configuration .....	1-2
Procedure 1: Hardware Installation and Setup .....	1-3
Rack-Mounting the RMX 1500/2000/4000 .....	1-3
RMX 1500 .....	1-3
RMX 2000 .....	1-5
RMX 4000 .....	1-6
Cabling the RMX 1500/2000/4000 .....	1-7
RMX 1500 Power, Signaling and Media Cables .....	1-7
RMX 2000 Power, Signaling and Media Cables .....	1-8
RMX 4000 AC and DC Power Sources .....	1-9
RMX 4000 Signaling, Media and Management Cables ...	1-12
Procedure 2: Gather Network Equipment and Address Information .....	1-14
IP Services .....	1-14
Management Network .....	1-14
Signaling Network .....	1-14
IP Network Services Required Information .....	1-14
ISDN/PSTN Services .....	1-16
Procedure 3: First Entry Configuration .....	1-17
Product Registration .....	1-17
Obtaining the Activation Key .....	1-17
First-time Power-up and Connection to MCU .....	1-18
Configuring the workstation for direct connection .....	1-18
Connecting to the Default Management Network .....	1-21
Product Activation .....	1-23
Modifying the Signaling Network Service and ISDN/PSTN Network Service Settings .....	1-25
Fast Configuration Wizard .....	1-26
Procedure 4: Enable Ultra Secure Mode .....	1-42
Connecting to the RMX .....	1-43



Procedure 5: Enable Secured Communication .....	1-45
Enabling to Secure Mode .....	1-46
Purchasing a Certificate .....	1-46
Installing the Certificate .....	1-48
Switching to Secure Communication Mode .....	1-49
Procedure 6: Set System Configuration Flags .....	1-51
Modifying Flag Values .....	1-54
Procedure 7: Enable Network Separation (RMX 2000) .....	1-55
Enabling Network Separation .....	1-55
Procedure 8: Configure IVR Settings. ....	1-57
Procedure 9: Optional. Modify Default Login and Main Screen Banner Text .....	1-59
Login Screen Banner .....	1-60
Main Screen Banner .....	1-62
Customizing Login and Main Screen Banners .....	1-62
Procedure 10: Rename the Default POLYCOM User .....	1-64
Procedure 11: Disable Inline AutoComplete Option in Web Browser .....	1-65
Procedure 12: Configure an Inbound and Outbound Access List	1-66
Antivirus .....	1-67
Guidelines .....	1-67
Scheduling .....	1-67
Scan Results .....	1-70
Antivirus Updates .....	1-70
Downloading and Converting the ZIP file to TAR .....	1-71
Active Alarms .....	1-72
Logger File Additions .....	1-72
Integration with Microsoft® Active Directory™ .....	1-73
Internal RMX Database and Active Directory in Ultra Secure Mode .....	1-73
Guidelines .....	1-73
Enabling Active Directory Integration .....	1-74
<b>Basic Operation .....</b>	<b>2-1</b>
Starting the RMX Web Client .....	2-1
RMX 1500/2000/4000 Web Client Screen Components .....	2-4
Viewing and System Functionality Permissions .....	2-5
Conferences List .....	2-6



List Pane .....	2-6
RMX Management .....	2-6
Status Bar .....	2-7
System Alerts .....	2-7
Participant Alerts .....	2-7
Port Usage Gauges .....	2-8
MCU State .....	2-9
Address Book .....	2-10
Displaying and Hiding the Address Book .....	2-11
Conference Templates .....	2-11
Displaying and Hiding Conference Templates .....	2-12
Customizing the Main Screen .....	2-13
Customizing the RMX Management Pane .....	2-14
Starting a Conference .....	2-16
Starting a Conference from the Conferences Pane .....	2-17
General Tab .....	2-18
Participants Tab .....	2-21
Information Tab .....	2-25
Starting a Reservation .....	2-27
Starting an Ongoing Conference From a Template .....	2-29
Connecting to a Conference .....	2-31
Direct Dial-in .....	2-31
H.323 Participants .....	2-32
Entry Queue Access .....	2-33
H.323 Participants .....	2-34
ISDN and PSTN Participants .....	2-34
Dial-out Participants .....	2-34
Text Indication in the Video Layout .....	2-35
Endpoint Names .....	2-35
Text Indication .....	2-37
Transparent Endpoint Names .....	2-38
Monitoring Ongoing Conferences .....	2-39
Operation Selection .....	2-39
Multi Selection .....	2-40
Conference Level Monitoring .....	2-40
Participant Level Monitoring .....	2-43
Participant Connection Monitoring .....	2-43



Operations Performed During On Going Conferences .....	2-47
Conference Level operations .....	2-47
Changing the Duration of a Conference .....	2-47
Adding Participants from the Address Book .....	2-48
Saving an Ongoing Conference as a Template .....	2-49
Copy and Paste Conference .....	2-49
Copy Conference .....	2-49
Paste Conference .....	2-50
Paste Conference As .....	2-51
Changing the Video Layout of a Conference .....	2-52
Video Forcing .....	2-54
Enabling and Disabling Video Clarity™ .....	2-56
Participant Level Operations .....	2-57
Copy Cut and Paste Participant .....	2-60
Copy Participant .....	2-60
Cut Participant .....	2-61
Paste Participant .....	2-61
Paste Participant As .....	2-62
Personal Layout Control with the RMX Web Client .....	2-65
Personal Layout Selection with Click&View .....	2-66
Conference Control Using DTMF Codes .....	2-68
Intrusion Detection .....	2-70
Network Intrusion Detection System (NIDS) .....	2-70
<b>Installing RMX Manager for Secure Communication</b>	
<b>Mode .....</b>	<b>3-1</b>
Using an Internal Certificate Authority .....	3-8
<b>USB Operations .....</b>	<b>4-1</b>
USB Ports on RMX 1500/2000/4000 .....	4-1
Restore to Factory Security Defaults .....	4-3
Comprehensive Restore to Factory Defaults .....	4-4
Comprehensive Restore to Factory Defaults Procedure .....	4-4
Procedure A: Backup Configuration Files .....	4-5
Procedure B: Restore to Factory Defaults .....	4-6
Procedure C: Restore the System Configuration	
From the Backup .....	4-12
Emergency CRL (Certificate Revocation List) Update .....	4-13
Emergency CRL Update Procedure .....	4-13



## **Deploying a Polycom RMX™ Serial Gateway S4GW . . . 5-1**

Guidelines .....	5-2
Configuring the RMX - Serial Gateway Connection .....	5-3
Procedure 1: Initial Setup of the Serial Gateway .....	5-3
Procedure 2: Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX .....	5-11
Testing .....	5-14
Dialing to the RMX from an ISDN Endpoint .....	5-14
Dialing to an ISDN Endpoint from the RMX .....	5-14
Advanced Commands .....	5-16







---

# First Time Installation and Configuration

## Workstation Requirements

The *RMX Web Client* and *RMX Manager* applications can be installed in an environment that meets the following requirements:

- **Minimum Hardware** – Intel® Pentium® III, 1 GHz or higher, 1024 MB RAM, 500 MB free disk space.
- **Workstation Operating System** – Microsoft® Windows® XP, Vista®.
- **Network Card** – 10/100 Mbps.
- **Web Browser** – Microsoft® Internet Explorer® Version 6 or higher.
- **FIPS** – Is always enabled in *Ultra Secure Mode*, and when *ClickOnce* is used to install RMX Manager, the workstation must have one of the following installed:
  - .NET Framework 3.5 or a later version of the .NET Framework.
  - .NET Framework 2.0 plus *Service Pack 1* or later.



.Net Framework 2.0 is required and installed automatically.

The RMX must be installed on the intranet or added to the trusted sites list. In both cases, the *ActiveX* control will install properly.



## RMX Hardware

*Version 7.5.0.J* requires that *MPM+* or *MPMx* be installed in the RMX.

## Installation and Configuration

First Time Installation and Configuration of the RMX 1500/2000/4000 consists of the following procedures:

- 1 Hardware Installation and Setup**
  - Mount the RMX in a rack.
  - Connect the necessary cables.
- 2 Gather Network Equipment and Address Information**
  - Get the information needed for integrating the RMX into the local (Signaling and Management) networks.
- 3 First Entry Configuration**
  - Register the RMX.
  - Power up the RMX.
  - Modify the *Default Management Network*.
  - Configure the *Signaling Network Service*.
  - Configure the *ISDN/PSTN Network Service*.
- 4 Enable Ultra Secure Mode**
- 5 Enable Secured Communication**
  - Purchase and Install the SSL/TLS certificate
  - Modify the *Management Network* settings
  - Create/Modify the relevant *System Flags*
- 6 Set System Configuration Flags**
- 7 Enable Network Separation (RMX 2000)**
- 8 Configure IVR Settings**
- 9 Modify Default Login Banner Text (if required)**
- 10 Rename the default POLYCOM user**
- 11 Disable Inline AutoComplete Option in Web Browser**
- 12 Configure an Inbound and Outbound Access List**



## Procedure 1: Hardware Installation and Setup

The RMX unit should be mounted in a 19" rack in a well ventilated area. It is important to adhere to the "Site Requirements" as described in each of the RMX 1500/2000/4000 Hardware Guides.

### Rack-Mounting the RMX 1500/2000/4000

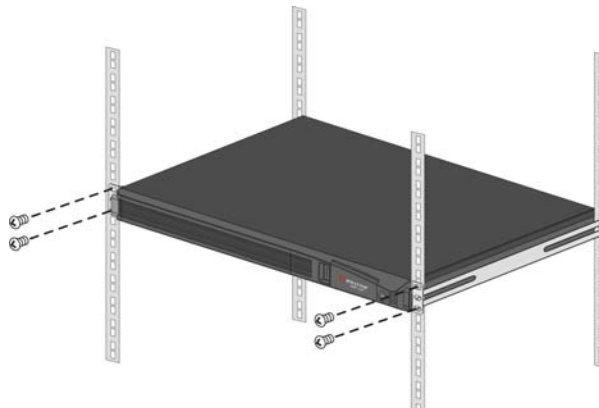
#### RMX 1500



For detailed instructions, precautions and requirements for installing the RMX 1500, refer to the *Polycom RMX 1500 Hardware Guide*.

There are two methods for installing the RMX in a 19" or 23" rack:

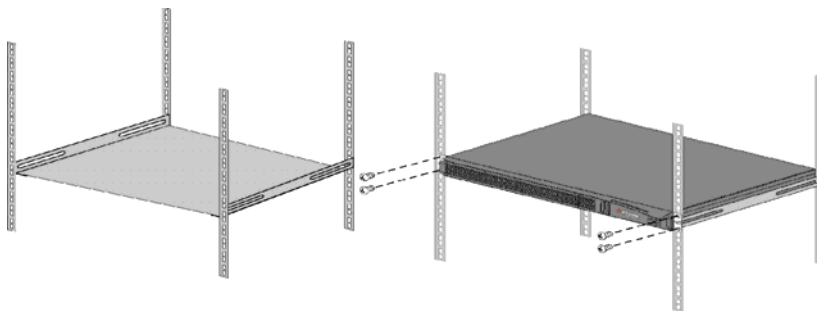
- **Using the chassis runners on the RMX 1500**
  - Install the chassis runners provided by Polycom in the rack using the screws supplied by the rack manufacturer; two screws per chassis runner.
  - Mount the RMX 1500 on top of the chassis runners.
  - Fasten the RMX to the rack with screws through the four holes in the RMX's front mounting brackets.



Chassis runners are 60cm (23.62") in length. If your rack depth is different, a shelf can be used instead.



- **Using a shelf**
  - Install the shelf supplied by the rack manufacturer, in the rack.
  - Mount the *RMX* on the shelf.
  - Fasten the *RMX* to the rack with screws through the four holes in the *RMX*'s front mounting brackets.





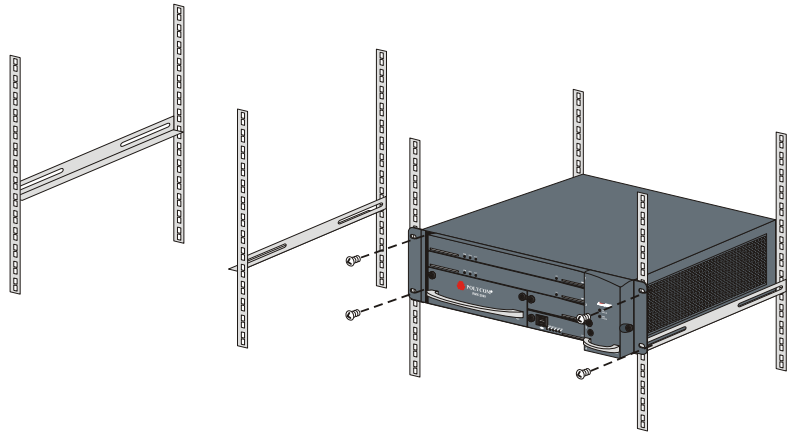
## RMX 2000



For detailed instructions, precautions and requirements for installing the *RMX 2000*, refer to the *Polycom RMX 2000 Hardware Guide*.

There are two methods for installing the *RMX 2000* in a rack:

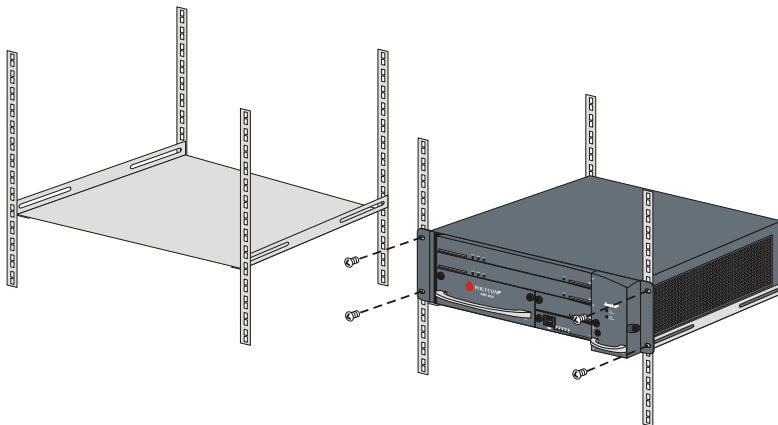
- **Using rack brackets** – Install rack brackets, supplied by the rack manufacturer, in the rack. Mount the *RMX* on top of the rack brackets. Fasten the *RMX* to the rack with screws through the four holes in the *RMX*'s front mounting brackets.



- **Using a shelf** – Install the shelf, supplied by the rack manufacturer, in the rack. Mount the *RMX* on the shelf. Fasten the *RMX* to the rack



with screws through the four holes in the RMX's front mounting brackets.



## RMX 4000



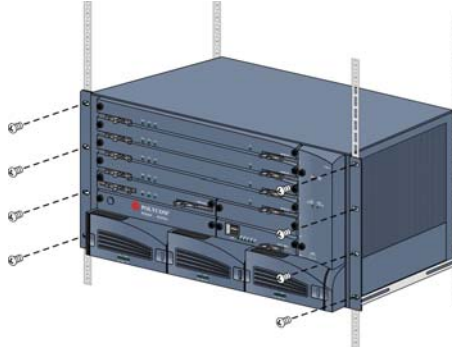
For a detailed description of the safety requirements and precautions and the installation of the *RMX 4000* as a standalone, in a 23" rack, or reverse mounting the *RMX 4000* on a 19" rack, see the *Polycom RMX 4000 Hardware Guide*.

There are two methods for installing the *RMX 4000* in a rack:

- **Using rack brackets** - Install the chassis runners supplied by *Polycom*, in the rack. Mount the *RMX* on top of the rack brackets. Fasten the *RMX* to the rack with screws through the eight holes in the *RMX*'s front mounting brackets.



- **Using a shelf** - Install the shelf, supplied by the rack manufacturer, in the rack. Mount the *RMX* on the shelf. Fasten the *RMX* to the rack with screws through the four holes in the *RMX*'s front mounting brackets.



## Cabling the RMX 1500/2000/4000



**Before connecting Power Cables** refer to the detailed precautions and requirements for the *RMX 1500/2000/4000* in the relevant *Hardware Guide*.

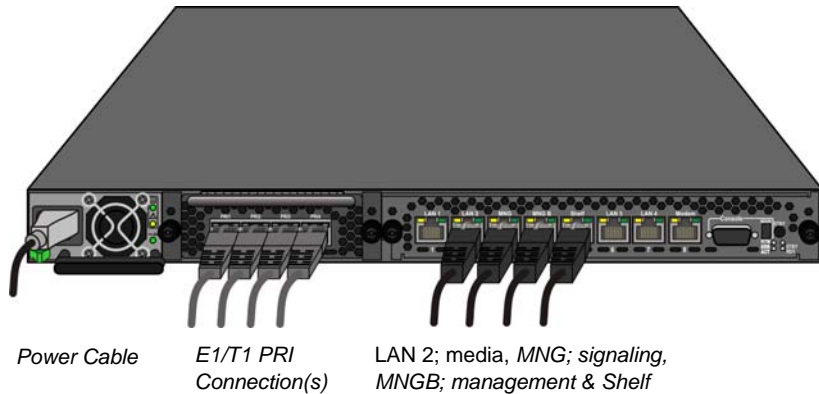
### RMX 1500 Power, Signaling and Media Cables

Connect the following cables to the back panel:

- Power cable
- For the **RTM-IP 1500 module**:
  - Connect the Media cable to **LAN 2** port.
  - Connect the Network cables to the **MNG** (*Signaling*) port & **MNGB** (*Management Network*) port.
  - (Optional) Connect the *Shelf Management* cable to the **Shelf** port.



- For the **RTM ISDN 1500 module**:
  - Connect the E1/T1 cables to their **PRI (1-4)** ports.



**Figure 1-1** RMX 1500 Rear Panel View with AC Power and Communication Cables



The LAN 1, LAN3, LAN4 and Modem ports are not be used and the plastic caps covering those ports should not be removed.

## RMX 2000 Power, Signaling and Media Cables

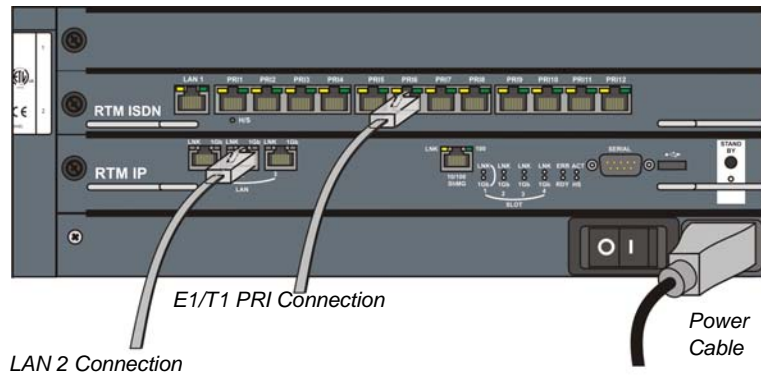


Do not remove the protective cap from the LAN1 port.

Connect the following cables to the back panel:

- Power cable
- Direct Connection / Signaling and Media LAN cable to **LAN 2** Port
- E1/T1 Cables to **PRI** Ports





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

## RMX 4000 AC and DC Power Sources



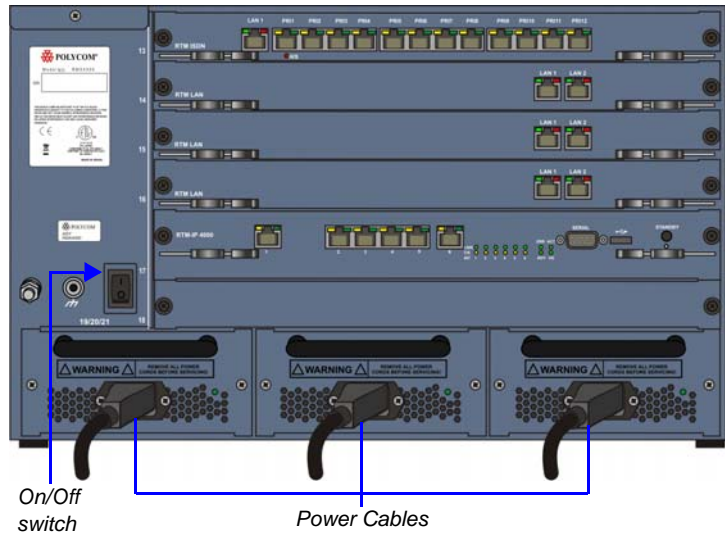
The size of the protective earthing conductor & cable should be a minimum of 10AWG.

Connect the following power cables to the *RMX 4000* back panel:



### AC Power Supply connections:

- 1 Insert power cables to each of the three AC Power Entry Modules (PEMs).



**Figure 1-2** RMX 4000 Rear Panel View with AC Power

### DC Power Supply connections:

- 1 On the DC Power Rail Modules set the two circuit breakers to OFF.



Two types of circuit breakers can be installed on the DC Power Rail Module (PRM). For more information, see the *RMX 4000 Hardware Guide*.

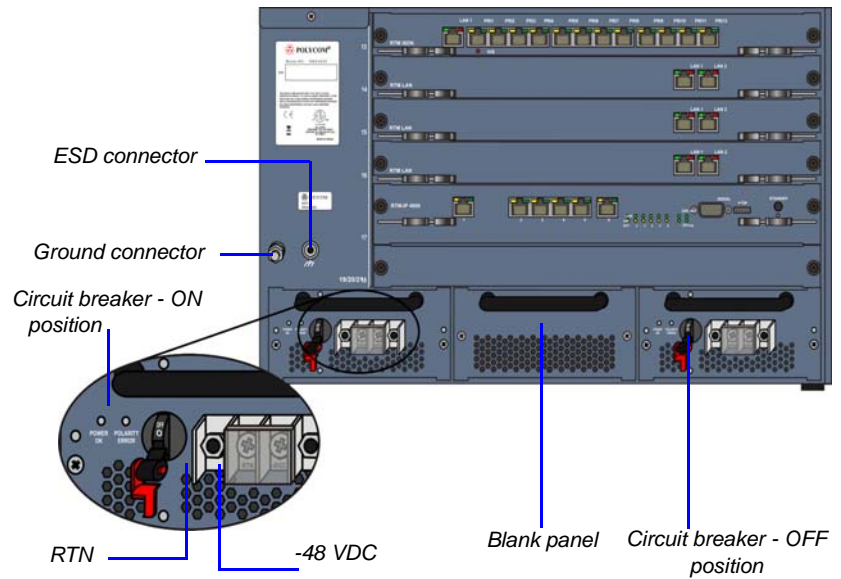
- 2 Ensure that the Main that supplies electricity to the DC power units is OFF and that the cables are disconnected.
- 3 Remove the transparent plastic caps on the terminal block.



- 4 Using the two wires of a 10 AWG cable running from the DC power distribution unit, connect the black wire into the -48VDC terminal block and the red wire to the RTN terminal block.



- A 10 AWG cable must be used to connect the mains with the *RMX 4000* DC Power Rail Model.
- The supply wires for DC version must be terminated using quick connectors.
- Extension cords may not be used.



The center PRM slot/module is fitted with a blank panel and the slot cannot be used on a system with DC Voltage.

- 5 Connect the green or green-yellow wire to the system single-point M6x15 "Ground" bolt.



The rating of the protective earthing conductor should be a minimum of 10AWG.

If the unit is rack mounted, the single-point ground on the MCU must be connected to the rack with a single conductor and fixed as to prevent loosening. When using bare conductors, they must be coated



with an appropriate antioxidant compound before crimp connections are made. Tinned, solder-plated or silver plated connectors do not have to be prepared in this manner.

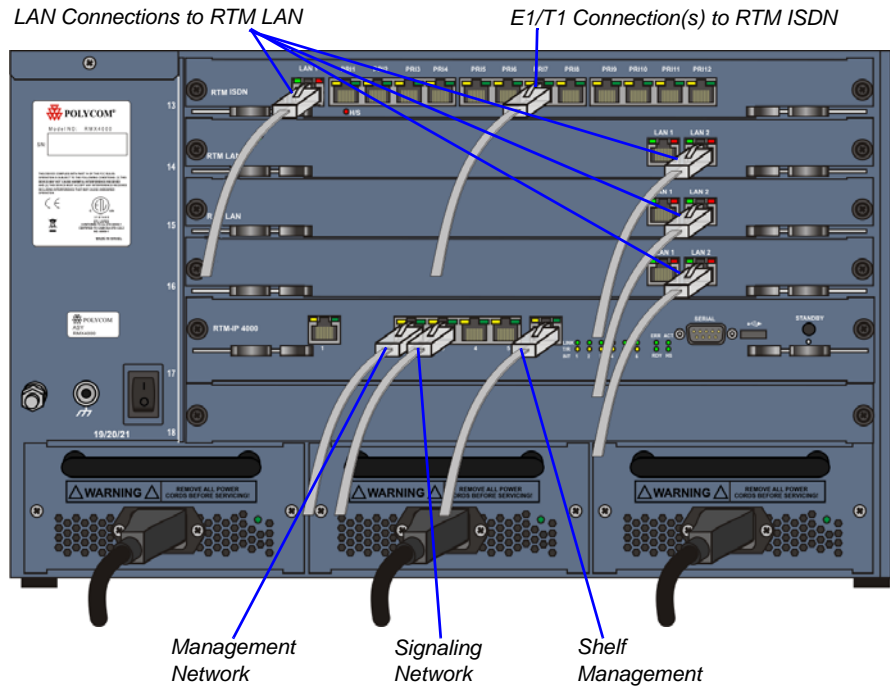
- 6** Replace the transparent plastic caps on the terminal block.
- 7** Turn ON the Main that supplies power to the RMX.
- 8** Turn ON the circuit breaker on each of the DC Power Rail Modules.

### **RMX 4000 Signaling, Media and Management Cables**

- **RTM-IP 4000:**
  - Connect the *Management Network* cable to **LAN 2**.
  - Connect the *Signaling* cable to **LAN 3**.
  - Connect the *Shelf Management* cable to **LAN 6**.
- For each installed **RTM LAN** - Connect the LAN cable to **LAN 2**.



- For each installed **RTM ISDN**:
  - Connect the E1/T1 cables to their **PRI** Ports.
  - Connect the LAN cable to **LAN 1**.

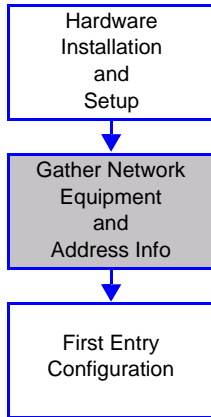


**Figure 1-3** RMX 4000 Rear Panel View with AC Power and Communication Cables



## Procedure 2: Gather Network Equipment and Address Information

### IP Services



The IP addresses and network parameters which enable communication between the RMX, its management application and the conferencing devices are contained in two IP services:

- **Management Network (Control Unit)**
- **Signaling Network (Conferencing Service)**

During the *First Entry Configuration*, the parameters of these two network services are modified to comply with your local network settings.

### Management Network

The *Management Network* enables communication between the RMX *Control Unit* and the *RMX Web Client* and is used to manage the RMX.

The RMX is shipped with default IP addresses as listed in Table 2-1.

### Signaling Network

The *Signaling Network* is used to configure and manage communications between the RMX and conferencing devices.

### IP Network Services Required Information

When installing an RMX unit, these default IP addresses must be modified to your local network settings. It is therefore important to obtain the information needed to complete the **Local Network Settings** section of the table from your network administrator before powering up the RMX for the first time.



The network administrator should allocate four IP addresses in the local network for an MCU with one MPM+ card and up to seven IP addresses for an MCU with up to four MPM+ cards.

**Table 1-1** Network Equipment and Address Information

Parameter	Factory Default	Local Network Settings
<i>Control Unit IP Address</i>	192.168.1.254	
<i>Control Unit Subnet Mask</i>	255.255.255.0	
<i>Default Router IP Address</i>	192.168.1.1	
<i>Shelf Management IP Address</i>	192.168.1.252	
<i>Signaling Host IP address</i>	—	
<i>Media Board IP address (MPM 1)</i>	—	
<i>Media Board IP address (MPM 2)</i> <b>RMX 2000/4000 only</b>	—	
<i>Media Board IP address (MPM 3)</i> <b>RMX 4000 only</b>	—	
<i>Media Board IP address (MPM 4)</i> <b>RMX 4000 only</b>	—	
<i>Gatekeeper IP address (optional)</i>	—	
<i>DNS IP address (optional)</i>	—	



**Table 1-1** Network Equipment and Address Information (Continued)

Parameter	Factory Default	Local Network Settings
SIP Server IP address (SIP is not Supported in Ultra Secure Mode.)	—	

## ISDN/PSTN Services

The ISDN/PSTN Network Service is used to define the properties of the ISDN/PSTN switch and the ISDN lines running from the ISDN/PSTN switch to the ISDN card installed in the RMX.

Before configuring the ISDN/PSTN Network Service, obtain the following information from your ISDN/PSTN Service Provider:

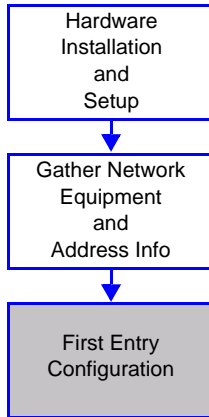
- Switch Type
- Line Coding and Framing
- Numbering Plan
- Numbering Type
- Dial-in number range



- The RMX does not support ISDN connections using restricted line rates (56k B channels).
- If the RMX is connected to the public ISDN Network, an external CSU or similar equipment is needed.



## Procedure 3: First Entry Configuration



There are four procedures necessary for setup of the new *RMX*. It is important that they are performed in the following sequence:

- 1 Product Registration.
- 2 Modifying the Factory Default Management Network Settings.
- 3 First-time Power-up and Connection to MCU.
- 4 Enable *Network Separation (RMX 2000)*
- 5 Modifying the *Default IP* and *ISDN/PSTN Service* settings (*Fast Configuration Wizard*).

## Product Registration

Before the *RMX* can be used, it is necessary to register the product and obtain an *Activation Key*.

During first-time power-up, the *Product Activation* dialog box is displayed, requesting you to enter an *Activation Key*.

### Obtaining the Activation Key

- 1 Access the *Service & Support* page of the Polycom website at:  
**`http://portal.polycom.com`**
- 2 Login with your *Email Address* and *Password* or register as a new user.
- 3 Select **Product Registration**.
- 4 Follow the on-screen instructions for *Product Registration* and *Product Activation*. (The *RMX*'s serial number is on a sticker on the back of the unit, if needed.)
- 5 When the *Product Activation Key* is displayed, write it down or **copy** it for later pasting into the *Activation Key* field of the *Product Activation* dialog box.



## First-time Power-up and Connection to MCU

Before powering up the RMX for the first time, it is necessary to establish a connection between the RMX and the control workstation.

A private network is set up between the RMX and the workstation and the *Default Management Network* parameters are modified using the *Fast Configuration Wizard* in the *RMX Web Client*.

### Configuring the workstation for direct connection

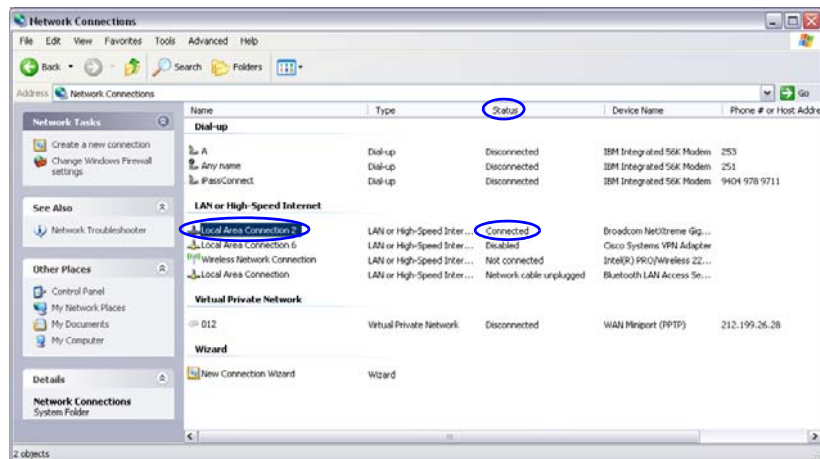
The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with either the RMX's *Default Management Network*.

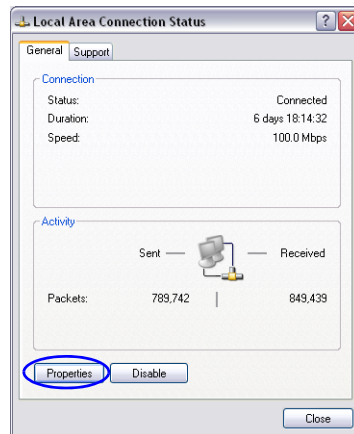
**To modify the workstation's IP addresses:**

- 1 On the Windows *Start* menu, select **Settings > Network Connections**.
- 2 In the *Network Connections* window, double-click the **Local Area Connection** that has *Connected* status.

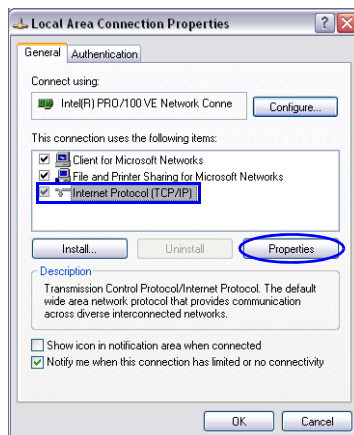




- 3 In the *Local Area Connection Status* dialog box, click the **Properties** button.



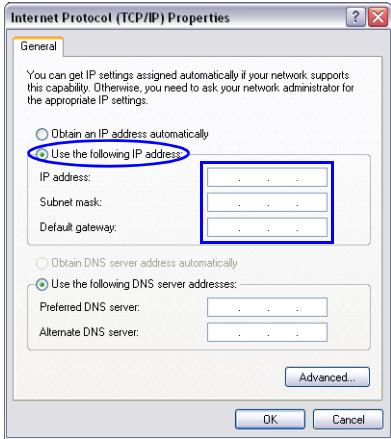
- 4 In the *Local Area Connection Properties* dialog box, select **Internet Protocol [TCP/IP] > Properties**.



- 5 In the *Internet Protocol (TCP/IP) Properties* dialog box, select **Use the following IP address**.



**6** Enter the *IP address*, *Subnet mask* and *Default gateway* for the workstation.



The workstation's IP address should be in the same network neighborhood as the *RMX's Control Unit* IP address.

**Example:** *IP address* – near **192.168.1.nn**



None of the reserved IP addresses listed in *Table 1-2* should be used for the IP Address.

The *Subnet mask* and *Default gateway* addresses should be the same as those for the *RMX's Default Management Network*.

The addresses needed for connection to the *RMX's Default Management Network* are listed in *Table 1-2*.

**Table 1-2** Reserved IP Addresses

Network Entity	Default Management Network IP Addresses (Factory Default)
<i>Control Unit IP Address</i>	192.168.1.254
<i>Control Unit Subnet Mask</i>	255.255.255.0
<i>Default Router IP Address</i>	192.168.1.1



**Table 1-2** Reserved IP Addresses

Network Entity	Default Management Network IP Addresses (Factory Default)
Shelf Management IP Address	192.168.1.252
Shelf Management Subnet Mask	255.255.255.0
Shelf Management Default Gateway	192.168.1.1

- 7 Click the OK button.

## Connecting to the Default Management Network

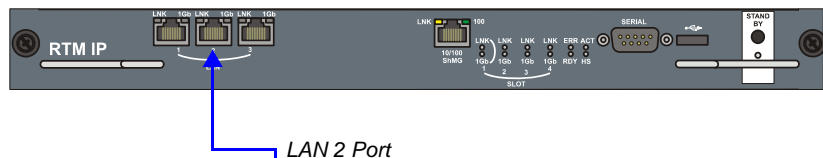
To connect directly to the RMX:

- 8 Using a LAN cable, connect the workstation to the *LAN 2* port on the RMX 2000/4000's back panel or the *MNGB Port* on the RMX 1500.

### RMX 1500



### RMX 2000



### RMX 4000



- 9 Connect the power cable and power the RMX On.
- 10 Start the *RMX Web Client* application on the workstation, by entering the factory setting *Management IP* address in the browser's address line and pressing **Enter**.



- 11** In the *RMX Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click the **Login** button. The *Fast Configuration Wizard* starts.



Both *IPv4* and *IPv6* are supported. For *IPv6* addressing information see the *Polycom RMX 1500/2000/4000 System Administrator's Guide for Maximum Security Environments "IP Network Services"* on page **11-2**.

If this is the *First Time Power-up* or the *Default IP Service* has been deleted and the *RMX* has been reset, the following dialog box is displayed:

**Fast Configuration Wizard**

- > **IP Manageme...**
  - > IP Signaling
  - > Routers
  - > DNS
  - > Network Type
  - > Gatekeeper
  - > SIP Server
  - > Security
  - > ISDN/PSTN
  - > PRI Settings
  - > Span Definition
  - > Phones
  - > Spans
  - > Video/Voice Ports
  - > System Flags

Network Service Name:

---

Control Unit IP Address:

Shelf Management IP Address:

Subnet Mask:

Default Router IP Address:

Back Save & Close Cancel

- 12** Enter the following parameters using the information supplied by your network administrator:
- *Control Unit IP Address*
  - *Shelf Management IP Address*
  - *Control Unit Subnet Mask*
  - *Default Router IP Address*
- 13** Click the **Save & Close** button.



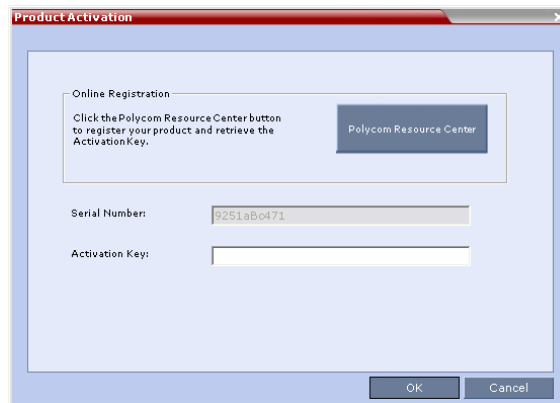
The system prompts you to sign in with the new *Control Unit IP Address*.



- 14** Disconnect the LAN cable between the workstation and the *LAN 2* port on the *RMX*'s back panel.
- 15** Connect *LAN 2* port on the *RMX*'s back panel to the local network using a LAN cable.
- 16** Enter the new *Control Unit IP Address* in the browser's address line, using a workstation on the local network, and press **Enter** to start the *RMX Web Client* application.
- 17** In the *RMX Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click the **Login** button.

## Product Activation

The *RMX Web Client* opens and the *Product Activation* dialog box appears with the serial number filled in:



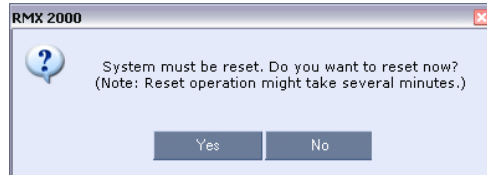
- 18** In the *Activation Key* field, enter or **paste** the *Product Activation Key* obtained earlier.
- 19** Click **OK**.



If you do not have an *Activation Key*, click **Polycom Resource Center** to access the *Service & Support* page of the Polycom website.

For more information, see "*Obtaining the Activation Key*" on page **1-17**.

The system prompts with a restart dialog box:



**20** In the dialog box, click **No**.



## Modifying the Signaling Network Service and ISDN/PSTN Network Service Settings

The *Fast Configuration Wizard* assists in configuring the *Signaling Network Service*. It starts automatically if no *Signaling Network Service* is defined. This happens during *First Time Power-up*, before the service has been defined or if the *Signaling Service* has been deleted, followed by an RMX restart.

The *IP Management Service* tab in the *Fast Configuration Wizard* is enabled only if the factory default *Management IP* addresses were not modified.



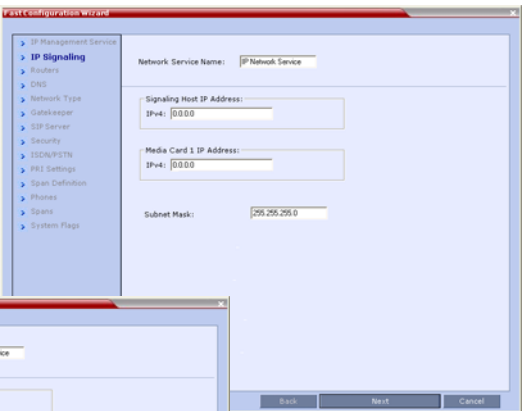
Both IPv4 and IPv6 are supported. For IPv6 addressing information see the *Polycom RMX 1500/2000/4000 System Administrator's Guide for Maximum Security Environments* "IP Network Services" on page [11-2](#).



# Fast Configuration Wizard

- 1 Enter the required IP Signaling information in the dialog box.

RMX 1500

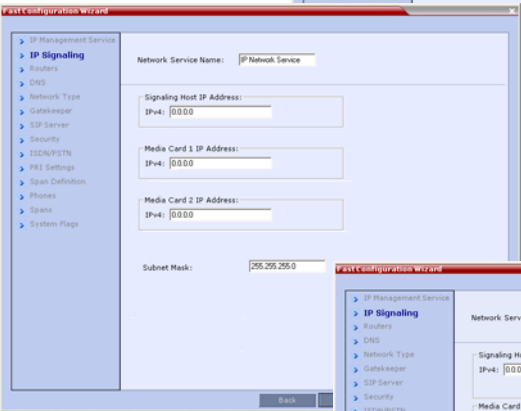


The RMX 1500 configuration window shows the 'IP Signaling' section selected in the left sidebar. The main area contains the following fields:

- Network Service Name: IP Network Service
- Signaling Host IP Address: IPv4: 0.0.0.0
- Media Card 1 IP Address: IPv4: 0.0.0.0
- Subnet Mask: 255.255.255.0

Buttons at the bottom: Back, Next, Cancel.

RMX 2000

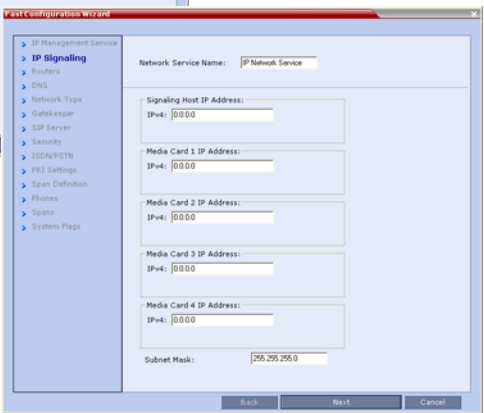


The RMX 2000 configuration window shows the 'IP Signaling' section selected in the left sidebar. The main area contains the following fields:

- Network Service Name: IP Network Service
- Signaling Host IP Address: IPv4: 0.0.0.0
- Media Card 1 IP Address: IPv4: 0.0.0.0
- Media Card 2 IP Address: IPv4: 0.0.0.0
- Subnet Mask: 255.255.255.0

Buttons at the bottom: Back.

RMX 4000



The RMX 4000 configuration window shows the 'IP Signaling' section selected in the left sidebar. The main area contains the following fields:

- Network Service Name: IP Network Service
- Signaling Host IP Address: IPv4: 0.0.0.0
- Media Card 1 IP Address: IPv4: 0.0.0.0
- Media Card 2 IP Address: IPv4: 0.0.0.0
- Media Card 3 IP Address: IPv4: 0.0.0.0
- Media Card 4 IP Address: IPv4: 0.0.0.0
- Subnet Mask: 255.255.255.0

Buttons at the bottom: Back, Next, Cancel.



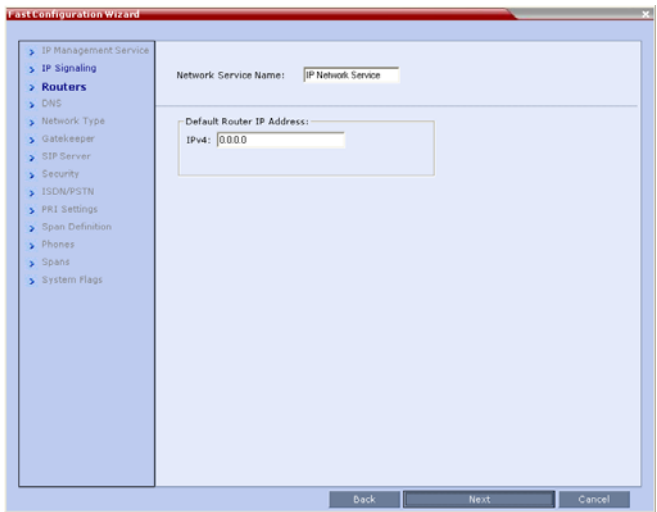
**Table 1-3**     *Signaling Network Service – IP Signaling*

Field	Description
<i>Network Service Name</i>	The name <i>Default IP Service</i> is assigned to the Signaling Network Service by the Fast Configuration Wizard. This name can be changed. <b>Note:</b> This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
<i>Signaling Host IP Address</i>	Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the RMX are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server.
<i>Media Card 1-4 IP Addresses</i>	Enter the IP address(es) of the media card (s) (MPM+/MPMx 1 and MPM+/MPMx 2-4 (if installed)) as provided by the network administrator. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.
<i>Subnet Mask</i>	Enter the subnet mask of the MCU. Default value: 255.255.255.0.

- 2 Click the **Next** button.



3 Enter the required **Routers** information in the dialog box.



**Table 1-4** Signaling Network Service – Routers

Field	Description
Default Router IP Address	Enter the IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.



- 4 Click the **Next** button.
- 5 Enter the required **DNS** information in the dialog box.

The screenshot shows the 'Fast Configuration Wizard' window. On the left is a tree view with the following items: IP Management Service, IP Signaling, Routers, DNS (selected), Network Type, Gatekeeper, SIP Server, Security, ISDN/PSTN, PRI Settings, Span Definition, Phones, Spans, and System Flags. The main content area is for the 'DNS' configuration. It includes the following fields:

- Network Service Name: IP Network Service
- MCU Host Name: (empty text field)
- DNS: Off (dropdown menu)
- Local Domain Name: (empty text field)
- Primary DNS Server IP Address: 0.0.0.0 (text field)

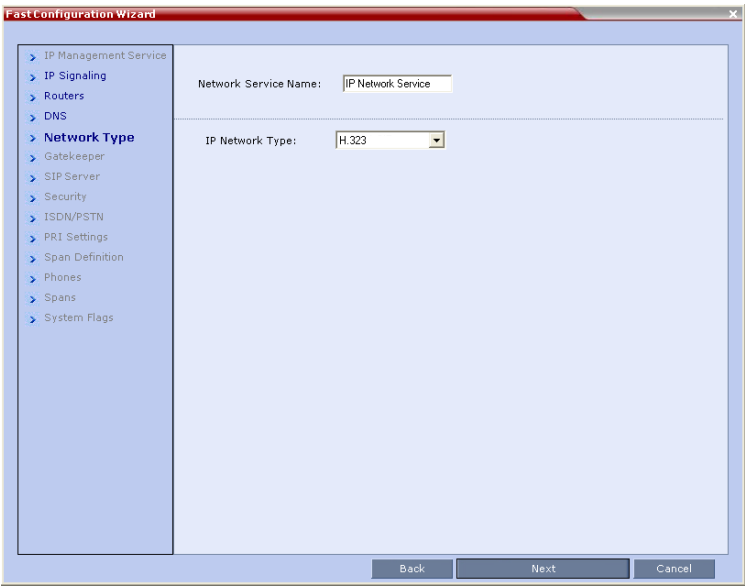
At the bottom of the window are three buttons: Back, Next, and Cancel.

**Table 1-5** Signaling Network Service – DNS

Field	Description
<i>MCU Host Name DNS</i>	Enter the name of the MCU on the network. Default name is RMX
<i>Local Domain Name</i>	Enter the name of the domain where the MCU is installed.
<i>Primary DNS Server IP Address</i>	The static IP addresses of the DNS servers. A maximum of three servers can be defined.



- 6 Click the **Next** button.
- 7 Enter the required **Network Type** information in the dialog box.



**Table 1-6** Signaling Network Service – IP

Field	Description
<i>IP Network Type</i>	Select: <ul style="list-style-type: none"><li>• <b>H.323:</b> For an H.323-only Network Service.</li></ul>

- 8 Click the **Next** button.



9 Enter the required **Gatekeeper** information in the dialog box.

The screenshot shows the 'Fast Configuration Wizard' window. On the left is a tree view with the following items: IP Management Service, IP Signaling, Routers, DNS, Network Type, **Gatekeeper** (selected), SIP Server, Security, ISDN/PSTN, PRI Settings, Span Definition, Phones, Spans, and System Flags. The main area on the right is titled 'Gatekeeper' and contains the following fields:

- Network Service Name:** A text box containing 'IP Network Service'.
- Gatekeeper:** A dropdown menu currently set to 'Off'.
- Primary Gatekeeper:** A label above a text box.
- IP Address or Name:** A text box.
- MCU Prefix in Gatekeeper:** A text box.
- Aliases:** A table with two columns: 'Alias' and 'Type'. There are five rows, each with 'None' in the 'Type' column.

At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.

**Table 1-7** Signaling Network Service – Gatekeeper Parameters

Field	Description
<i>Gatekeeper</i>	Select <b>Specify</b> to enable configuration of the gatekeeper IP address. When <b>Off</b> is selected, all gatekeeper options are disabled.
<i>Primary Gatekeeper IP Address or Name</i>	Enter either the gatekeeper's host name as registered in the DNS or IP address.
<i>MCU Prefix in Gatekeeper</i>	Enter the number with which this Network Service registers with the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU. When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.



**Table 1-7**    *Signaling Network Service – Gatekeeper Parameters*

Field	Description
<b>Aliases:</b>	
<i>Alias</i>	The alias that identifies the RMX's Signaling Host within the network. Up to five aliases can be defined for each RMX. <b>Note:</b> When a gatekeeper is specified, at least one alias must be entered in the table. Additional aliases or prefixes may also be entered.
<i>Type</i>	The type defines the format in which the card's alias is sent to the gatekeeper. Each alias can be of a different type: <ul style="list-style-type: none"><li>• H.323 ID (alphanumeric ID)</li><li>• E.164 (digits 0-9, * and #)</li><li>• Email ID (email address format, e.g. abc@example.com)</li><li>• Participant Number (digits 0-9, * and #)</li></ul> <b>Note:</b> Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.

**10** Click the **Next** button.

The IP Network Service is created and confirmed.



**11** Click **OK**.

During the initial RMX setup, if the system detects the presence of the RTM ISDN card, the ISDN /PSTN Network Service definition screens of the Fast Configuration Wizard are enabled.



If there is no *RTM ISDN* card in the *RMX* or if you do not want to define an *ISDN/PSTN Network Service*, go to Step 26.



- The RMX does not support ISDN connections using restricted line rates (56k B channels).
- A new ISDN/PSTN Network Service can be defined even if no RTM ISDN card is installed in the system **but** only via the *ISDN/PSTN Network Service* ->Add New Service dialog box.

The *Fast Configuration Wizard's* *ISDN/PSTN* configuration sequence begins with the *ISDN/PSTN* dialog box:

## 12 Define the following parameters:

**Table 1-8** Fast Configuration Wizard – ISDN Service Settings

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



**Table 1-8** Fast Configuration Wizard – ISDN Service Settings

Field	Description
Span Type	Select the type of spans (ISDN/PSTN) lines, supplied by the service provider, that are connected to the RMX. Each span can be defined as a separate Network Service, or all the spans from the same carrier can be defined as part of the same Network Service. Select either: <ul style="list-style-type: none"><li>• <b>T1</b> (U.S. – 23 B channels + 1 D channel)</li><li>• <b>E1</b> (Europe – 30 B channels + 1 D channel)</li></ul> Default: T1 <b>Note:</b> Only one <i>Span Type</i> (E1 or T1) is supported on the RMX. If you define the first span as type E1 all other spans that you may later define must also be of type E1.
Service Type	PRI is the only supported service type. It is automatically selected.

**13** Click **Next**.

The *PRI Settings* dialog box opens.

The screenshot shows the 'Fast Configuration Wizard' window. On the left is a tree view with the following items: IP Management Service, IP Signaling, Routers, DNS, Network Type, Gatekeeper, SIP Server, Security, ISDN/PSTN, PRI Settings (highlighted), Span Definition, Phones, Spans, and System Flags. The main content area is titled 'PRI Settings' and contains the following fields:  
- Network Service Name: A text box containing 'Default PSTN Service'.  
- Default Num Type: A dropdown menu with 'Unknown' selected.  
- Num Plan: A dropdown menu with 'ISDN/PSTN' selected.  
- Net Specific: A dropdown menu with 'None' selected.  
- Dial-out Prefix: An empty text box.  
At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.



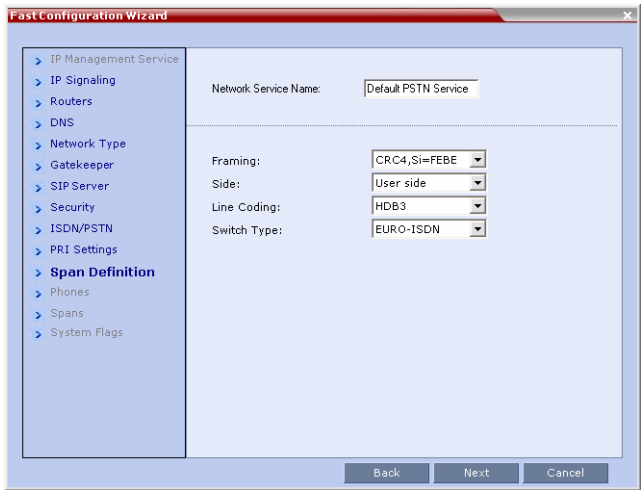
**14** Define the following parameters:**Table 1-9** Fast Configuration Wizard – PRI Settings

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

**15** Click **Next**.



The *Span Definition* dialog box opens.



**16** Define the following parameters:

**Table 1-10** Fast Configuration Wizard – Spans Definition

Field	Description
<i>Framing</i>	Select the Framing format used by the carrier for the network interface from the list. <ul style="list-style-type: none"><li>For T1 spans, default is SFSF.</li><li>For E1 spans, default is FEFE.</li></ul>
<i>Side</i>	Select one of the following options: <ul style="list-style-type: none"><li>User side (default)</li><li>Network side</li><li>Symmetric side</li></ul> <p><b>Note:</b> If the PBX is configured on the network side, then the RMX unit must be configured as the user side, and vice versa, or both must be configured symmetrically.</p>
<i>Line Coding</i>	Select the PRI line coding method from the list. <ul style="list-style-type: none"><li>For T1 spans, default is B8ZS.</li><li>For E1 spans, default is HDB3.</li></ul>

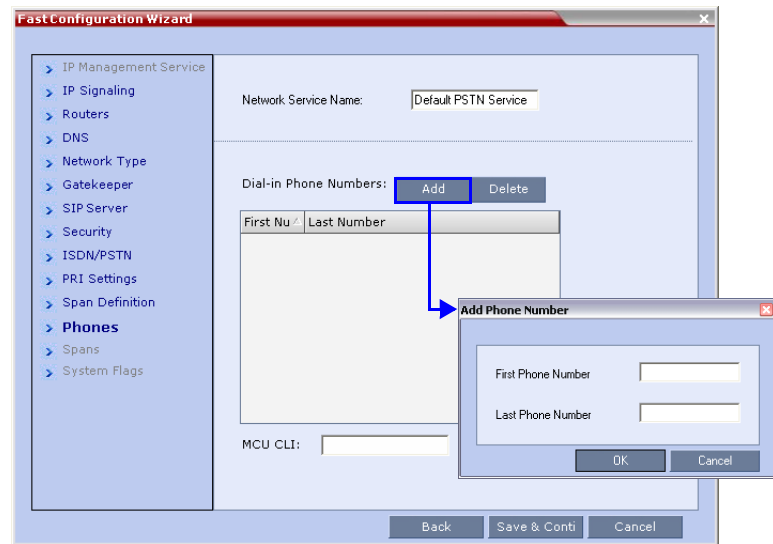


**Table 1-10** Fast Configuration Wizard – Spans Definition

Field	Description
<i>Switch Type</i>	Select the brand and revision level of switch equipment installed in the service provider's central office. <ul style="list-style-type: none"> <li>For T1 spans, default is AT&amp;T 4ESS.</li> <li>For E1 spans, default is EURO ISDN.</li> </ul>

**17** Click **Next**.

The *Phones* dialog box opens.

**18** Click **Add** to define dial-in number ranges.

The *Add Phone Number* dialog box opens.

**19** Define the following parameters:**Table 1-11** Fast Configuration Wizard – Add Phone Numbers

Field	Description
<i>First Number</i>	The first number in the phone number range.
<i>Last Number</i>	The last number in the phone number range.





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

**20** Click **OK**.

The new range is added to the *Dial-in Phone Numbers* table.

**21** **Optional.** Repeat steps **18** to **19** to define additional dial-in ranges.

**22** In the *Phones* tab enter the *MCU CLI (Calling Line Identification)*.

With dial-in connections, the *MCU CLI* indicates the MCU's number dialed by the participant. In a dial-out connection, indicates the MCU (*CLI*) number as seen by the participant.

**23** Click **Save & Continue**.

After clicking **Save & Continue**, you cannot use the **Back** button to return to previous configuration dialog boxes.

The *ISDN/PSTN Network Service* is created and is added to the *ISDN/PSTN Network Services* list.

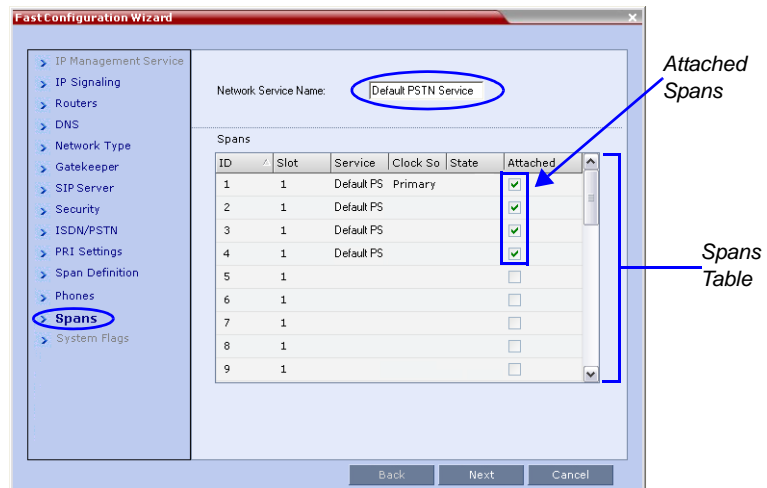
If the system cannot create the *ISDN/PSTN Network Service*, an error message is displayed indicating the cause and allowing you access the appropriate dialog box in the *Fast Configuration Wizard* for corrective action.



**24** Click **OK** to continue the configuration.



The *Spans* dialog box opens displaying the following read-only fields:



- **ID** – the connector on the ISDN RTM card (PRI1 to PRI12).
- **Slot** – the MPM+ card that the ISDN RTM card is connected to (MPM 1 or MPM 2).
- **Service** – the ISDN/PSTN Network Service to which the span is assigned.
- **Clock Source** – indicates if ISDN signaling synchronization is being supplied by the *Primary* or *Secondary* clock source. The first span to synchronize becomes the *Primary* clock source.
- **State** – the *System Alert* level of the span (*Major*, *Minor*). If there are no span related alerts, this column contains no entries.

- 25** Click the check boxes in the *Attached* field to attach spans (E1 or T1 PRI lines) to the network service named in the *Network Service Name* field.

The *Spans Table* displays the configuration of all spans and all ISDN network services in the system.

When using the *Fast Configuration Wizard* during *First Entry Configuration*, you are defining the first ISDN/PSTN Network Service in the system. Spans can only be attached to this service.

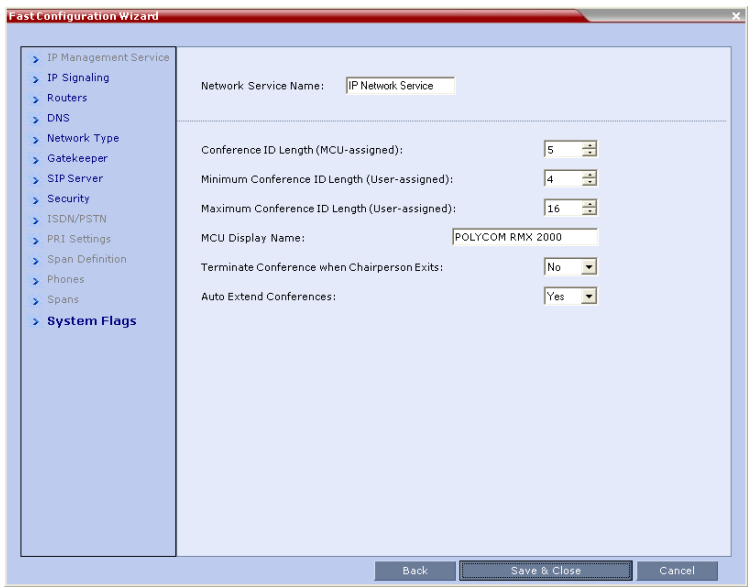
Additional ISDN/PSTN Network Services can be defined by using the **ISDN/PSTN Network Services > New PSTN Service** button in the RMX Web Client.



Spans can be attached to, or moved between ISDN network services by using the **ISDN/PSTN Network Services > ISDN Properties > Spans** tab in the *RMX Web Client*.

Each ISDN RTM card can support either 7 *E1* or 9 *T1 PRI* lines (*E1* and *T1* connections cannot be used simultaneously).

- 26 Click **Next**.
- 27 Enter the required **System Flags** information in the dialog box.



**Table 1-12** Signaling Network Service – System Flags

Flag	Description / Default	
<i>Conference ID Length (MCU)</i>	The number of digits of the Conference ID to be assigned by the MCU. Range: 2-16 (Default: 5)	<b>Note:</b> Selecting 2 digits limits the number of simultaneous ongoing conferences to 99.
<i>Minimum Conference ID Length (User)</i>	The minimum number of digits that the user must enter when manually assigning a numeric ID to a conference. Range: 2-16 (Default: 4)	



**Table 1-12** Signaling Network Service – System Flags (Continued)

Flag	Description / Default	
<i>Maximum Conference ID Length (User)</i>	The maximum number of digits that the user can enter when manually assigning a Numeric ID to a conference. Range: 2-16 (Default: 8)	<b>Note:</b> Selecting 2 digits limits the number of simultaneous ongoing conferences to 99.
<i>MCU Display Name</i>	The MCU name is displayed on the endpoint's screen. Default name: <i>Polycom RMX 1500</i> , <i>Polycom RMX 2000</i> or <i>Polycom RMX 4000</i> .	
<i>Terminate Conference when Chairperson Exits</i>	When <b>Yes</b> is selected (default), the conference ends when the chairperson exits even if there are other participants connected. When <b>No</b> is selected, the conference automatically ends at the predefined end time, or when all the participants have disconnected from the conference.	
<i>Auto Extend Conferences</i>	When <b>Yes</b> is selected (default), allows conferences running on the RMX to be automatically extended as long as there are participants connected and there are available resources. The maximum extension time allowed by the MCU is 30 minutes.	

**28** Click **Save & Close**.

The RMX confirms successful configuration.

**29** In the *Success Message* box, click **OK**.**30** In the *Reset Confirmation* dialog box, click **Yes**.**31** In the *Please wait for system reset* message box, click **OK**.

System restart may take up to five minutes.

**32** Refresh the browser periodically until the *Login* screen is displayed.**33** When the *Login* screen is displayed, enter your *Username* and *Password* and click **Login**.

On first entry, the default *Username* and *Password* are both **POLYCOM**.



The system is now fully configured and if there are no *System Errors*, the green RDY LED on the CNTL module on the RMX's front panel turns ON.

## Procedure 4: Enable Ultra Secure Mode

The *Ultra Secure Mode* is disabled by default and can be enabled by changing the value of the **ULTRA\_SECURE\_MODE** *System Flag* to **YES** using the **Setup > System Configuration** menu. After modifying the value of the **ULTRA\_SECURE\_MODE** *System Flag* to **YES**, all RMX users are forced to change their *Login* passwords.

**To enable Ultra Secure Mode:**

- 1** On the RMX menu, click **Setup > System Configuration**.  
The *System Flags* dialog box opens.
- 2** Locate and double-click on the **ULTRA\_SECURE\_MODE** *System Flag* entry.  
The *Update Flag Name* dialog box opens.
- 3** In the *New Value* field, enter **YES**.
- 4** Click the **OK** button to close the *Update Flag Name* dialog box.
- 5** Click the **OK** button to close the *System Flags* dialog box.
- 6** In the *Reset Confirmation* dialog box, click **Yes**.
- 7** In the *Please wait for system reset* message box, click **OK**.



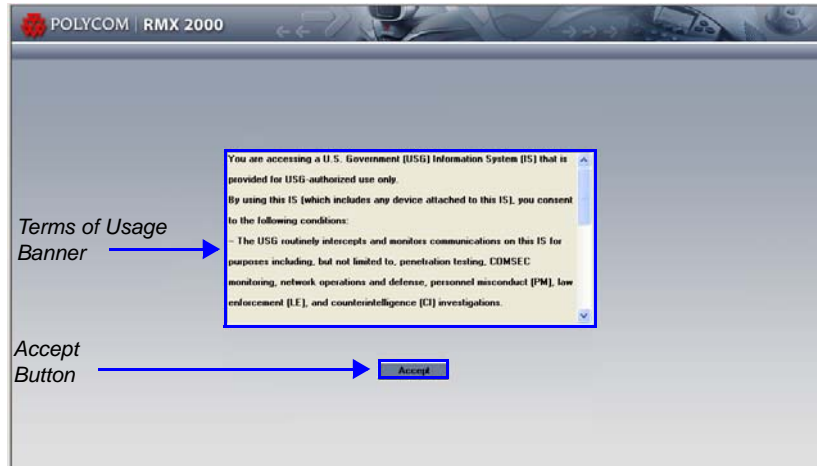
System restart may take up to five minutes.

- 8** Refresh the browser periodically until the *RMX Web Client – Terms of Usage* screen is displayed.



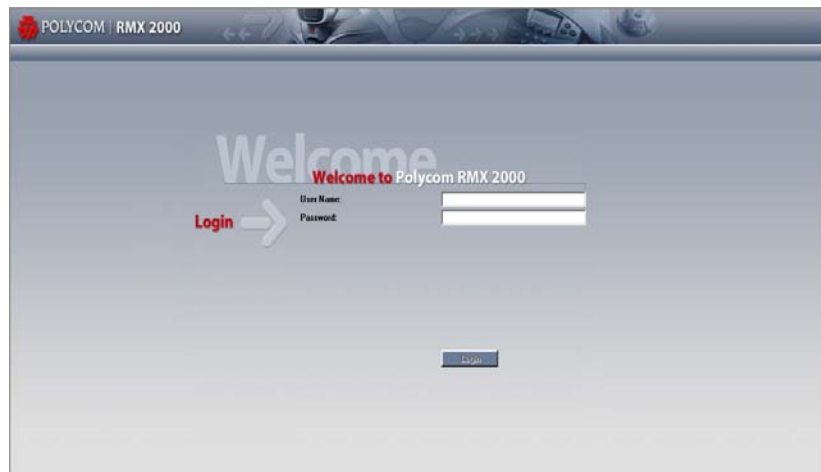
## Connecting to the RMX

The *RMX Web Client – Terms of Usage* screen is displayed.



- 9 Click the **Accept** button to agree to the terms and conditions displayed in the banner.

The *Login - Welcome* screen is displayed:

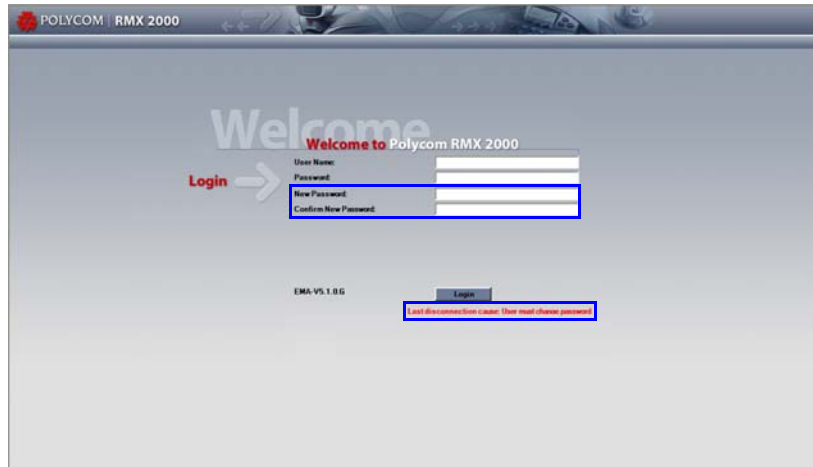


- 10 Enter **POLYCOM** in the *User Name* field.
- 11 Enter **POLYCOM** in the *Password* field.
- 12 Click **Login**.



The *Change Password/Login - Welcome* screen is displayed:

- A message: **Last disconnection cause: User must change password** is displayed in red.
- Two additional fields are displayed:
  - *New Password*
  - *Confirm New Password*



- 13** Re-enter the old password in the *Password* field
- 14** Enter a *Strong Password* in the *New Password* field.
- 15** Re-enter the *Strong Password* in the *Confirm New Password* field.
- 16** Click **Login**.



If the default POLYCOM user is defined in the *RMX Web Client*, an active alarm is displayed and the MCU status changes to Major until the administrator changes the default username and password. System access is not permitted until the default password is changed.



If the value of the ULTRA\_SECURE\_MODE System Flag is YES, only TLS mode connections are permitted. If the Management Network Service has not yet been configured to be secured, an Active Alarm is created and a message is displayed stating that Secured Communications Mode must be enabled. For more information, see the *RMX 1500/2000/4000 Administrator's Guide* for Maximum Security Environments "Secure Communication Mode" on page [F-1](#).



## Procedure 5: Enable Secured Communication

If the **ULTRA\_SECURE\_MODE** *System Flag* is set to YES, a valid *TLS* certificate must be installed, and a secured connection between the *RMX Web Client* (or *RMX Manager*) and the *RMX* unit must be defined.

- If the **ULTRA\_SECURE\_MODE** *System Flag* is set to YES and the *Management Network Service* has not yet been configured to be secured, an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.
- If the **ULTRA\_SECURE\_MODE** *System Flag* is set to YES and a valid *TLS* certificate has not been installed, an *Active Alarm* is created and a message is displayed stating that the system is in *Ultra Secure Mode* but *Secured Communications Mode* is not enabled until the *TLS* certificate is installed.
- If the **ULTRA\_SECURE\_MODE** *System Flag* is set to YES and *Secured Communications Mode* is enabled, the user is not able to disable *Secured Communications Mode*. An error message is displayed stating that *Secured Communications Mode* cannot be disabled while in *Ultra Secure Mode*.
- *TLS* private keys saved by the current version when the **ULTRA\_SECURE\_MODE** *System Flag* is set to YES are not compatible with *TLS* private keys saved by previous *RMX* versions. An *Active Alarm* is created and a message is displayed requesting that a new *TLS* certificate be installed.
- *TLS* private keys saved by the current version will be compatible with *TLS* private keys saved by future *RMX* versions.



# Enabling to Secure Mode

The following operations are required to switch the *RMX* to *Secure Mode*:

- Purchase and Install the *SSL/TLS certificate*
- Modify the *Management Network* settings

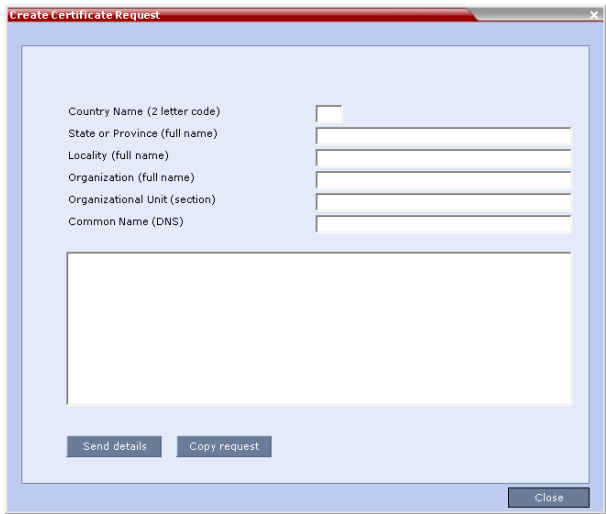
## Purchasing a Certificate

Once a certificate is purchased and received it is stored in the *RMX* and used for all subsequent secured connections.

To create/purchase a certificate:

- 1 In the *RMX* menu, click **Setup > Secured RMX Communications > Create certificate request**.

The *Create Certificate Request* dialog box is displayed.



- 2 Enter information in all the following fields:

**Table 1-13** *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.



**Table 1-13** Create Certificate Request (Continued)

Field	Description
<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.

### 3 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.

Country Name (2 letter code)

State or Province (full name)

Locality (full name)

Organization (full name)

Organizational Unit (section)

Common Name (DNS)

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBkjCEAIBADBTMQswCQYDVQQGEwJ0DELMAkGA1UECBMCDUxhCzA1BgNVBACQ
AjMyHRAdDgYDVQQKEwQQT0xZQ09NMQswCQYDVQQLLEw1ZDELMAkGA1UEAxMCNDMw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALBshuzaZVgBuXwh/LTICqJvZrTG
6HTchQumEt8Hlx+ROQmvEsaxug9A34/DVYA3MHWhbmcQbJNUairVbaurLxMhqDrp
olZukBN6nm+5pdv6j/gFN7o43aqWEvhzDubbHnTwa/R92JoZ738t/y9p2b+69rrh
efOidxCQBvAp4ajAgMBAAQgADANBgkqhkiG9w0BAQQAQFAAOBgQCW1qzGlubeZOEH
qJNi6TBzE9cmOs2NU1zf+Ub7IZOIMoskx9wwX1pjdKByF5jd1x+Nyrv6RGHdf
XSVv8wwm0FX7IZ6n6VvpdoENeIPP9Qms2eWlUZWUP0n075JIKZqj7XA0y/nib4
JKI/TH9/RAOCTkm7eX4dik2HuTSdQ==
-----END NEW CERTIFICATE REQUEST-----

```

### 4 Click Copy Request to copy the New Certificate Request to the workstation's clipboard.

### 5 Connect to your preferred Certificate Authority's website using the web browser.



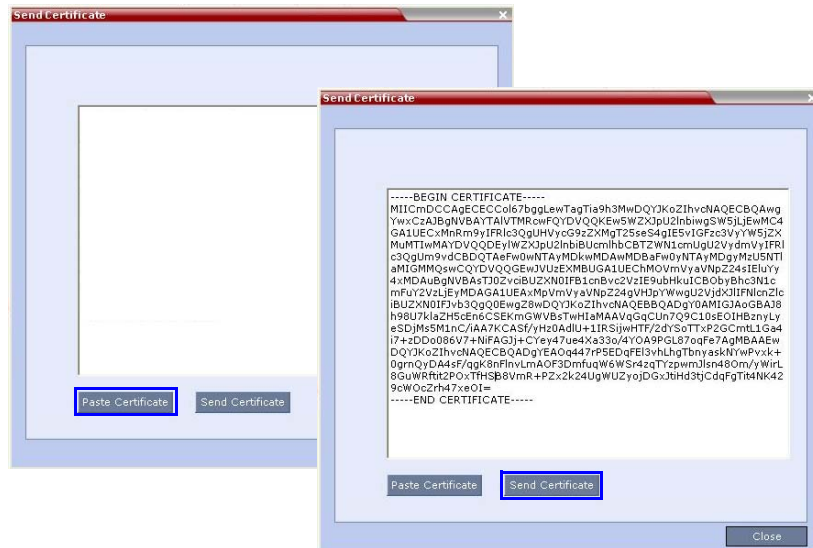
- 6 Follow the purchasing instructions at the *Certificate Authority's* website.  
Paste (**Ctrl + V**) the *New Certificate Request* as required by the *Certificate Authority*.  
The *Certificate Authority* issues the *TLS/SSL* certificate, and sends the certificate to you by e-mail.

## Installing the Certificate

To install the certificate:

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

- 1 **Copy** (**Ctrl + C**) the certificate information from the *Certificate Authority's* e-mail to the clipboard.
- 2 In the *RMX* menu, click **Setup > Secured RMX Communications > Send Certificate**.
- 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*.  
The *RMX* 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.

A *System Restart* is **not** required at this point.

The certificate expiry date is checked daily. An active alarm is raised two weeks before the certificate is due to expire, stating the number of days to expiry.

If the certificate expires, the RMX continues to work in secure mode and an *Active Alarm* is raised with *Security mode failed – Certificate expired* in the description field.



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

## Switching to Secure Communication Mode

After the *SSL/TLS* certificate is installed, secure communications are enabled by modifying the properties of the *Management Network* in the *Management Network* properties dialog box.

When *Secure Communications Mode* is enabled:

- Only **https://** commands from the browser to the *Control Unit IP Address* of the RMX are accepted.
- The RMX listens only on secured port 443.
- All connection attempts on port 80 are rejected.
- A secure communication indicator (🔒) is displayed in the browser's status bar.

**To enable secure communications mode:**

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



The *Management Network Properties* dialog box is displayed.

ManagementNetwork Properties

- > IP
- > Routers
- > DNS
- > LAN Ports

Network Service Name: Management Network

IP Version: IPv4

Control Unit IP Address:  
IPv4: 172.22.187.153

Shelf Management IP Address:  
IPv4: 172.22.187.154

Subnet Mask: 255.255.248.0

☒ Secured Communication

- 3** Select the *Secured RMX Communication* check box.
- 4** Click **OK**.
- 5** In the *Reset Confirmation* dialog box, click **Yes**.
- 6** In the *Please wait for system reset* message box, click **OK**.



System restart may take up to five minutes.

Refresh the browser periodically until the *RMX Web Client – Terms of Usage* screen is displayed



## Procedure 6: Set System Configuration Flags

*Maximum Security Environments* have additional *System Flags* that control:

- *Network Security*
- *User Management*
- *Strong Passwords*
- *Login and Session Management*
- *Cyclic File Systems*

When the *Maximum Security Environment* is enabled by setting the **ULTRA\_SECURE\_MODE** *System Flag* to **YES**, the enhanced security features are enforced. *Table 1-14* lists the default values of these flags.

**Table 1-14** *System Flags and their default values*

Flag	Description	Value
<code>ALLOW_NON-ENCRYPT_PARTY_IN_ENCRYPT_CONF</code>	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No	NO
<code>DISABLE_INACTIVE_USER</code>	Determines the number of consecutive days a user can be inactive before being disabled. Default: 30 Range: 1-90	30
<code>ENABLE_CYCLIC_FILE_SYSTEM_ALARMS</code>	When set to YES an Active Alarm is created when a Cyclic File (Log, CDR, Audit) reaches a file retention time or file storage capacity limit. Default: YES	YES
<code>FORCE_STRONG_PASSWORD_POLICY</code>	Enables or disables all password related flags. This flag cannot be set to NO when the RMX is in <i>Ultra Secure Mode</i> . Default: YES	YES
<code>HIDE_CONFERENCE_PASSWORD</code>	When set to YES, Conference and Chairman passwords are replaced by asterisks in the RMX Web Client, RMX Manager, Audit Event and Log files. Default: YES	YES



**Table 1-14** System Flags and their default values

Flag	Description	Value
<i>LAST_LOGIN_ATTEMPTS</i>	When set to YES, the system displays a record of the last Login of the user in the Main Screen of the RMX Web Client or RMX Manager. Default: YES	YES
<i>MAX_KEEP_ALIVE_REQUESTS</i>	The number of 15-second <i>KeepAliveTimeout</i> request intervals for the Apache server. A value of <b>2880</b> keeps the server alive for 12 hours while a value of <b>5760</b> keeps the server alive for 24 hours. Default: 0 (This value should <b>never</b> be used)	2880
<i>MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM</i>	Determines the maximum number of management sessions per system. Default: 80 Range: 4-80	80
<i>MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER</i>	Determines the maximum number of management sessions per user. Default: 10 Range: 4-80	10
<i>MIN_PASSWORD_LENGTH</i>	Determines the minimum length of a user password. Default: 15 Range: 15-20	15
<i>MIN_PWD_CHANGE_FREQUENCY_IN_DAYS</i>	Determines the minimum number of days that users must retain passwords. Default: 1 Range: 1-7	1
<i>NUMERIC_CHAIR_PASS_MIN_LEN</i>	Determines the minimum length of a user chairperson password. Default: 9 Range: 9-16	9



**Table 1-14** System Flags and their default values

Flag	Description	Value
<i>NUMERIC_CONF_PASS_MIN_LEN</i>	Determines the minimum length of a conference password. Default: 9 Range: 9-16	9
<i>PASSWORD_EXPIRATION_DAYS</i>	Determines the number of days that passwords remain valid. Default: 60 Range: 7-90	60
<i>PASSWORD_EXPIRATION_WARNING_DAYS</i>	Determines how many days before password expiration a warning of pending password expiration will be displayed to the users. Default: 7 Range: 7-14	7
<i>PASSWORD_HISTORY_SIZE</i>	Determines how many previous passwords are recorded to prevent users from re-using previous passwords. The list is cyclic, with the most recently recorded password causing the deletion of the oldest recorded password. Default: 10 Range: 10-16	10
<i>SESSION_TIMEOUT_IN_MINUTES</i>	The number of minutes after which, if there is no input from the user, the user's connection to the RMX is terminated. Default: 15 Range: 1-999	15
<i>USER_LOCKOUT</i>	When this flag is set to YES, a user is locked out of the system after three consecutive Login failures with same User Name. The user is disabled and only the administrator can enable the user within the system. Default: YES	YES



**Table 1-14** System Flags and their default values

Flag	Description	Value
<i>USER_LOCKOUT_DURATION_IN_MINUTES</i>	Determines the time period during which three consecutive Login failures occur that will result in the user being locked out. Default: 0 Range: 0-480	0
<i>USER_LOCKOUT_WINDOW_IN_MINUTES</i>	Determines the time period for which the user is locked out. Default: 60 Range: 0-45000	60

## Modifying Flag Values

System security can be further strengthened by modifying the default flag values. These modified values are applied to the system when the **ULTRA\_SECURE\_MODE** *System Flag* is set to **YES**.

### To modify the system configuration flags:

- 1 On the *RMX* menu, click **Setup > System Configuration**.  
The *System Flags* dialog box opens.
- 2 Locate and double-click on the *System Flag* to be modified.  
The *Update Flag Name* dialog box opens.
- 3 In the *New Value* field, enter the value required for the flag.
- 4 Click the **OK** button to close the *Update Flag Name* dialog box.
- 5 Repeat steps 2 to 4 for each flag value to be modified.
- 6 Click the **OK** button to close the *System Flags* dialog box.
- 7 In the *Reset Confirmation* dialog box, click **Yes**.
- 8 In the *Please wait for system reset* message box, click **OK**.



System restart may take up to five minutes.

- 9 Refresh the browser periodically until the *RMX Web Client – Terms of Usage* screen is displayed.
- 10 Connect to the *RMX*. See “*Connecting to the RMX*” on page [1-43](#).



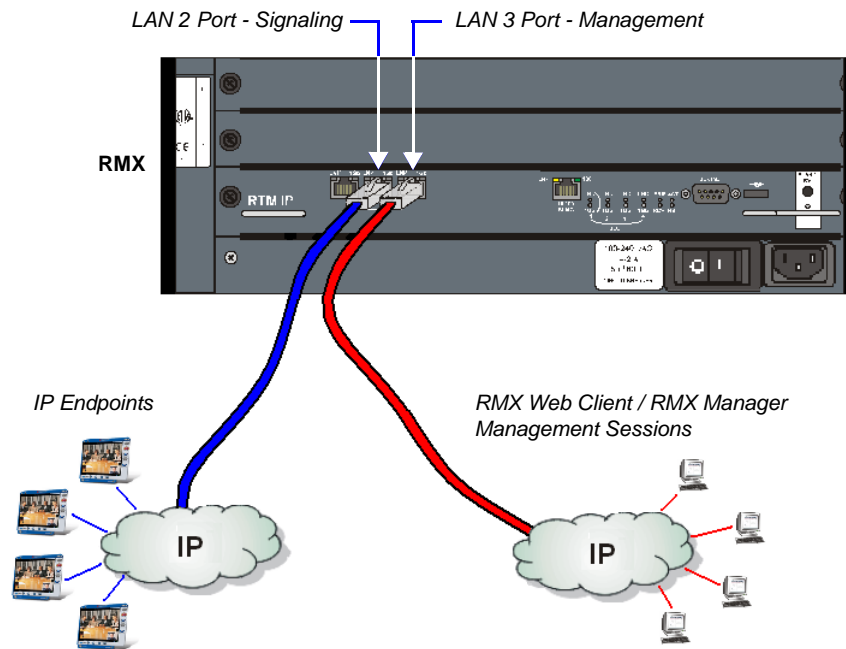
## Procedure 7: Enable Network Separation (RMX 2000)

The RMX 2000, prior to the *Network Separation* procedure, hosts all signaling, management, and media traffic via the LAN 2 port.

*Network Separation* is enabled/disabled according to the setting of the **SEPARATE\_MANAGEMENT\_NETWORK** System Flag. When the System Flag value is **YES**, media and signaling traffic between IP endpoints and the RMX is hosted using the LAN 2 port, while RMX management sessions are hosted using the LAN 3 port.

The RMX 1500 and RMX 4000 are designed with separate ports and networks for signaling, management and media, therefore this flag setting is not relevant. For more information see "RMX 1500 Power, Signaling and Media Cables" on page 1-7 and "RMX 4000 Signaling, Media and Management Cables" on page 1-12.

### Enabling Network Separation





**Figure 2** Signaling and Management Network Separation



**To enable network separation:**

(The **RMX** must be in *Ultra Secure Mode*.)

- 1** On the *RMX* menu, click **Setup > System Configuration**.  
The *System Flags* dialog box opens.
- 2** Locate and double-click on the **SEPARATE\_MANAGEMENT\_NETWORK** *System Flag* entry.  
The *Update Flag Name* dialog box opens.
- 3** In the *New Value* field, enter **YES**.
- 4** Click the **OK** button to close the *Update Flag Name* dialog box.
- 5** Click the **OK** button to close the *System Flags* dialog box.
- 6** In the *Reset Confirmation* dialog box, click **No**.
- 7** In the *RMX Management* pane, click the **IP Network Services** () button.
- 8** In the *IP Network Services* list pane, right-click the **Management Network** () entry and select **Properties**.
- 9** Enter the *Control Unit IP*, *Shelf Management IP* and *Subnet Mask* addresses in their respective field boxes.
- 10** Click the **Routers** tab.
- 11** Enter the *Default Router IP Address*.
- 12** Click the **OK** button.  
A *Reset Confirmation* dialog box is displayed.
- 13** Connect a workstation that is connected to the Management LAN to the *RMX*'s **LAN 3** port.
- 14** In the *Reset Confirmation* dialog box, click **Yes**.



System restart may take up to five minutes.

- 15** On the workstation that was connected to the *RMX* in **Step 13**, start the *RMX Web Client* application:
  - a** In the browser's address line, enter the *Control Unit IP Address* in the format: **https://<Control Unit IP Address>**.
  - b** Press **Enter**.
- 16** Connect to the *RMX*. See "*Connecting to the RMX*" on page **1-43**.



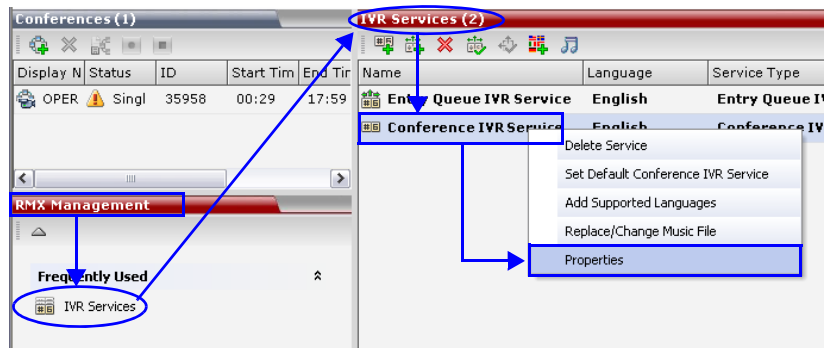
## Procedure 8: Configure IVR Settings.



Perform this procedure if a password is to be used to access the conference, otherwise skip.

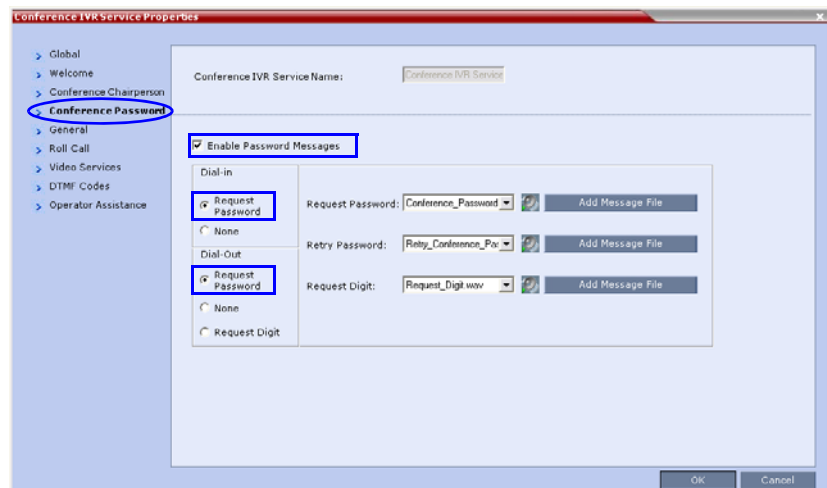
- 1 In the *RMX Management* pane, click **IVR Services**.

The *IVR Services* list opens.



- 2 Right-click the **Conference IVR Service** and select **Properties**
- 3 Click the **Conference Password** tab.

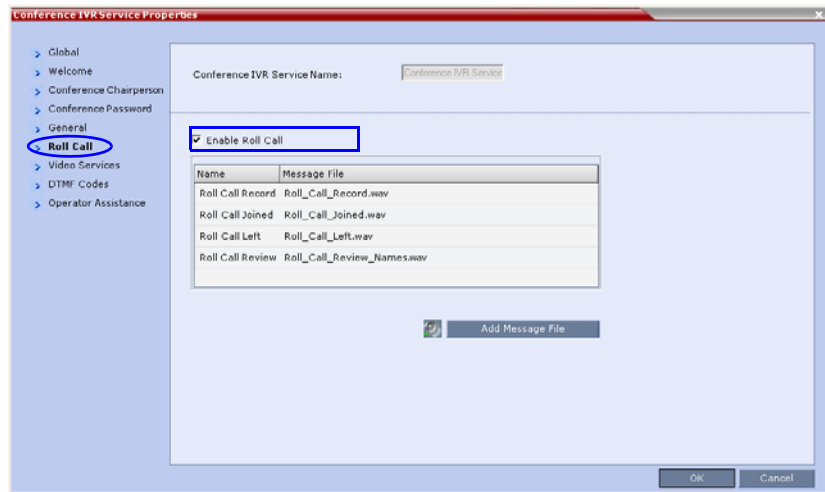
The *Conference IVR Service Properties - Conference Password* dialog box is displayed.





- 4** Select the **Enable Password** messages.
- 5** Set *Dial-in* to **Request Password**
- 6** Set *Dial-Out* to **Request Password**
- 7** Click the **Roll Call** tab.

The *Conference IVR Service Properties - Roll Call* dialog box is displayed.



- 8** Select **Enable Roll Call**.
- 9** Click the **OK** button.



## Procedure 9: Optional. Modify Default Login and Main Screen Banner Text

The *Login* and *Main Screens* of the *RMX Web Client* and the *RMX Manager* display warning text banners cautioning users to the terms and conditions under which they may log into and access the system.

The *Login* and *Main Screen* banners can be enabled when the *RMX* is not in *Ultra Secure Mode* but cannot be disabled when the *RMX* is in *Ultra Secure Mode*.

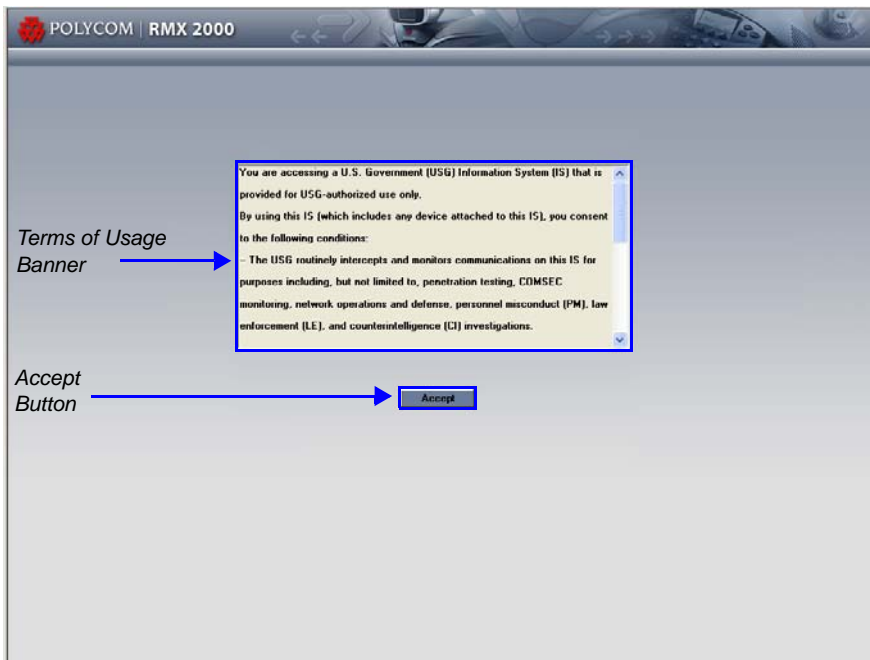
The **ULTRA\_SECURE\_MODE** *System Flag* affects the display of the *Login* and *Main Screen* banners as follows:

- When set to **YES**, the banners cannot be disabled.
- When set to **NO**, banner display is according to the check box selection in the *Banners Configuration* dialog box.



# Login Screen Banner

The *Login* screen banner displays the terms and conditions for system usage as follows:





The default text is:

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

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

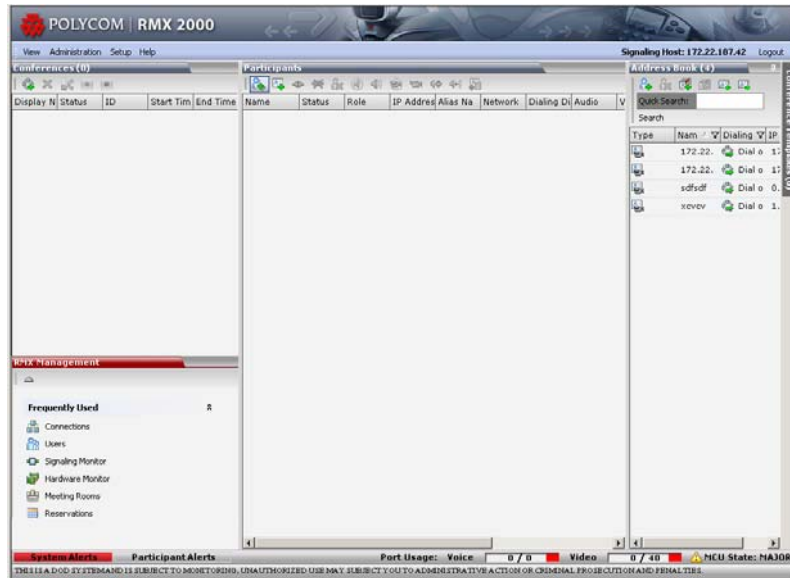
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG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

The user must click the **Accept** button before the *Login* screen is displayed.



## Main Screen Banner

The *Main Screen* banner is displayed at the bottom of the screen. It is initially blank and can be customized



Banner →

## Customizing Login and Main Screen Banners

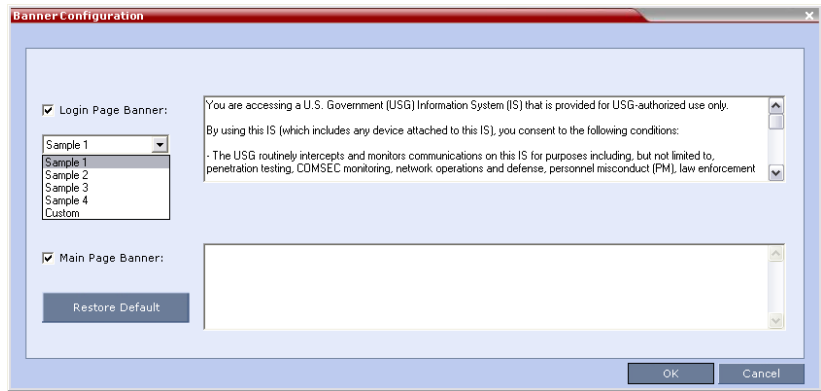
The *Login* and *Main Screen* banners can be customized when the RMX is in either *Ultra Secure Mode* or non-*Ultra Secure Mode*.

To customize the banners:

- 1 In the RMX menu, click **Setup > Customize Display Settings > Banners Configuration**.



The *Banners Configuration* dialog box opens.



- 2 Customize the banners by modifying the following fields:

**Table 1-15** *Banner Configuration*

Field	Description		
	Check Box	Text Field	Restore Default Button
<i>Login Page Banner</i>	Select or clear the check box to enable or disable the display of the banner. Banner display cannot be disabled in Ultra Secure Mode.	Edit the text in this field to meet local requirements: <ul style="list-style-type: none"> <li>Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used.</li> <li>Maximum banner size is 100KB.</li> <li>The banner may not be left blank in Ultra Secure Mode.</li> </ul>	Click the button to restore the default text to the banner.
<i>Main Page Banner</i>			

- 3 Click the **OK** button.



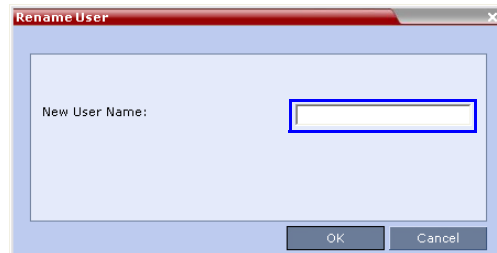
## Procedure 10: Rename the Default POLYCOM User

To rename the default POLYCOM user:

- 1 In the *RMX Management* pane, click the **Users** (👤) button.
- 2 The *Users* pane is displayed.
- 3 Select the **POLYCOM** user.



- 4 Select **Rename User** in the menu.  
The *Rename User* dialog box is displayed.



- 5 Enter a new *User Name* in the *New User Name* field and click **OK**.  
The user is renamed and is forced to change his/her password.

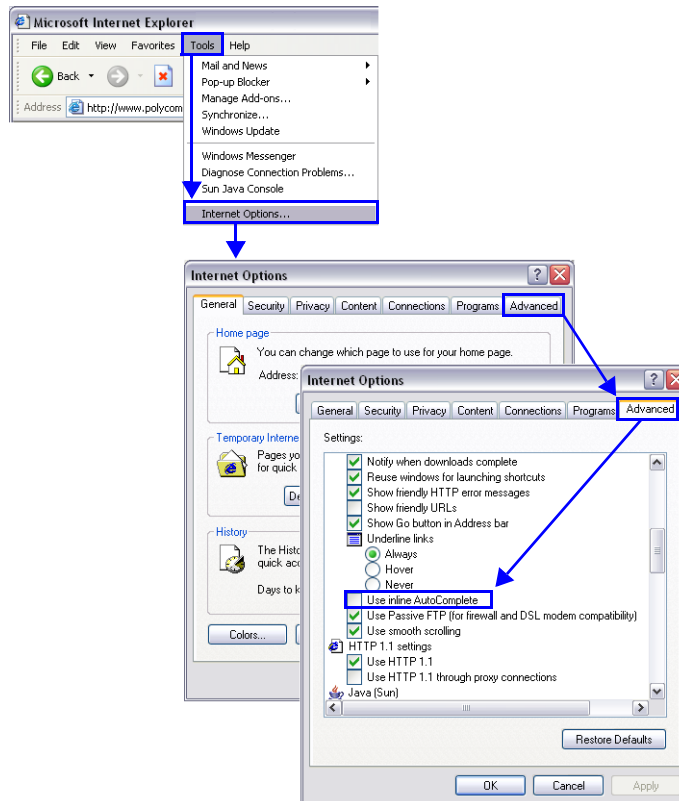


## Procedure 11: Disable Inline AutoComplete Option in Web Browser

To protect both *User Names* and *Passwords* it is recommended to disable the *Inline AutoComplete* option in the web browser on the workstation.

**To disable the Inline AutoComplete option in Internet Explorer®:**

- 1 In the web browser menu, select **Tools > Internet Options**.
- 2 Select the **Advanced** tab.
- 3 Clear the **Use inline AutoComplete** check box.



- 4 Click the **OK** button.



## Procedure 12: Configure an Inbound and Outbound Access List

For security reasons it is important that an *Access Control List* is configured for both inbound and outbound network traffic on the switch port that the *RMX Management Network (LAN 3 port)* is connected to. The format and configuration method of the *Access Control List* will vary depending on the type of switch that is used.



## Antivirus

*McAfee® SDK Antivirus*, included in this version, can be enabled/disabled, updated and scanning times can be set and scheduled.

The *McAfee® SDK Antivirus* application scans the following types of files:

- All files that are sent and loaded to the RMX
- All RMX versions
- IVR files
- TLS certificates
- *Restore* and *Backup* configuration files

## Guidelines

- *McAfee® SDK Antivirus* is supported in *Ultra Secure Mode*.
- *Audit* files entries resulting from *Antivirus* scans are time stamped in GMT.
- *Zip* files cannot be un compressed.
- RMX 2000's with 512Mb Control Units are not supported.

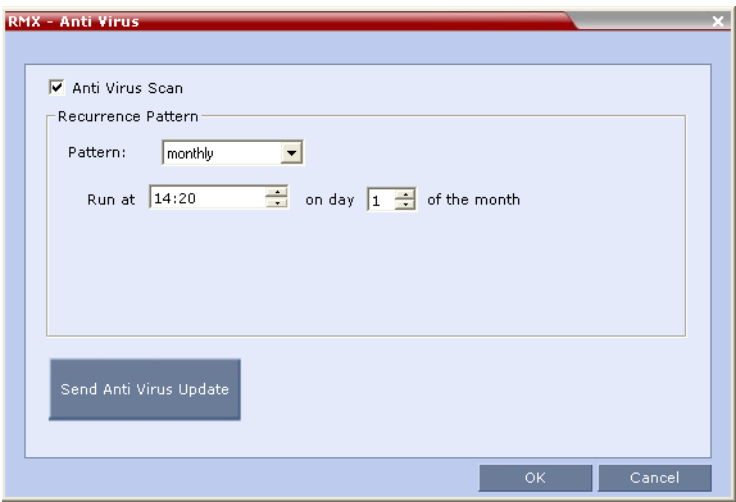
## Scheduling

The *McAfee® SDK Antivirus* application must be enabled and scheduled by an administrator or a user with administrator permissions.

- 1** To enable/disable the Antivirus Application/Scan:
- 2** In the *Setup* menu, click **Antivirus** to open the *Antivirus* dialog box.
- 3** Enable/Disable the Antivirus application/scan by selecting the **Anti Virus Scan** check box. When enabled and a scan is not

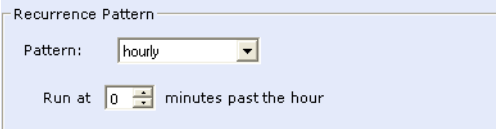


scheduled, the system will initiate based on the default setting.



- 4 When enabled, adjust the antivirus scheduling by modifying the fields as described in Table 1-16.

**Table 1-16** Antivirus – Scheduling

Field	Description	
Recurrence Pattern	Hourly	If <i>hourly</i> is selected, then choose the <i>minutes past the hour</i> to run the antivirus application. 



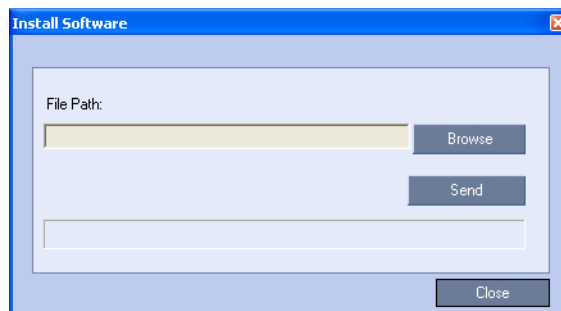
**Table 1-16** Antivirus – Scheduling

Field	Description	
Recurrence Pattern (cont.)	Daily	<p>If <i>Daily</i> is selected, choose the day of the week to run the antivirus application.</p> <p>Pattern: <input type="text" value="daily"/></p> <p>Run at <input type="text" value="15:35"/> every:</p> <p> <input type="checkbox"/> Sunday           <input type="checkbox"/> Monday           <input type="checkbox"/> Tuesday           <input type="checkbox"/> Wednesday           <input type="checkbox"/> Thursday           <input type="checkbox"/> Friday           <input type="checkbox"/> Saturday         </p>
	Monthly	<p>Select the day (1-31) of the month to run the antivirus application.</p> <p>Recurrence Pattern</p> <p>Pattern: <input type="text" value="monthly"/></p> <p>Run at <input type="text" value="09:32"/> on day <input type="text" value="0"/> of the month</p>

### Update the Antivirus DAT file

For more information see “Antivirus Updates” on page 1-70.

- Click **Send Aniti Virus Update** to open the *Install Software* dialog box.



- Click **Browse** and determine the file location and then select the file.



The McAfee file is converted automatically to a TAR file with a .tgz file extension.



- 7** Click **Send** to install the file. When uploaded, the DAT file is checked and verified on the RMX.
  - a** If the file is found to be invalid, an error message “*The DAT file is invalid*” appears on screen.
  - b** Reload the DAT file.
- 8** Click **Close**.



- Schedule anti-virus scans in accordance with your site policies.
- Anti-virus scans impose a significant burden on the system that could impact system performance. Schedule system scans for times when the system is in maintenance mode or when little or no conferencing activity is anticipated.

## Scan Results

If a virus is detected an *Active Alarm* is triggered: “*Antivirus detected: <text from Antivirus>*”.

Reset the RMX to remove or cancel the *Active Alarm*. When a new scan is initiated and the antivirus warning has not been removed the *Active Alarm* is reactivated.

In the *Faults* list when the *Antivirus* scan activates the following message appears: “*Antivirus scan running*”.

Upon completion of the scan the *Fault* list displays a follow-up message: “*Antivirus scan completed*”.

## Antivirus Updates

The administrator must manually update the .dat file, containing signature file updates, of the McAfee® SDK Antivirus application. This DAT file must be retrieved from the official McAfee® web site at the following web address:















**<http://update.nai.com/Products/CommonUpdater>**

Locate the 75+ Mb file: **avvdat-xxxx.zip**

For example: **avvdat-6194.zip**



## Index of /Products/CommonUpdater

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">current/</a>	03-Sep-2010 15:59	-	
 <a href="#">61596160avv.gem</a>	11-Dec-2010 11:11	79K	
 <a href="#">61856186avv.gem</a>	11-Dec-2010 11:11	29K	
 <a href="#">61866187avv.gem</a>	11-Dec-2010 11:11	170K	
 <a href="#">61876188avv.gem</a>	11-Dec-2010 11:11	51K	
 <a href="#">61886189avv.gem</a>	11-Dec-2010 11:11	57K	
 <a href="#">61896190avv.gem</a>	11-Dec-2010 11:11	65K	
 <a href="#">61906191avv.gem</a>	11-Dec-2010 11:11	43K	
 <a href="#">61916192avv.gem</a>	11-Dec-2010 11:11	108K	
 <a href="#">61926193avv.gem</a>	11-Dec-2010 11:11	112K	
 <a href="#">61936194avv.gem</a>	11-Dec-2010 11:10	116K	
 <a href="#">avvdat-6194.zip</a>	11-Dec-2010 11:10	75M	
 <a href="#">avvdat.ini</a>	11-Dec-2010 05:40	3.4K	

This zip file is regularly updated at McAfee® web site. Installing the file overwrites the current installed file and this file can be updated even if the antivirus application is scanning the system.

During every scan, the RMX system checks if there is a DAT file update. When the DAT file is not updated in the past 30 days, an active alarm is triggered: “Antivirus initial DAT files are outdated and must be updated”. This alarm appears in the *Active Alarms* list. The active alarm terminates when the antivirus scan activates.

### Downloading and Converting the ZIP file to TAR

Download the zip file to a local PC/laptop. The McAfee file is automatically converted to a TAR file with a .tgz file extension..



Schedule signature file updates in accordance with your site policies.



# Active Alarms

Table 1-17 lists the Active Alarms that can occur on the system.

**Table 1-17** *Antivirus Active Alarms*

Active Alarm	Description
Virus scan in progress	RMX system is running a virus scan.
Invalid DAT (virus database) file	The DAT file downloaded onto the system is corrupt or invalid. Upload the file again.
A virus threat has been detected	A virus has been detected on the RMX.
Virus scan has been terminated by time-out	The Virus scan was terminated by a time-out on the RMX system.
Antivirus initial DAT files are outdated and must be updated	The Antivirus initial DAT files are outdated and must be updated on the RMX system.

# Logger File Additions

New antivirus statuses have been added to registry of the *Logger Utility*. The following new antivirus statuses are written to the logger file:

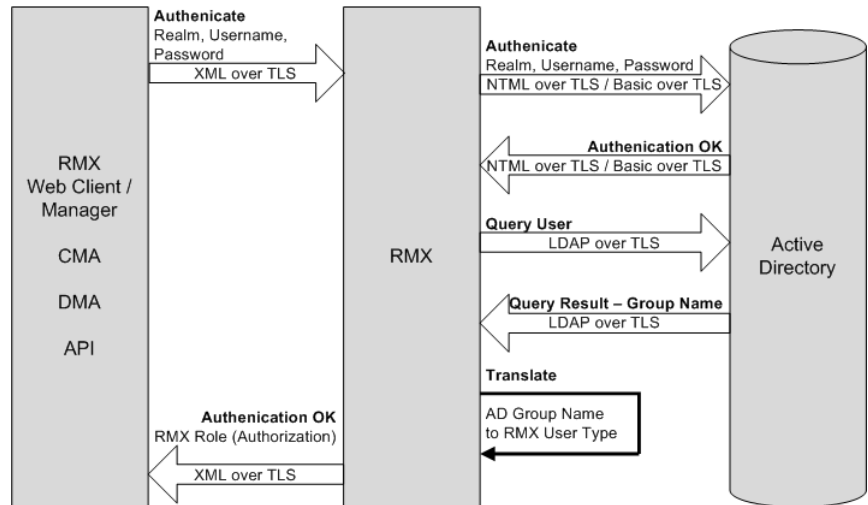
- Scan start
- Scan end
- Scan schedule
- Scan schedule change
- Virus found
- DAT file update
- Any *Antivirus* alert



## Integration with Microsoft® Active Directory™

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

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



## Internal RMX Database and Active Directory in Ultra Secure Mode

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

### Guidelines

- The *RMX* maintains a local record of:
  - Audit Events* – users that generate these events are marked as being either internal or external.
  - Successful user logins
  - Failed user login attempts



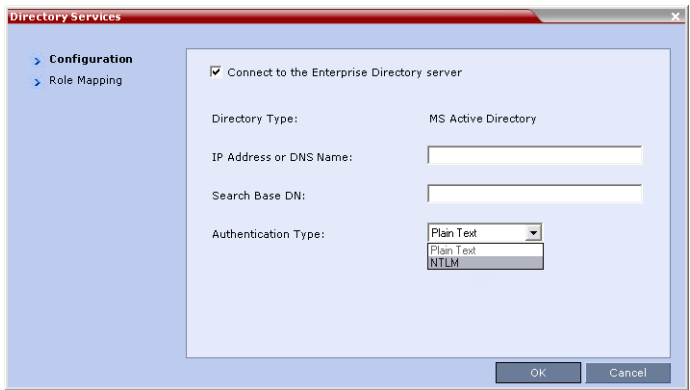
- User passwords and user lockout policy for external users are managed via *Active Directory's* integration with the user's host machine.
- Enabling or disabling *Active Directory* integration does not require a reset.
- Multiple *Machine Accounts* with various roles are supported.
- *Microsoft Active Directory* is the only directory service supported.
- *Active Directory* integration is configured as part of the *Management Network*.
- Both *IPv4* and *IPv6* addressing are supported.

## Enabling Active Directory Integration

To configure Directory Services:

- 1 On the *RMX* menu, click **Setup > Directory Services**.

The *Directory Services - Configuration* dialog box is displayed.



- 2 Modify the following fields.

**Table 1-18** *Directory Services - Configuration*

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

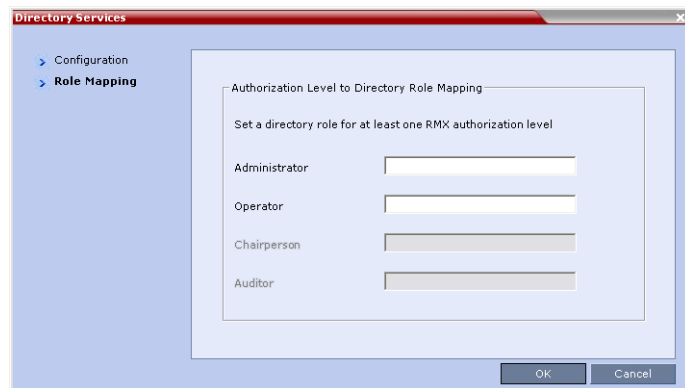


**Table 1-18** Directory Services - Configuration (Continued)

Field	Description
<i>IP Address or DNS Name</i>	Enter the IP address or DNS name of the Enterprise Directory Server (Active Directory).
<i>Search Base DN</i>	Enter the starting point when searching for <i>User</i> and <i>Group</i> information in the <i>Active Directory</i> . For example if the <i>Domain Name</i> is: mainoffice.bigcorp.com.uk The entry in this field should be: CN=Users,DC=mainoffice,DC=bigcorp,DC=come,DC=uk
<i>Authentication Type</i>	Select the <i>Authentication Type</i> from the drop-down menu: <ul style="list-style-type: none"> <li>Plain Text</li> <li>NTLM</li> </ul> <b>Note:</b> NTLM must be selected when working in a secure environment.

**3** Click the **Role Mapping** tab.

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



In *Ultra Secure Mode* there are only two user types: *Administrator* and *Operator*.

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



- An *RMX* user that belongs to multiple *Active Directory Groups* is assigned to the *Group* with the least privileges.
- 4** Map the *RMX User Types*, to their *Active Directory* roles by modifying the following fields.

**Table 1-19** *Directory Services - Role Mapping*

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

- 5** Click **OK**.



---

# Basic Operation

The most common operations performed via the *RMX Web Client* are:

- Starting, monitoring and managing conferences
- Monitoring and managing **participants** and **endpoints** as individuals or **groups**.
  - **Participant** – A person using an endpoint to connect to a conference. When using a *Room System*, several participants use a single endpoint.
  - **Endpoint** – A hardware device, or set of devices, that can call, and be called by an MCU or another endpoint. For example, an endpoint can be a phone, a camera and microphone connected to a PC or an integrated *Room System* (conferencing system).
  - **Group** – A group of participants or endpoints with a common name.

## Starting the RMX Web Client

Before you begin, get the following information from your system administrator:

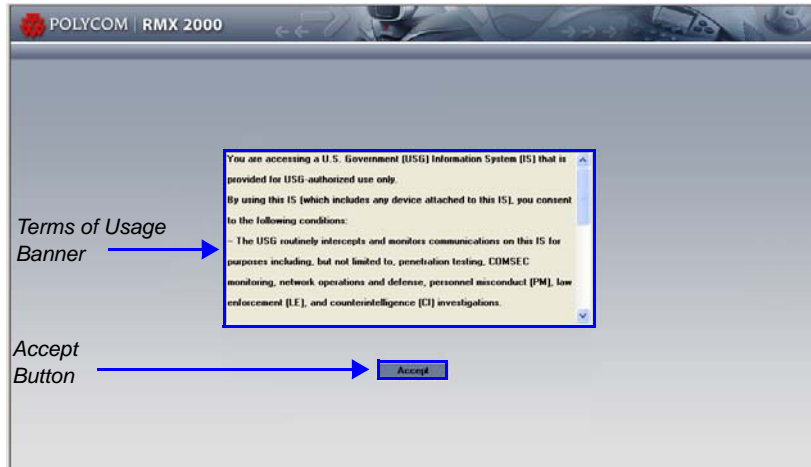
- *Username*
- *Password*
- *MCU Control Unit IP Address*



**To start the RMX 1500/2000/4000 Web Client:**

- 1 In the browser address line, enter **https://<Control Unit IP Address>** and press the **Enter** key.

The *RMX Web Client – Terms of Usage* screen is displayed.



- 2 Click the **Accept** button to agree to the terms and conditions displayed in the banner.

The *Login - Welcome* screen is displayed:



- 3 Enter your *User Name*.
- 4 Enter your *Password*.



**5 Click Login.**

The *RMX Web Client - Main Screen* is displayed.



The *RMX Manager* is faster than the *RMX Web Client* and can give added efficiency to RMX management tasks, especially when deployed on workstations affected by:

- Lack of performance due to bandwidth constraints within the LAN/WAN environment.
- Slow operation and disconnections that can be caused by the anti-phishing component of various antivirus applications.

For more information see "*Installing RMX Manager for Secure Communication Mode*" on page [3-1](#).

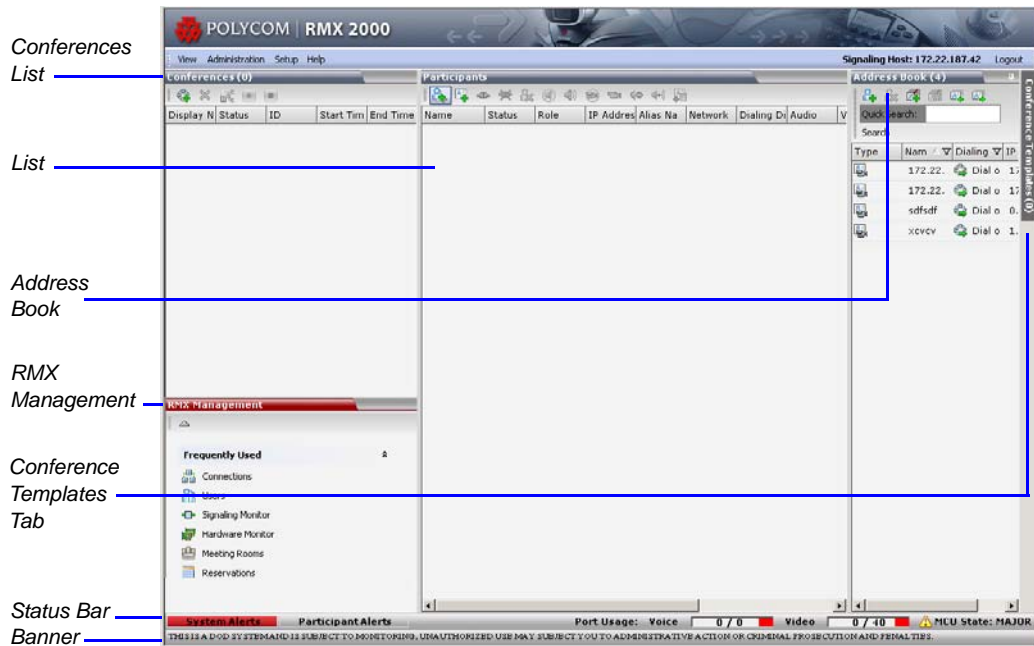


## RMX 1500/2000/4000 Web Client Screen Components

The RMX 1500/2000/4000 Web Client's main screen consists of five panes:

- *Conference List*
- *List Pane*
- *RMX Management*
- *Status Bar*
- *Address Book*
- *Conference Templates*

For more information, see the RMX 1500/2000/4000 Administrator's Guide, "Users, Connections and Notes" on page [10-1](#).



The main screen can be customized. For more information, see "Customizing the Main Screen" on page [2-13](#).



## Viewing and System Functionality Permissions

*Viewing* and *System Functionality* permissions for Administrators and Operators are summarized in Table 2-1:

**Table 2-1** *Viewing and System Permissions*

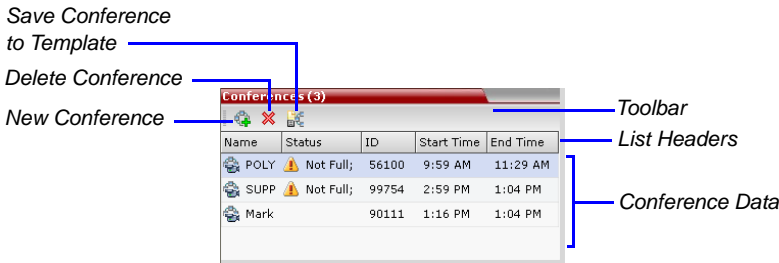
	Authorization Level	
	Operator	Administrator
	Viewing Permissions	
Conference List	✓	✓
List Pane	✓	✓
Address Book	✓	✓
Conference Templates	✓	✓
Status Bar	✓	✓
RMX Management	✓	✓
Conference Alarms	✓	✓
Conference Status	✓	✓
Configurations	✓	✓
	System Functionality	
Start Conferences	✓	✓
Monitor Conferences	✓	✓
Monitor Participants	✓	✓
Solve Basic Problems	✓	✓
Modify MCU Configuration		✓



# Conferences List

If you are logged in as a user with Operator or Administrator permissions:

The *Conferences* pane lists all the conferences currently running on the MCU along with their *Status*, *Conference ID*, *Start Time* and *End Time* data. The number of ongoing conferences is displayed in the pane's title.



The *Conferences* list toolbar contains the following buttons:

- **New Conference** – to start a new ongoing conference.
- **Delete Conference** – delete the selected conference(s).

# List Pane

The *List* pane displays details of the item selected in the *Conferences* pane or *RMX Management* pane. The title of the pane changes according to the selected item.



# RMX Management

The *RMX Management* pane lists the entities that need to be configured to enable the RMX to run conferences. Only users with Administrators permission can modify these parameters.

The *RMX Management* pane is divided into two sections:

- **Frequently Used** – parameters often configured monitored or modified.
- **Rarely Used** – parameters configured during initial system set-up and rarely modified afterward.



## Status Bar

The Status Bar at the bottom of the *RMX Web Client* contains *System* and *Participant Alerts* tabs as well as *Port Usage Gauges* and an *MCU State* indicator.



## System Alerts

This is a list of system problems. The alert indicator flashes red when at least one system alert is active. The flashing continues until a user with Operator or Administrator permission reviews the list.

The *System Alerts* pane is opened and closed by clicking the **System Alerts** button in the left corner of the *Status Bar*.

Active

Alarms

Faults

List

System Alerts (6)						
Time	Category	Level	Code	Process Name	Description	
9/25/2006	general	major	IP_SERVICE_CHANGED	CSMgr	ip service was changed, reset the RMX (Task status: Normal)	
9/13/2006	card	major	NO_CONNECTION_WITH_CARD	Cards	Board ID:0, Card Type:switch, Description: No connection with Switch (Task status: Normal)	
9/13/2006	general	major	INTERNAL_MCU_RESET	McmsDaemo	No connection with Switch (Task status: Normal)	
9/13/2006	general	major	INSUFFICIENT_RESOURCES	Resource	Insufficient resources (Task status: Normal)	
9/13/2006	card	major	CARD_STARTUP_FAILURE	Cards	Board ID:0, Card Type:illegal, Description: MFA startup failure	
9/13/2006	general	major	CFG_CHANGED	McuMgr	SYSTEM CFG was changed, reset the RMX (Task status: Normal)	

For more information about **Active Alarms** and **Faults List**, see the *RMX 1500/2000/4000 Administrator's Guide, "System and Participant Alerts"* on page [14-18](#).

## Participant Alerts

This is a list of participants that are experiencing connection problems. It is sorted by conference.

The *Participant Alerts* pane is opened and closed by clicking the **Participant Alerts** button in the left corner of the *Status Bar*.

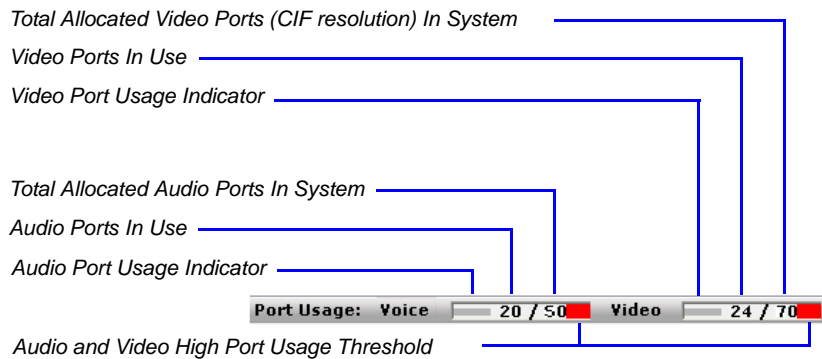
Participant Alerts (2)										
Conference	Name	Status	Disconnection Time	Role	IP Address	Alias	Network	Dialing Direction	Audio	Video
Marketing	V69	discon	9/21/2006 2:18 PM		172.22.189	H.323		Dial out		
Marketing	V96	discon	9/21/2006 2:18 PM		172.22.186	H.323		Dial out		



## Port Usage Gauges

The *Port Usage* gauges indicate:

- The total number of *Video* or *Voice* ports in the system according to the *Video/Voice Port Configuration*.
- The number of *Video* and *Voice* ports in use.
- The *High Port Usage* threshold.




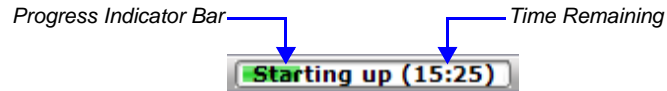
The *High Port Usage* threshold represents a percentage of the total number of video or voice ports available. It is set to indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes and a *System Alert* is generated. The default port usage threshold is 80% and it can be modified by the system administrator. For more information, see the *RMX 1500/2000/4000 Administrator's Guide for Maximum Security Environments*, "Setting the Port Usage Threshold" on page 14-60.





## MCU State

The *MCU State* indicator displays one of the following:

-  – The MCU is starting up. The time remaining until the system start-up is complete is displayed between brackets while a green progress indicator bar indicates the start-up progress.



-  – The MCU is functioning normally.
-  – The MCU has a major problem. MCU behavior could be affected and attention is required.

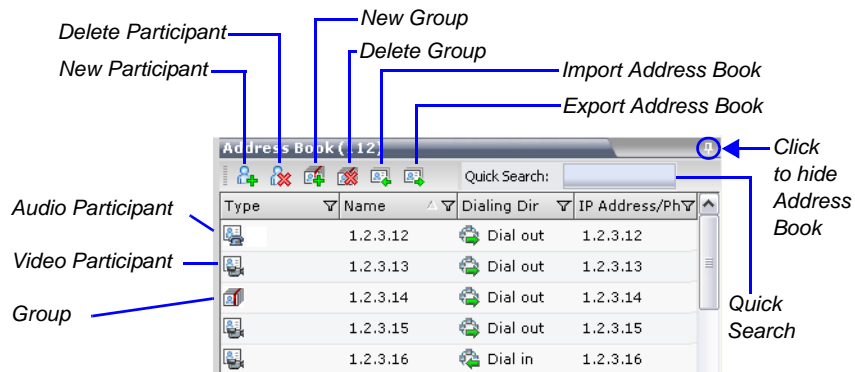


## Address Book

The *Address Book* is a list of *Participants* and *Groups* that have been defined on the RMX. The information in the *Address Book* can be modified only by an administrator. All RMX users can, however, view and use the *Address Book* to assign participants to conferences.

The *Address Book* toolbar contains a *Quick Search* field and the following six buttons:

- *New Participant*
- *Delete Participant*
- *Import Address Book*
- *New Group*
- *Delete Group*
- *Export Address Book*



*Address Book* entries are listed according to:

- **Type** - whether an individual *Participant* or a *Group* of participants
- **Name** - of the participant or group
- **Dialing Direction** - Dial-in or Dial-out
- **IP Address/Phone** - of the participant



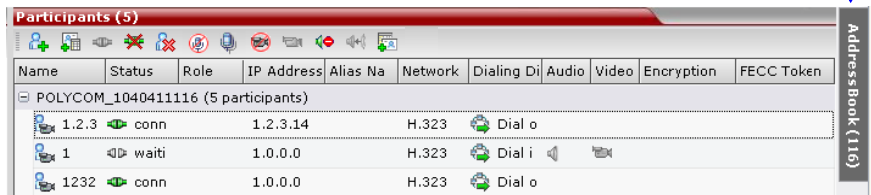
## Displaying and Hiding the Address Book

The first time you access the *RMX Web Client*, the *Address Book* pane is displayed. You can hide it by clicking the anchor pin (📌) button.

The *Address Book* pane closes and a tab appears at the right edge of the screen.

Click the tab to re-open the *Address Book*.

Click tab to open Address Book



## Conference Templates

*Conference Templates* enable administrators and operators to create, save, schedule and activate identical conferences.

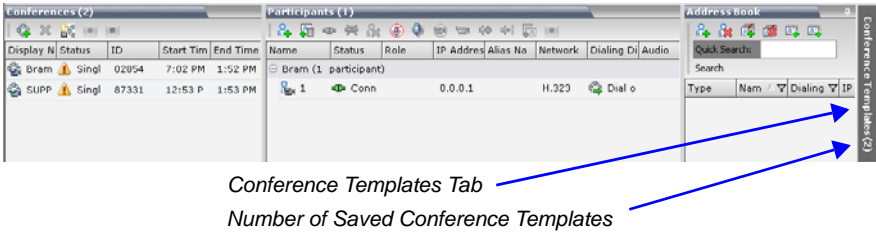
A *Conference Template*:

- Saves conference and Operator conference Profiles.
- Saves all participant parameters including their *Personal Layout* and *Video Forcing* settings.
- Simplifies the setting up *Telepresence* conferences where precise participant layout and video forcing settings are crucial.

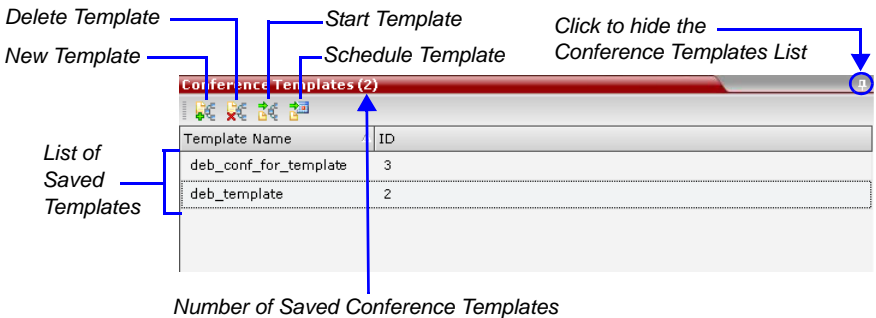


## Displaying and Hiding Conference Templates

The *Conference Templates* list pane is initially displayed as a closed tab in the *RMX Web Client* main window. The number of saved *Conference Templates* is indicated on the tab.



Clicking the tab opens the *Conference Templates* list pane.



Hide the *Conference Templates* list pane by clicking the anchor pin (📌) button in the top right corner of the pane.

The *Conference Templates* list pane closes and a tab appears in the top right corner of the screen.




## Customizing the Main Screen

You can customize the main screen according to your preferences. Pane sizes can be changed, column widths can be adjusted and data lists can be sorted.




Customization settings are automatically saved for each logged-in user. The next time the *RMX Web Client* is opened, the main screen settings appear as they were when the user exited the application.



### To re-size a pane:

- >> Move the pointer over the pane border and when the pointer becomes a  click and drag the pane border to the required size and release the mouse button.

### To adjust column width:

- 1 In the column header row, place the pointer on the vertical field-separator bar of the column.
- 2 When the pointer becomes a , click and drag the field separator bar to the required column size and release the mouse button.

### To sort the data by any field (column heading):

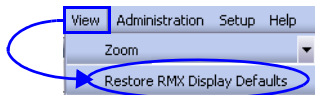
- 1 In the *Conference* list or *List* view pane, click on the column heading of the field to be used for sorting.  
A  or  symbol appears in the column heading indicating that the list is sorted by this field, as well as the sort order.
- 2 Click on the column heading to toggle the column's sort order.

### To change the order of columns in a pane:

- >> Click the column heading to be moved and drag it to its new position. When a set of red arrows appears indicating the column's new position, release the mouse button.

### To restore the RMX 1500/2000/4000 display window to its default configuration:

- >> On the *RMX 1500/2000/4000* menu, click **View > Restore RMX Display Defaults**.





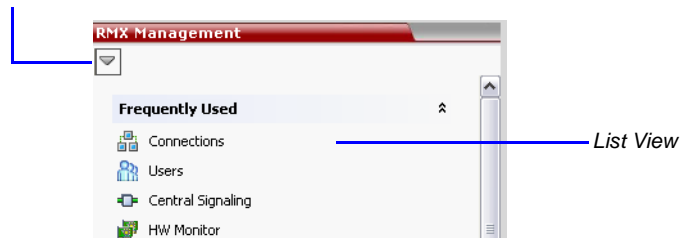
## Customizing the *RMX Management* Pane

The *RMX Management* pane can be viewed either as a list or as a toolbar.

### To switch between Toolbar and List Views:

- >> In the *RMX Management* pane, click the *Toolbar View* button to switch to Toolbar view.
- >> In Toolbar view, click the *List View* button to switch back to List view.

*Toolbar View Button*





*List View Button*



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


This only works in *List* view because in *Toolbar* view, all items are represented by icons.

### To expand or Collapse the Frequently Used and Rarely Used sections:

The *Frequently Used* and *Rarely Used* sections can be expanded or collapsed by clicking the  and  buttons.

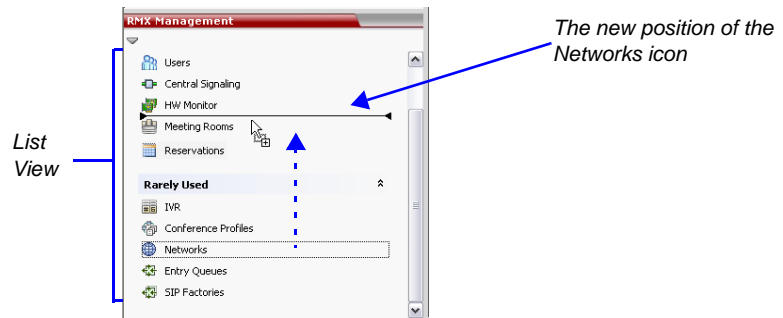
### To move items within and between the Frequently Used and Rarely Used sections:

- 1 In the *RMX Management* pane click and drag the icon of the item that you wish to move.

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



- 2 Release the mouse button when the icon is in the desired position.





## Starting a Conference

There are several ways to start a conference:

- Clicking the *New Conference* button in the *Conferences* pane. For more information, see "*Starting a Conference from the Conferences Pane*" on page [2-17](#).
- Dialing in to a *Meeting Room*.

- A *Meeting Room* is a conference that is saved on the MCU. It remains in passive mode until it is activated by the first participant, or the meeting organizer, dialing in.

For more information about Meeting Rooms, see the *RMX 1500/2000/4000 Administrator's Guide*, "*Meeting Rooms*" on page [3-1](#).

- Dialing in to an *Ad Hoc Entry Queue* which is used as the access point to the MCU.

For a detailed description of *Ad Hoc Entry Queues*, see the *RMX 1500/2000/4000 Administrator's Guide*, "*Entry Queues, Ad Hoc Conferences and SIP Factories*" on page [4-1](#).

- Start a *Reservation*:
  - If the *Start Time* of the *Reservation* is past due the conference becomes ongoing immediately.
  - If the *Start Time* of the *Reservation* is in the future the conference becomes ongoing, at the specified time on the specified date.

For more information, see "*Starting a Reservation*" on page [2-27](#).

- Start from any Conference Template saved in the *Conference Templates* list.

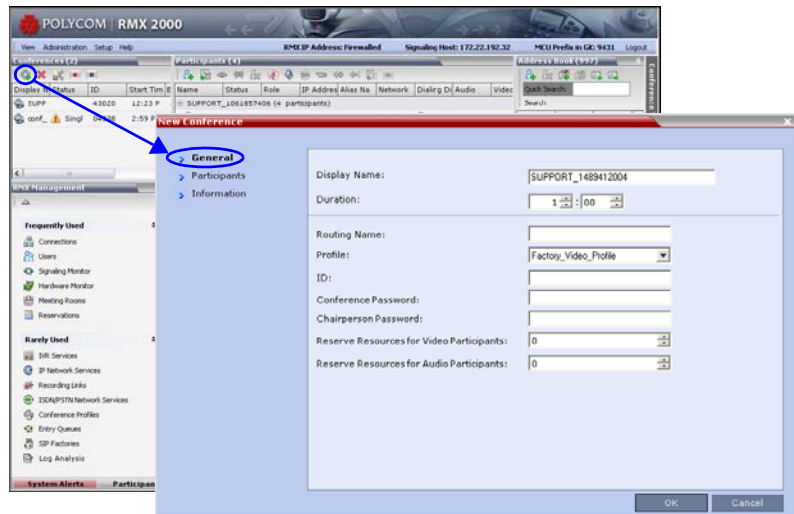


## Starting a Conference from the Conferences Pane

To start a conference from the Conference pane:

- 1 In the *Conferences* pane, click the **New Conference** (🌐) button.

The *New Conference – General* dialog box opens.



The system displays the conference's default *Name*, *Duration* and the default *Profile*, which contains the conference parameters and media settings.

The RMX automatically allocates the conference *ID*, when the conference starts.

In most cases, the default conference *ID* can be used and you can just click **OK** to launch the conference. If required, you can enter a conference *ID* before clicking **OK** to launch the conference.

You can use the *New Conference – General* dialog box to modify the conference parameters. If no defined participants are to be added to the conference, or you do not want to add additional information, click **OK**.



## General Tab

**2** Define the following parameters:

**Table 2-2** New Conference – General Options

Field	Description
<i>Display Name</i>	<p>The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Web Client.</p> <p>In conferences, Meeting Rooms and Entry Queues the system automatically generates an ASCII name for the <i>Display Name</i> field that can be modified using Unicode encoding.</p> <ul style="list-style-type: none"><li>• English text uses ASCII encoding and can contain the most characters (length varies according to the field).</li><li>• European and Latin text length is approximately half the length of the maximum.</li><li>• Asian text length is approximately one third of the length of the maximum.</li></ul> <p>The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII).</p> <p>Maximum field length in ASCII is 80 characters.</p> <p>If the same name is already used by another conference, Meeting Room or Entry Queue, the RMX displays an error message requesting you to enter a different name.</p> <p><b>Note:</b> This field is displayed in all tabs.</p>
<i>Duration</i>	<p>Define the duration of the conference in hours using the format HH:MM (default 01:00).</p> <p><b>Note:</b> This field is displayed in all tabs.</p>



**Table 2-2** New Conference – General Options (Continued)

Field	Description
<i>Routing Name</i>	<p><i>Routing Name</i> is the name with which ongoing conferences, Meeting Rooms and Entry Queues register with various devices on the network such as gatekeepers. This name must be defined using ASCII characters.</p> <p><b>Comma, colon and semicolon characters cannot be used in the <i>Routing Name</i>.</b></p> <p>The <i>Routing Name</i> can be defined by the user or automatically generated by the system if no <i>Routing Name</i> is entered as follows:</p> <ul style="list-style-type: none"> <li>• If ASCII characters are entered as the <i>Display Name</i>, it is used also as the <i>Routing Name</i></li> <li>• If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the <i>Display Name</i>, the <i>ID</i> (such as Conference ID) is used as the <i>Routing Name</i>.</li> </ul> <p>If the same name is already used by another conference, Meeting Room or Entry Queue, the RMX displays an error message and requests that you to enter a different name.</p>
<i>Profile</i>	<p>The system displays the name of the default Conference Profile. Select the required Profile from the list.</p> <p>The Conference Profile includes the Conference line rate, media settings and general settings.</p> <p>For a detailed description of Conference Profiles, see the <i>RMX 1500/2000/4000 Administrator's Guide</i>, "Conference Profiles" on page 1-1.</p>
<i>ID</i>	<p>Enter the unique-per-MCU conference ID. If left blank, the MCU automatically assigns a number once the conference is launched.</p> <p>This ID must be communicated to conference participants to enable them to dial in to the conference.</p>



**Table 2-2** New Conference – General Options (Continued)

Field	Description
<i>Conference Password</i>	<p>Enter a password to be used by participants to access the conference. If left blank, no password is assigned to the conference.</p> <p>This password is valid only in conferences that are configured to prompt for a conference password.</p>
<i>Chairperson Password</i>	<p>Enter a password to be used by the RMX to identify the <i>Chairperson</i> and grant him/her additional privileges. If left blank, no chairperson password is assigned to the conference.</p> <p>This password is valid only in conferences that are configured to prompt for a chairperson password.</p>
<i>Reserve Resources for Video Participants</i>	<p>Enter the number of video participants for which the system must reserve resources.</p> <p>Default: 0 participants.</p> <p>Maximum: 80 participants.</p>
<i>Reserve Resources for Audio Participants</i>	<p>Enter the number of audio participants for which the system must reserve resources.</p> <p>Default: 0 participants.</p> <p>Maximum: 120 participants.</p>

- 3** If all participants are undefined, dial-in and no additional information is required for the new conference, click **OK**.
- 4** To add participants from the *Participants Address Book* or to define participants (mainly dial-out participants) click the *Participants* tab.



## Participants Tab



This procedure is optional.

The *Participants* tab is used to add participants to the conference from the *Address Book*.

It is also used to add defined dial-out participants to the conference. Defined dial-out participants are connected to the conference automatically when the conference is launched

### 5 Click the **Participants** tab.

The *Participants* tab opens.

**New Conference**

> General  
**> Participants**  
> Information

Display Name: SUPPORT\_1291004024

Duration: 1 : 00

*Participants List*

Name	IP Address	Alias Name	Network	Dialing ID	Encryption
------	------------	------------	---------	------------	------------

New Remove Add from Address Book

Lecturer: [Dropdown]

OK Cancel

When defining a new conference, the *Participants List* is empty.



The following table describes the information displayed in the *Participants List* and the operations that can be performed.

**Table 2-3** *New Conference – Participants Tab*

Column / Button	Description
<b>Participants List</b>	
<i>Name</i>	A Unicode field that displays the participant's name and an icon representing the endpoint type: <i>Audio Only</i> or <i>Video</i> .
<i>IP Address/Phone</i>	Indicates the IP address or phone number of the participant's endpoint. <ul style="list-style-type: none"> <li>For dial-out connection, displays the IP address or phone number of the endpoint called by the Polycom RMX 1500/2000/4000.</li> <li>For dial-in connection, displays the participant's IP address or phone number used to identify and route the participant to the appropriate conference.</li> </ul>
<i>Alias Name (IP Only)</i>	Displays the alias name of an H.323 endpoint.
<i>Network</i>	The network communication protocol used by the endpoint to connect to the conference: <i>H.323</i> or <i>ISDN/PSTN</i> .
<i>Dialing Direction</i>	<b>Dial-in</b> – The participant dials in to the conference <b>Dial-out</b> – The RMX dials out to the participant
<i>Encryption</i>	Displays whether the endpoint uses encryption for its media.  The default setting is <i>Auto</i> , indicating that the endpoint must connect according to the conference's encryption setting.



**Table 2-3** *New Conference – Participants Tab (Continued)*

Column / Button	Description
<b>Buttons</b>	
New	Click to define a new participant. For more information, see the <i>RMX 2000/4000 Administrator's Guide for Maximum Security Environments</i> , "Adding a new participant to the Address Book Directly" on page 5-4.
Remove	Click to remove the selected participant from the conference.
Add from Address Book	Click to add a participant from the <i>Address Book</i> to the conference.
<i>Lecturer</i>	This option is used to activate the <i>Lecture Mode</i> . Select the participant you want to designate as <i>Lecturer</i> from the drop-down menu list of conference participants.

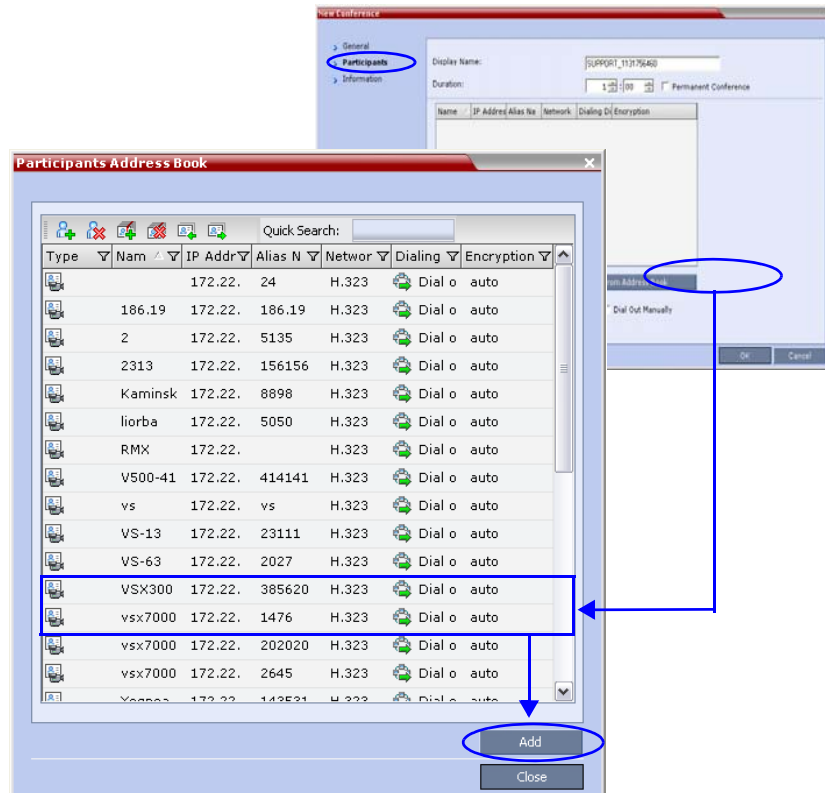
Participants can be added to the conference in the following methods:

- Defining a new participant during the definition of the conference (clicking the New button).
- Adding pre-defined participants from the *Address Book* by either selecting the participants from the list or dragging and dropping the participants from the *Address Book* to the Participants list.
- Dial-in participants can connect to the conference after it was started (without using the New Conference - Participants dialog box).
- Once the conference has started, participants can be added to a conference directly from the *Participants Address Book* without having to use the *New Conference – Participants* tab. For more details, see "Adding Participants from the Address Book" on page 2-48.



### To add participants from the Address Book:

- 6 In the *Participants List*, click the **Add from Address Book** button to open the *Participants Address Book*.



- 7 In the *Participants Address Book*, select the participants that you want to add to the conference and click the **Add** button.

Standard Windows multiple selection techniques can be used in this procedure.

- 8 The selected participants are assigned to the conference and appear in the *Participant List*.
- 9 Select additional Participants or click the **Close** button to return to the *Participants* tab.



## Information Tab

In the *Info* fields, you can add general information about the conference, such as contact person name, company name, billing code, etc.

This information is written to the *Call Detail Record (CDR)* when the conference is launched.

Changes made to this information once the conference is running are **not** saved to the *CDR*.



This procedure is optional.

The information entered into these fields does not affect the conference.

### To add information to the conference:

- 10 Click the **Information** tab.

The *Information* tab opens.

The screenshot shows a web interface titled "New Conference". On the left, there is a sidebar with three tabs: "General", "Participants", and "Information". The "Information" tab is selected and highlighted with a blue oval. The main content area on the right contains the following fields:

- Display Name:** A text box containing "SUPPORT\_472738258".
- Duration:** A time selector showing "1" hour and "00" minutes, with a "Permanent Conference" checkbox to its right.
- Info1:** A text input field.
- Info2:** A text input field.
- Info3:** A text input field.
- Billing Info:** A text input field.



**11** Enter the following information:

**Table 2-4** *New Conference – Info Options*

Field	Description
<i>Info1, 2, 3</i>	There are three information fields that allow you to enter general information for the conference such as company name, contact person etc. Unicode can be used in these fields. The maximum length of each field is 80 characters.
<i>Billing</i>	Enter the conference billing code if applicable.

**12** Click **OK**.

An entry for the new conference appears in the *Conferences* pane.

If an ISDN/PSTN dial-in number was assigned to the conference either automatically or manually, this number can be viewed in the *Conferences* pane.

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

The status changes when participants connect to the conference.

If no participant connects within the time specified in the *Conference Profiles > Auto Terminate > Before First Joins* field, the conference is automatically terminated by the system.

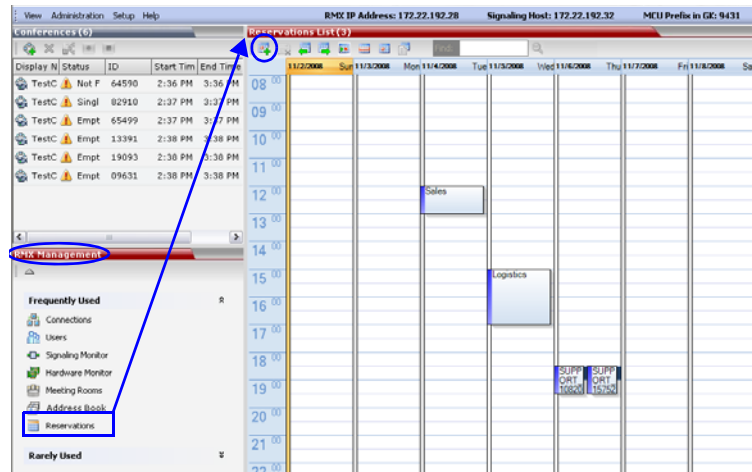


## Starting a Reservation

To start a conference from the Reservation Calendar:

- 1 In the *RMX Management* pane, click the *Reservation Calendar* button (📅).

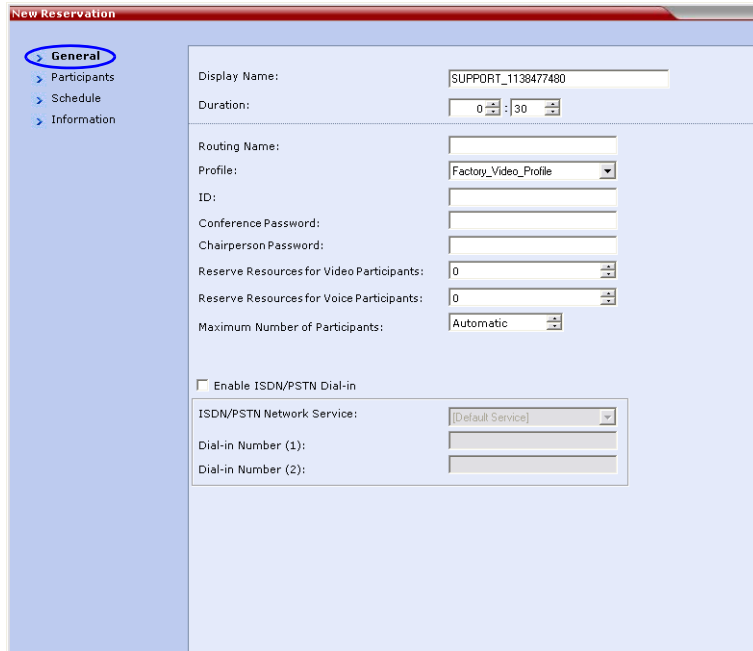
The *Reservation Calendar* is displayed.



- 2 Click the **New Reservation** (📅+) button.



The *New Reservation – General* tab dialog box opens.



**New Reservation**

- General**
- Participants
- Schedule
- Information

Display Name: SUPPORT\_1138477480

Duration: 0:30

Routing Name:

Profile: Factory\_Video\_Profile

ID:

Conference Password:

Chairperson Password:

Reserve Resources for Video Participants: 0

Reserve Resources for Voice Participants: 0

Maximum Number of Participants: Automatic

☐ Enable ISDN/PSTN Dial-in

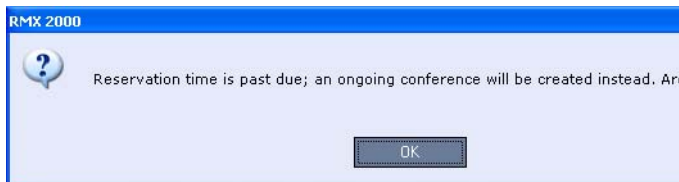
ISDN/PSTN Network Service: [Default Service]

Dial-in Number (1):

Dial-in Number (2):

- 3 Optional.** Select the **Enable ISDN/PSTN Dial-in** check box if you want ISDN and PSTN participants to be able to connect directly to the conference.
- 4** If *Enable ISDN/PSTN Dial-in* option is selected, either enter a dial-in number, or leave the *Dial-in Number* field blank to let the system automatically assign a number from the dial-in range defined for the selected ISDN/PSTN Network Service.
- 5** Click the **OK** button.

A confirmation box is displayed stating that the *Reservation* time is past due and that the conference will become ongoing.





**6** Click the **OK** button.

The conference is started. If an ISDN/PSTN dial-in number was assigned to the conference either automatically or manually, this number can be viewed in the *Conferences* pane.

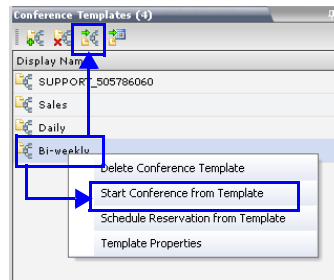
For more information about *Reservations*, see the *RMX 1500/2000/4000 Administrator's Guide, "Reservations"* on page 6-1.

## Starting an Ongoing Conference From a Template

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

**To start an ongoing conference from a Template:**

- 1** In the *Conference Templates* list, select the Template you want to start as an ongoing conference.
- 2** Click the **Start Conference from Template** (🔗) button.  
or  
Right-click and select **Start Conference from Template**.



The conference is started.



If a Conference Template is assigned a dial-in number that is already assigned to an ongoing conference, Meeting Room, Entry Queue or Gateway Profile, when the template is used to start an ongoing conference or schedule a reservation it will not start. However, the same number can be assigned to several conference templates provided they are not used to start an ongoing conference at the same time. If a dial in number conflict occurs prior to the conference's start time, an alert appears: "ISDN dial-in number is already assigned to another conferencing entity" and the conference cannot start.

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



Participants that are connected to other ongoing conferences when the template becomes an ongoing conference are not connected.



If an ongoing conference, Meeting Room or Entry Queue with the same *Display Name*, *Routing Name* or *ID* already exist in the system, the conference will not be started.

For detailed description of Conference Templates, see *RMX 2000 Administrator's Guide for Maximum Security Environments*, "Conference Templates" on page [7-1](#).

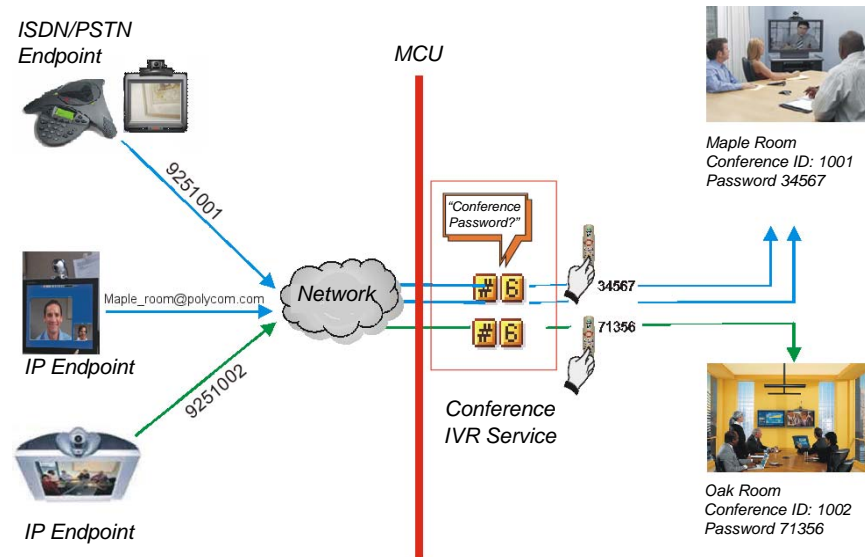


# Connecting to a Conference

## Direct Dial-in

Participants must be provided with a dialing string which can vary according to the network type, conference password and chairperson password.

Participants dial the conference dial-in string and are connected to the conference *IVR Service*. Once the correct information, such as the conference password and chairperson password are entered, the participants are connected to the conference.



*Dial-in Connection via IVR System*

The chairperson can use the chairperson password as the conference password and does not need to enter the conference password.



Participants connecting to HD Video Switching conferences must have HD capable endpoints and must connect using the same line rate as defined for the conference. If not, they are connected as Secondary (audio only participants).



## H.323 Participants

For *H.323* participants, the dialing string is composed of the MCU prefix in the Gatekeeper and the Conference ID.

**Example:**

Prefix in gatekeeper	925
Conference ID	1001
Conference Name	Maple_Room

>> The participant dials 9251001 or 925Maple\_room

If there is no gatekeeper defined for the network, *H.323* participants dial the MCU's signaling host IP address and the conference ID, separated by ##.

**Example:**

MCU (Signaling Host) IP address	172.22.30.40
Conference ID	1001

>> The participant dials 172.22.30.40##1001



## Entry Queue Access

Access via an Entry Queue allows all participants to dial the same entry point that acts as a routing lobby. Once in the Entry Queue, participants are guided to the conference according to the conference ID they enter.

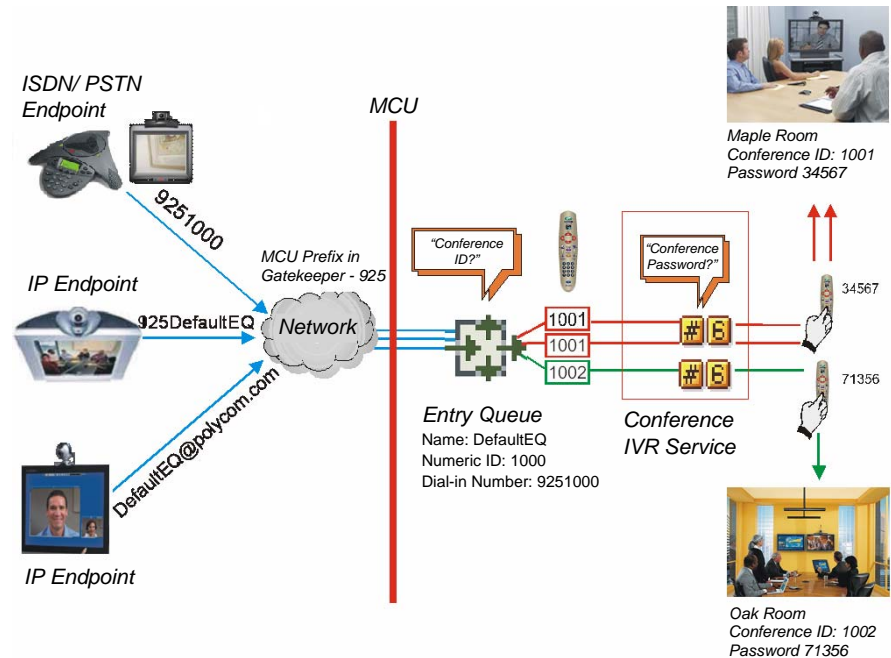


Figure 2-1: Dial-in Connection via Entry Queue

Dialing is executed in the same way as for conferences, where the Entry Queue ID/Name replaces the Conference ID/Name.



## H.323 Participants

H.323 participants dial [Gatekeeper Prefix][Entry Queue ID/Name].

### Example:

Prefix in gatekeeper	925
Entry Queue ID	1000
>> The participant dials	9251000

H.323 participants can bypass the Entry Queue IVR voice messages by adding the correct Conference ID of destination conference to the initial dial string:

[Gatekeeper Prefix][EQ ID][##Destination Conference ID]

### Example:

Conference ID	1001
>> H.323 participants dial	9251000##1001

## ISDN and PSTN Participants

Up to two dial-in numbers can be allocated to an Entry Queue for use by ISDN and PSTN participants.

Calls to numbers within the ISDN and PSTN *Dial-in Range* that are not allocated to an Entry Queue are routed to the *Transit Entry Queue*.

Dial-in ISDN and PSTN participants dial one of the dial-in numbers assigned to the Entry Queue, including the country and area code (if needed). They are routed to their conference according to the conference ID.

### Example:

Entry Queue ID	1000
Assigned Dial-in number	9251000
>> ISDN/PSTN participants dial	9251000

Once connected to the Entry Queue, they enter the conference Numeric ID or password to be routed to the appropriate conference.

## Dial-out Participants

Dial-out participants are defined with their dial-out number. Once they are added to the ongoing conference, the MCU automatically calls them at a rate of 1 dial-out per second, using the default H.323 or ISDN/PSTN Network Service defined for them.

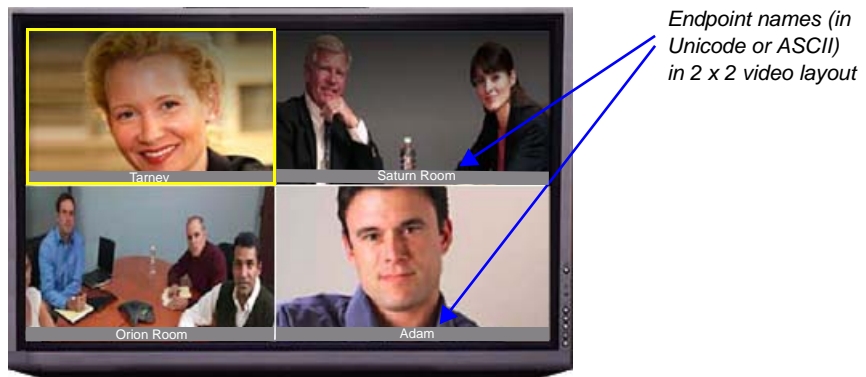


## Text Indication in the Video Layout

### Endpoint Names

During conferences you can view the names of the endpoints that are connected to the conference in your endpoint's video layout windows. The MCU can display up to 33 characters of the endpoint's name, depending on the window's layout (size).

The following is an example of endpoint name display in the endpoint screen:



The displayed name is determined as follows:

- The system displays the name that is defined at the endpoint.
- If the endpoint does not send its name:
  - For a defined H.323 participant:
    - The system displays the name from the participant definition.
  - For an undefined H.323 participant:
    - Display the *H.323 ID* alias.
    - or
    - Display the *E.164* alias.
    - or
    - Display nothing if all the fields are empty.

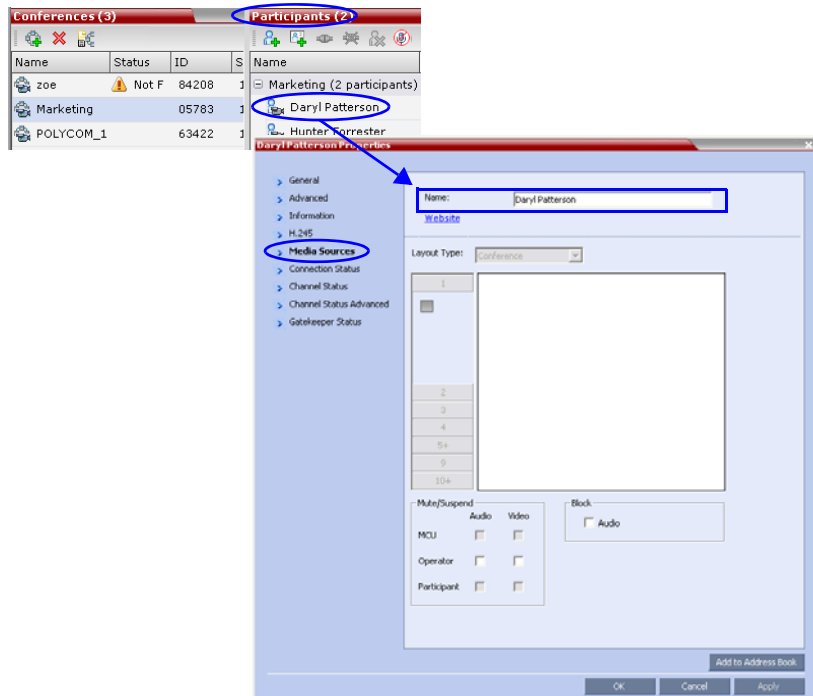


- For a defined H.320 participant:
  - The system displays the name from the participant definition.
- For an undefined H.320 participant:
  - Display the *Terminal Command String* (TCS-2) to identify the participant.
- or
- Display nothing if the string is not received or empty.
- If the endpoint's *Display Name* is changed in the *RMX Web Client*, it overrides all the above.

### To change the Display Name:

- 1 In the *Participants* list, double-click the participant or right-click the participant and then select **Participant Properties**.

The *Participant Properties – Media Sources* dialog box opens:



- 2 Enter the new *Display Name* in the *Name* field.
- 3 Click **OK**.

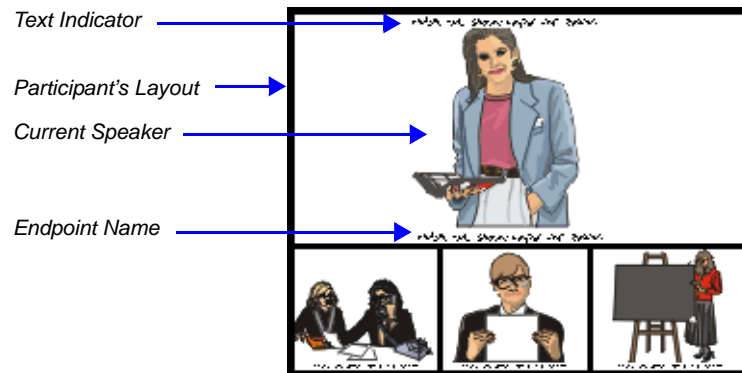


## Text Indication

The *Text Indication* appears in the window of the current speaker in the participant's layout in addition to the endpoint name. It displays the conference Secure mode (on or off), total number of connected participants, number of video participants and number of audio participants.

The text indication is automatically displayed when there is a change in the conference Secure state (when Secure is implemented or cancelled) and it appears only for a few seconds (the same duration as the endpoint names).

The conference chairperson or participants can request the display of a *Textual Indication* of the conference's statistics by entering the DTMF code \*88 on the endpoint's DTMF input device, such as remote control.



The Text Indication is displayed according to the permission set in the Conference IVR Service:

- Chairperson permission: Only the chairperson sees the indication
- Everyone permission: All participants see the indication.



Participants connected as Secondary (no video) will be considered as audio participants; defined participant which are not currently connected to the conference (disconnected, redial, disconnecting, etc.) are not counted.

*Text Indication* can be disabled by adding a new flag to the *System Configuration* and setting its value to NO as follows:  
ENABLE\_TEXTUAL\_CONFERENCE\_STATUS=NO.



This setting is recommended for MCUs running *Telepresence* conferences. For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "System Configuration" on page [14-22](#).

## **Transparent Endpoint Names**

Endpoint name backgrounds are 50% transparent, and while maintaining contrast, do not completely obscure the overlaid video.

The *Endpoint Name Transparency* feature can be disabled by adding a new flag to the *System Configuration* and setting its value to NO as follows:  
SITE\_NAME\_TRANSPARENCY=NO.

For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "System Configuration" on page [14-22](#).



# Monitoring Ongoing Conferences



Recording of conferences is not supported in *Ultra Secure Mode*.

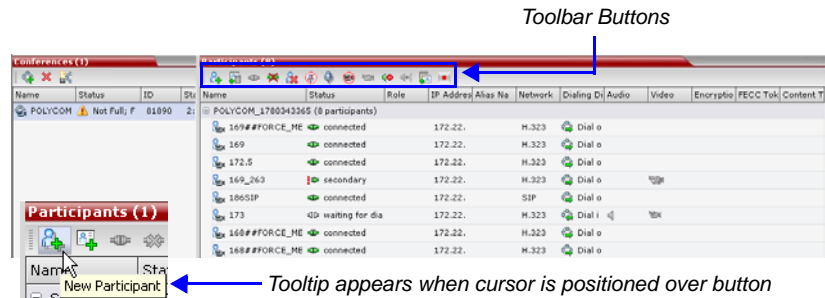
Conference monitoring enables you to keep track of conferences and their participants: if all its participants are correctly connected and whether errors or faults have occurred.

The maximum number of participants that can connect to a conference is 200. Of these, 80 can be video participants.

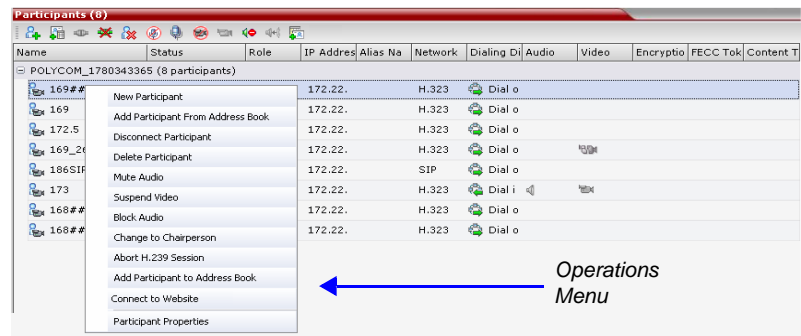
## Operation Selection

All monitoring and operations procedures performed during ongoing conferences can be performed by either of two methods:

- Using the buttons in the toolbars.



- Right-clicking anywhere in the *Conferences* or *Participants* pane and selecting an operation from the menu.



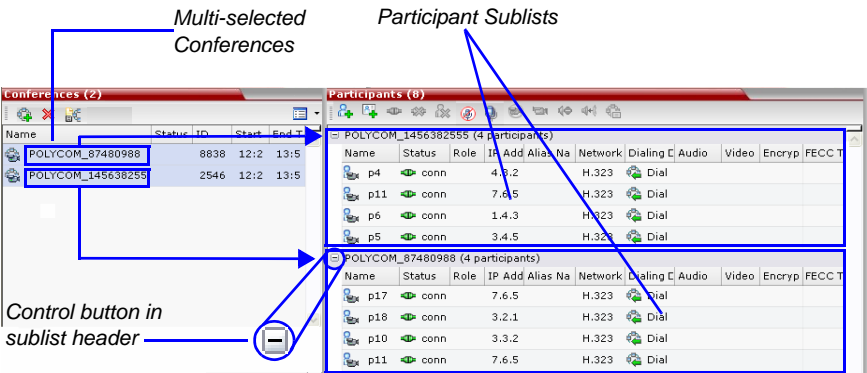


### Multi Selection

Using multiple selection, you can monitor and perform simultaneous operations on multiple participants in multiple conferences.

The selected conferences are displayed as sub-lists in the *Participants* list pane.

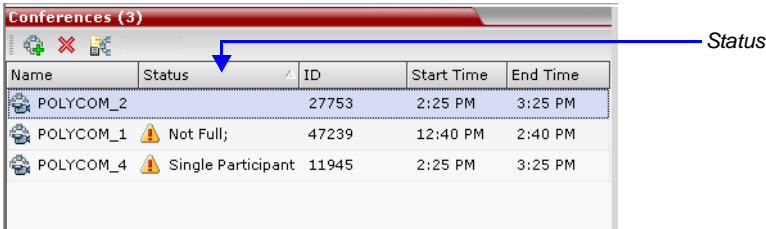
The sub-lists can be expanded and collapsed by clicking the **+** and **-** sublist control buttons that appear next to the conference name in the sublist headings.



### Conference Level Monitoring

Conference level monitoring is available to the administrator and operator.

The *Conference List* pane displays information about ongoing conferences.







No status indicator display in the *Status* column means that the conference is running without problems.



One or more of the status indicators listed in Table 2-5 may appear in the *Status* column.

**Table 2-5** Conferences – Monitoring Information

Field	Description
<i>Name</i>	<p>Displays conference name and type of conference:</p> <ul style="list-style-type: none"> <li> – Video Conference (including HD CP conferences).</li> <li> – High Definition Video Conference running in Video Switching mode.</li> <li> – The conference has been secured using the *71 DTMF code.</li> </ul>
<i>Status</i>	<p>Displays the status of the ongoing conference.</p> <p>If there is no problem with the participant's connection no indication is displayed.</p> <p>If one of the following statuses occurs, the appropriate indication is displayed, preceded by a warning icon (.</p> <ul style="list-style-type: none"> <li><b>Audio</b> – There is a problem with the participant's audio.</li> <li><b>Empty</b> – No participants are connected.</li> <li><b>Faulty Connection</b> – Participants are connected, but the connection is problematic.</li> <li><b>Not Full</b> – Not all the defined participants are connected.</li> <li><b>Partially Connected</b> – The connection process is not yet complete; the video channel has not been connected.</li> <li><b>Single Participant</b> – Only one participant is connected.</li> <li><b>Video</b> – There is a problem with the participant's video.</li> </ul>
<i>ID</i>	The Conference ID assigned to the conference.
<i>Start Time</i>	Conference start time.
<i>End Time</i>	The time the conference is expected to end.

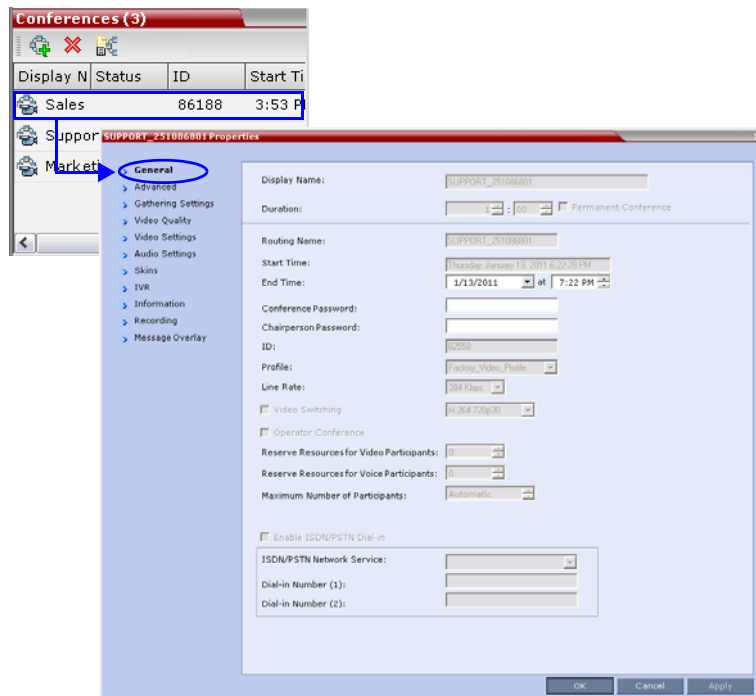


Additional information about the conference can be viewed when accessing the conference properties.

**To monitor a conference:**

- >> In the *Conference List* pane, double click the name of the conference you wish to monitor or right-click the conference and then click **Conference Properties**.

The *Conference Properties* dialog box appears with the *General* tab open.



You can view all the conference's properties but those that appear with a gray background cannot be modified.

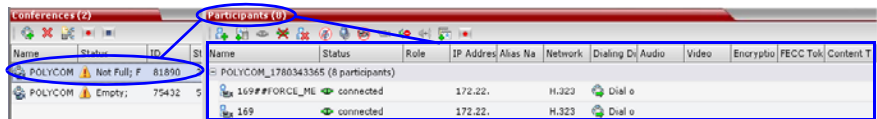
For more information, see the *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "Conference Level Monitoring" on page 8-3.



## Participant Level Monitoring





### Participant Connection Monitoring

When a conference is selected in the *Conference List*, details of its participants appear in the *List* pane.











The following participant indicators and properties are displayed:

**Table 2-6** Participant Monitoring – Indicators and Properties

Column	Icon/Description
Name	Displays the name and type (icon) of the participant:
	 <b>Audio Participant</b> – Connected via IP phone or ISDN/PSTN.
	 <b>Video Participant</b> – Connected with audio and video channels.
Status	Displays the connection status (text and icon) of the participant. If there is no problem with the participant's connection no indication is displayed.
	 <b>Connected</b> – The participant is successfully connected to the conference.
	 <b>Disconnected</b> – The participant is disconnected from the conference. This status applies only to defined participants.












**Table 2-6** Participant Monitoring – Indicators and Properties (Continued)

Column	Icon/Description	
Status (cont.)		<b>Waiting for Dial-in</b> – The system is waiting for the defined participant to dial into the conference.
		<b>Partially Connected</b> – The connection process is not yet complete; the video channel has not been connected.
		<b>Faulty Connection</b> – The participant is connected, but problems occurred in the connection, such as synchronization loss.
		<b>Secondary Connection</b> – The endpoint's video channel cannot be connected to the conference and the participant is connected only via audio.
Role	Displays the participant's role or function in the conference:	
		<b>Chairperson</b> – The participant is defined as the conference chairperson. The chairperson can manage the conference using touch-tone signals (DTMF codes).
		<b>Lecturer</b> – The participant is defined as the conference Lecturer.
		<b>Lecturer and Chairperson</b> – The participant is defined as both the conference Lecturer and Chairperson.
		<b>Cascade Enabled Dial-out Participant</b> – A special participant functioning as a link in a cascaded conference.
IP Address/ Phone	The IP participant's IP address or the ISDN/PSTN participant's phone number.	
Alias Name	<p>The participant's Alias Name.</p> <p>The alias of an <i>RSS 2000 Recording System</i> if the participant is functioning as a recording link.</p> <p><b>Note:</b> <i>Recording</i> of conferences is not supported in <i>Ultra Secure Mode</i>.</p>	




**Table 2-6** Participant Monitoring – Indicators and Properties (Continued)

Column	Icon/Description	
<i>Network</i>	The participant's network connection type – H.323 or ISDN/PSTN.	
<i>Dialing Direction</i>		<b>Dial-in</b> – The participant dialed the conference.
		<b>Dial-out</b> – The MCU dialed the participant.
<i>Audio</i>	Displays the status of the participant's audio channel. If the participant's audio is connected and the channel is neither muted nor blocked, no indication is displayed.	
		<b>Muted</b> – Participant's audio channel is muted. The participant can still hear the conference.
		<b>Blocked</b> – Transmission of audio from the conference to the participant is blocked.
		<b>Muted and Blocked</b> - Audio channel is muted and blocked.
<i>Video</i>	Displays the status of the participant's video channel. If there is no problem with the participant's video connection and the channel is neither suspended nor secondary, no indication is displayed.	
		<b>Suspended</b> – Video transmission from the endpoint to the conference is suspended.
		<b>Secondary</b> – Participant is connected only through the audio channel due to problems with the video channel.
<i>Encryption</i>		Indicates that the endpoint is using encryption for its connection to the conference.
<i>FECC Token</i>		Participant is the holder of the FECC token and has Far End Camera Control capabilities. The FECC token can be allocated to only one participant at a time and remains un-allocated if no participant requests it.



**Table 2-6**    *Participant Monitoring – Indicators and Properties (Continued)*

Column	Icon/Description	
<i>Content Token</i>		Participant is the holder of the Content token and has content sharing permission. The Content token can be allocated to only one participant at a time and remains un-allocated if no participant requests it. For more information, see the <i>RMX 1500/2000/4000 Administrator's Guide</i> , "H.239" on page <a href="#">2-12</a> .

For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Participant Level Monitoring" on page [8-10](#).



# Operations Performed During On Going Conferences

## Conference Level operations

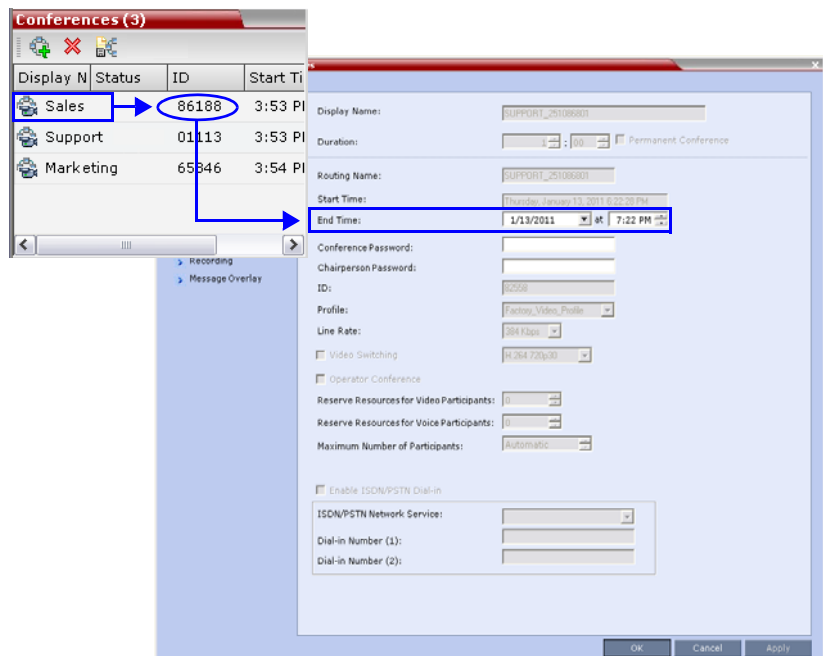
### Changing the Duration of a Conference

The duration of each conference is set when the new conference is created. The default duration of a conference is 1 hour. All conferences running on the RMX are automatically extended as long as there are participants connected to the conference.

A conference's *Duration* can be extended or shortened while it is running, by modifying its scheduled *End Time*.

To extend or shorten a conference manually:

- 1 In the *Conference List* pane, double-click the conference **Name**.
- 2 In the *General* tab, modify the *End Time* fields and click **OK**.



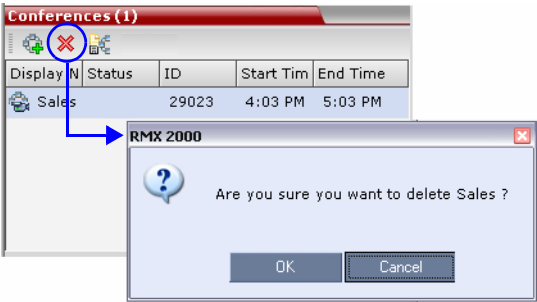
The *End Time* is changed and the *Duration* field is updated.



**To terminate a conference manually:**

- 1 In the *Conferences* list, select the conference you wish to delete and click the **Delete Conference (X)** button.

You are prompted for confirmation.



- 2 Click **OK** to terminate the conference.

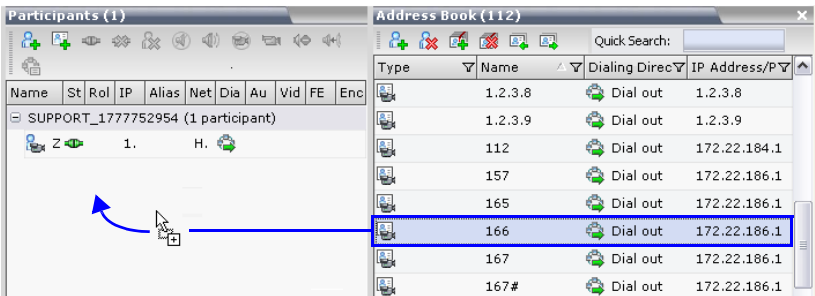
**Adding Participants from the Address Book**

Once the conference has started, you can add participants to a conference directly from the *Participants Address Book* without having to use the *New Conference – Participants* tab.

**To drag & drop participants into the Participants List:**

- 1 Open the *Address Book*.
- 2 Select, drag and drop the participant that you wish to add to the conference directly from the *Participant Address Book* into the *Participant List*.

Standard Windows multiple selection techniques can be used in this procedure.



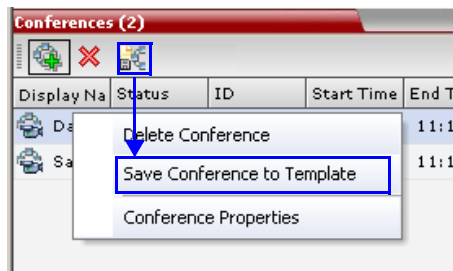


## Saving an Ongoing Conference as a Template

Any conference that is ongoing can be saved as a template.

**To save an ongoing conference as a template:**

- 1 In the *Conferences List*, select the conference you want to save as a Template.
- 2 Click the **Save Conference** (📄🔗) button.  
or  
Right-click and select **Save Conference to Template**.



The conference is saved to a template whose name is taken from the ongoing conference *Display Name*.

## Copy and Paste Conference

The RMX user can **Copy**, and **Paste** conferences. When using the *RMX Web Client*, conferences can be copied and pasted on the same RMX, however when using the *RMX Manager*, with its ability to manage multiple RMXs, conferences can be copied and pasted between different RMXs.

### Copy Conference

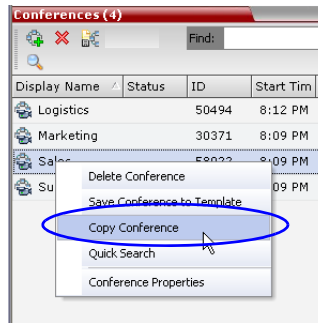
The **Copy** command copies all the conference's properties including connected participants and makes these properties available for pasting, starting a new conference. The copied conference remains active until it terminates or is deleted.

**To copy a conference:**

- 1 In the *Conferences List* pane, right-click the conference you want to copy.



- 2 In the drop-down menu select **Copy Conference**.



## Paste Conference

The **Paste Conference** command starts the new conference on the same *RMX* or on a different *RMX*.

To paste a conference:

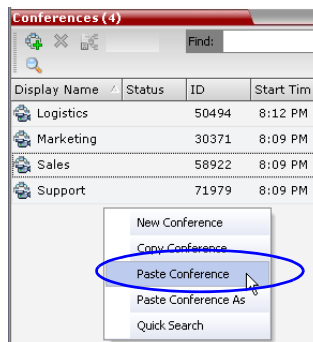
- >> Right-click in the *Conferences List* pane and in the drop-down menu select

**Paste Conference.**

or

If you are using the *RMX Manager* and you want to paste the conference to a different *RMX*:

- a In the *MCUs list* pane, click the *RMX* that is to receive the conference.
- b In the *Conferences list* pane, right-click, and in the drop-down menu select **Paste Conference**.





The conference is pasted to the *RMX*.

## **Paste Conference As**

The **Paste Conference As** command allows the *RMX* user to create a new conference using the copied conference's properties as a template. It automatically opens the *Conference Properties* dialog box allowing the *RMX* user to modify the *General*, *Participants* and *Information* tabs to create the new conference. When the **OK** button in the *Conference Properties* dialog box *conference Properties* dialog box is clicked the new conference is started.

### **To paste a conference as a new conference:**

- 1** Right-click in the *Conferences List* pane and in the drop-down menu select

**Paste Conference As.**

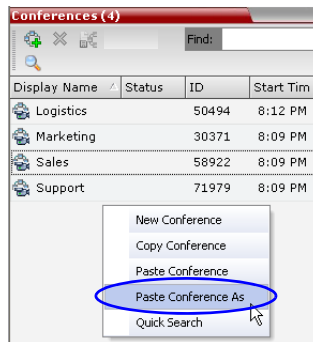
**or**

If you are using the *RMX Manager* and you want to paste the conference to a different *RMX*:

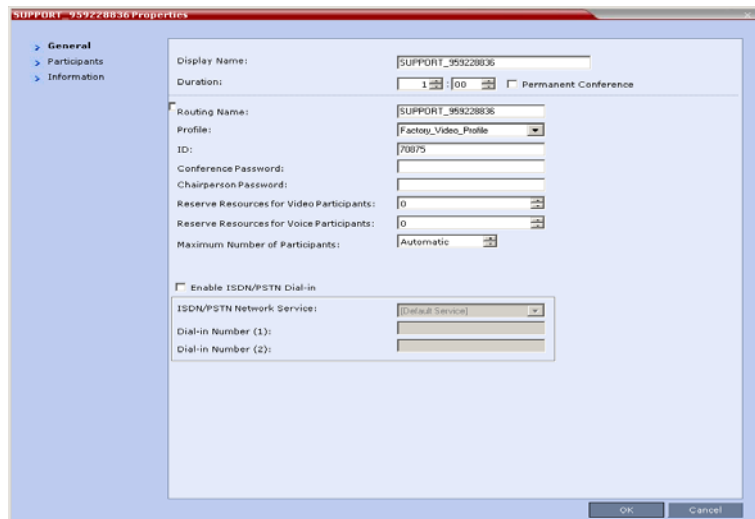
- a** In the *MCUs* list pane, click the *RMX* that is to receive the conference.



- b** In the *Conferences* list pane, right-click, and in the drop-down menu select **Paste Conference As**.



The *Conference Properties* dialog box is displayed.



- 2** Modify the conference information as required.
- 3** Click the OK button to paste and start the new conference.

## Changing the Video Layout of a Conference

While the conference is running, you can change the video layout and select one of 24 video layouts supported by the RMX.

Video Layout selection can be done in two levels:



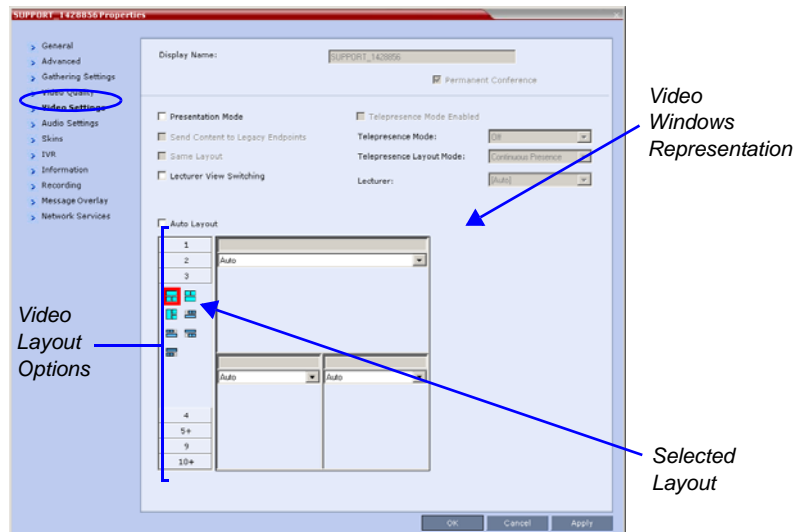
- **Conference Level** – Applies to all conference participants. All participants have the same video layout.
- **Participant Level** – The participant's video layout is changed. All other conference participants' video layouts are not affected.

The initial video layout is selected for the conference in the *Conference Profile*.

Participant level video layout selection overrides conference level video layout settings.

**To change the video layout of a conference:**

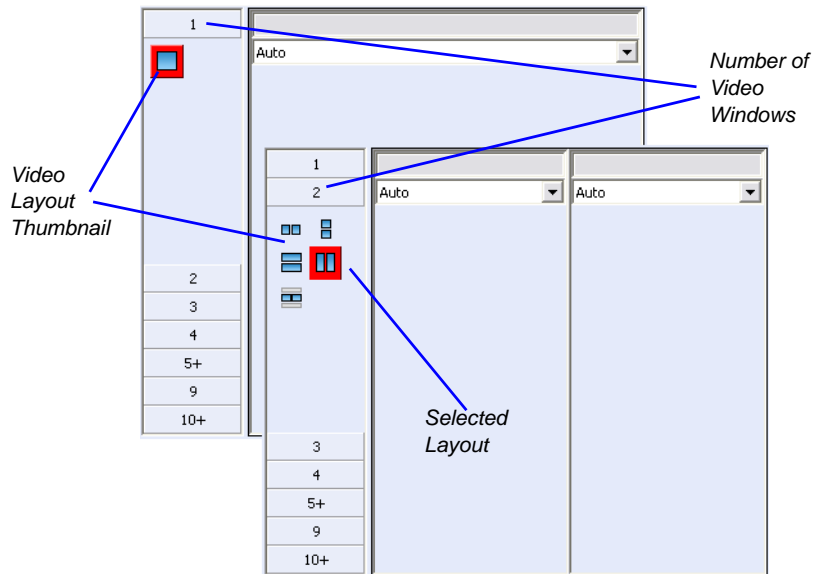
- 1 In the *Conference Properties* dialog box, select **Video Settings**.



- 2 If **Auto Layout** check box is selected, clear it.



- 3** From the *Video Layout* options, select the *Number of Windows* to display and the *Video Layout* thumbnail required and click **OK**.



## Video Forcing

Users with Administrator or Operator permission can select which participant appears in each of the video layout windows using *Video Forcing*. When a participant is forced to a layout window, switching between participants is suspended for that window and only the assigned participant is viewed. Video Forcing works on Conference Level or Participant Level:

- **Conference Level** – When forcing a participant to a window, all conference participants will see that participant in the selected window.
- **Participant Level** – When forcing a participant to a window, only the participant's video layout display is affected. All other participants see the conference layout.

### Video Forcing Guidelines:

- A participant cannot appear in two or more windows at the same time.



- ### To video force a participant to a window:

- 
- Support - 1426856 Properties
- General  
Advanced  
**Video Settings**  
Video Quality  
Video Settings  
Audio Settings  
Skins  
IVR  
Information  
Recording  
Message Overlay  
Network Services
- Display Name: SUPPORT\_1426856
- ☒ Permanent Conference
- ☐ Presentation Mode
- ☐ Send Content to Legacy Endpoints
- ☐ Same Layout
- ☐ Lecturer View Switching
- ☐ Auto Layout
- Telepresence Mode Enabled
- Telepresence Mode:
- Telepresence Layout Mode:
- Lecturer:
- 1  
2  
3  
4  
5+  
9  
10+
- Auto  
Auto  
Auto  
Start  
Stop  
Pause  
Video
- Auto
- Auto
- OK Cancel Apply
- List of Conference Participants
- Video Windows
- Selected Layout



- 5** Repeat step 3 to force participants to other windows.
- 6** Click **OK**.

**To cancel Video Forcing for a window:**

- 1** In the *Conference Properties* dialog box, select the **Video Settings** tab.
- 2** In the video layout window, in the *Participants* list, select **Auto**.
- 3** Click **OK**.

Switching between participants is renewed and is audio activated.

## **Enabling and Disabling Video Clarity™**

The user can enable or disable Video Clarity™ during an ongoing conference.

**To enable or disable Video Clarity:**










- 1** In the *Conference List* pane, double-click the name of the conference for which you want to enable or disable *Video Clarity*  
or  
right-click the conference name and then click **Conference Properties**.
- 2** Click the **Video Settings** tab.
- 3** Select or clear the **Video Clarity** check box as required.
- 4** Click **OK**.



## Participant Level Operations










Participant Level Operations enable you to modify and control the connections and statuses of participants in ongoing conferences, as described in Table 2-7.

**Table 2-7** *Participant Level Operations*

Menu Option	Button	Description
<i>New Participant</i>		Define a new participant. For more information about the <i>New Participant</i> dialog box tab, see Table 2-3 on page 2-22.
<i>Add Participant From Address Book</i>		Open the <i>Address Book</i> to select the participant for the conference. For more information about the <i>Address Book</i> , see the <i>RMX 1500/2000/4000 Administrator's Guide</i> , "Address Book" on page 5-1.
<i>Connect Participant</i>		Connect a disconnected defined dial-out participant to the conference.
<i>Disconnect Participant</i>		Disconnect the participant from the conference.
<i>Delete Participant</i>		Delete the selected participants from the conference.
<i>Mute Audio</i>		Mute the audio transmission from the participant to the conference. The <i>Audio Muted</i> indicator appears in the <i>Participants List</i> and the <i>Unmute Audio</i> button (  ) becomes active.
<i>Unmute Audio</i>		Resume the participant's audio transmission to the conference. The <i>Mute Audio</i> button (  ) becomes active.



**Table 2-7** Participant Level Operations (Continued)

Menu Option	Button	Description
<i>Suspend Video</i>		Suspend the video transmission from the participant to the conference. The suppressed participant's video is not transmitted to the conference but the participant still receives conference video. The <i>Suspend Video</i> indicator appears in the <i>Participants List</i> and the <i>Resume Video</i> button (  ) becomes active.
<i>Resume Video</i>		Resume the participant's video transmission to the conference. The <i>Suspend Video</i> button becomes active (  )
<i>Block Audio</i>		To block the audio transmission from the conference to the participant. When blocked, the participant can still be heard by the conference. The <i>Audio Blocked</i> indicator appears in the <i>Participants List</i> and the <i>Unblock Audio</i> button (  ) becomes active.
<i>Unblock Audio</i>		Resume the audio transmission from the conference to the participant. The <i>Block Audio</i> button (  ) becomes active.
<i>Add Participant to Address Book</i>		Add selected participant's details to the <i>Participant Address Book</i> .
<i>Abort H.239 Session</i>		To withdraw the Content Token from the participant back to the MCU for re-assignment.
<i>Change to Chairperson</i>		Define the selected participant as the conference leader/chairperson.
<i>Change to Regular Participant</i>		Define the chairperson as a regular participant without chairperson privileges.



**Table 2-7** Participant Level Operations (Continued)

Menu Option	Button	Description
<i>Connect to Website</i>		Connect directly to the internal website of the participant's endpoint to perform administrative, configuration and troubleshooting activities.
<i>AGC (Auto Gain Control)</i>		Enable AGC for the participant with weak audio signal during ongoing conferences. <b>Note:</b> Enabling AGC may result in amplification of background noise.
<i>Participant Properties</i>		To view all <i>Participant Properties</i> . For more information, see the <i>RMX 1500/2000/4000 Administrator's Guide</i> , "Participant Level Monitoring" on page 8-10.

## Copy Cut and Paste Participant

The *RMX* user can **Copy**, **Cut** and **Paste** participants between different conferences running on the *RMX*, including his/her current conference. These functions, when used via the *RMX Manager*, with its ability to manage multiple *RMX*s, participants, allows the *RMX* user to **Copy**, **Cut** and **Paste** participants between conferences running on different *RMX*s.

### Copy Participant

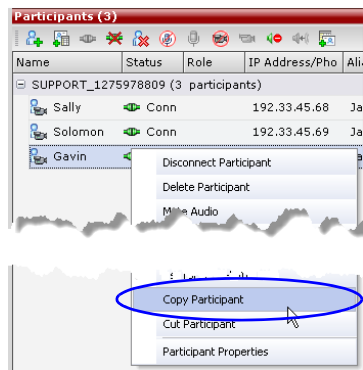
The **Copy** command copies all the participant's properties and makes them available for pasting. The participant remains connected to his/her current conference.

#### To copy a participant:

- 1 In the *Participants List* pane, right-click the participant you want to copy.



**2** In the drop-down menu select **Copy Participant**.

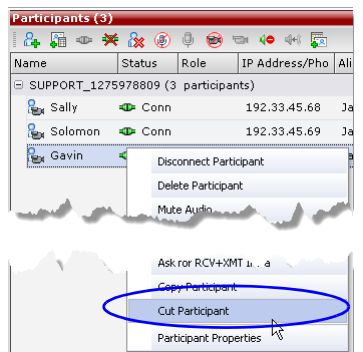


## Cut Participant

The **Cut** command copies all the participant's properties and makes them available for *pasting*. The participant is deleted from his/her current conference.

**To cut a participant:**

- 1** In the *Participants List* pane, right-click the participant you want to cut.
- 2** In the drop-down menu select **Cut Participant**.





## Paste Participant

The **Paste** command connects the *copied* or *cut* participant to the selected conference.

If the participant was *copied*, he/she should be deleted from the conference he/she was *copied* from, unless it is required that the participant is connected to two (or more) conferences. (There are endpoints that permit a participant to be connected to multiple conferences).

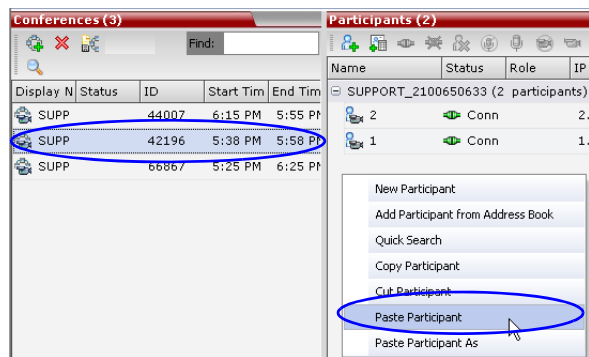
### To paste a participant:

- 1 In the *Conferences List* pane, click the conference you want to paste the copied/cut participant into.
- 2 Right-click in the *Participants List* pane of the selected conference and in the drop-down menu select **Paste Participant**.

or

If you are using the *RMX Manager* and you want to paste the participant to a conference to different RMX:

- a In the *MCUs list* pane, click the RMX that is hosting the conference that is to receive the participant.
- b In the *Conferences* list pane, click the conference you want to paste the copied/cut participant into.
- c Right-click, and in the drop-down menu select **Paste Participant**.



The participant is connected to the conference.



## Paste Participant As

The **Paste Participant As** command allows the RMX user to create a new participant using the copied participant's properties as a template. It automatically opens the *Address Book - Participant Properties* dialog box allowing the RMX user to modify the participant's properties effectively creating a new participant. When the **OK** button in the *Participant Properties* dialog box is clicked the new participant is connected to the selected conference.

### To paste a participant as a new participant:

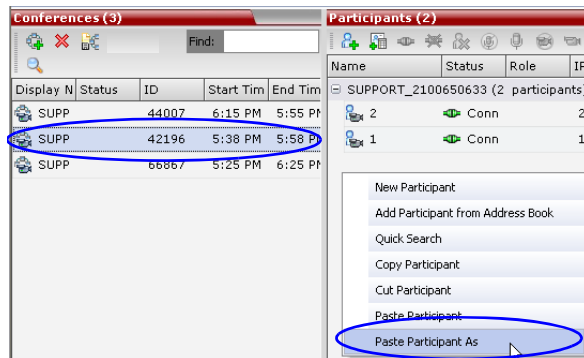
- 1 In the *Conferences List* pane, click the conference you want to paste the copied/cut participant into.

Right-click in the *Participants List* pane of the selected conference and in the drop-down menu select **Paste Participant As**.

or

If you are using the *RMX Manager* and you want to paste the participant to a conference on another RMX:

- a In the *MCUs* list pane, click the RMX that is hosting the conference that is to receive the participant.
- b In the *Conferences* list pane, click the conference you want to paste the copied/cut participant into.
- c Right-click, and in the drop-down menu select **Paste Participant As**.





The *Address Book - Participant Properties* dialog box is displayed.

**Gavin Properties**

> General  
> Advanced  
> Information

Name: Gavin

[Endpoint Website](#)

Dialing Direction: Dial out

Type: H.323

IP Address: 192.33.45.90

Alias Name / Type: Jack H.323 ID

Website IP Address:

Ip Service Network: Primary

☐ Audio Only

Extension/Identifier String:

Add to Address Book

OK Cancel

- 2 Modify the participant information as required. For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "Modifying Participants in the Address Book" on page 6-10.

**Optional.** If not already in the *Address Book*, the copied/cut participant can be added to the *Address Book*.

**Optional.** The new participant can be added to the *Address Book*.

- 3 Click the **OK** button to connect the new participant to the selected conference.



## Personal Layout Control with the RMX Web Client

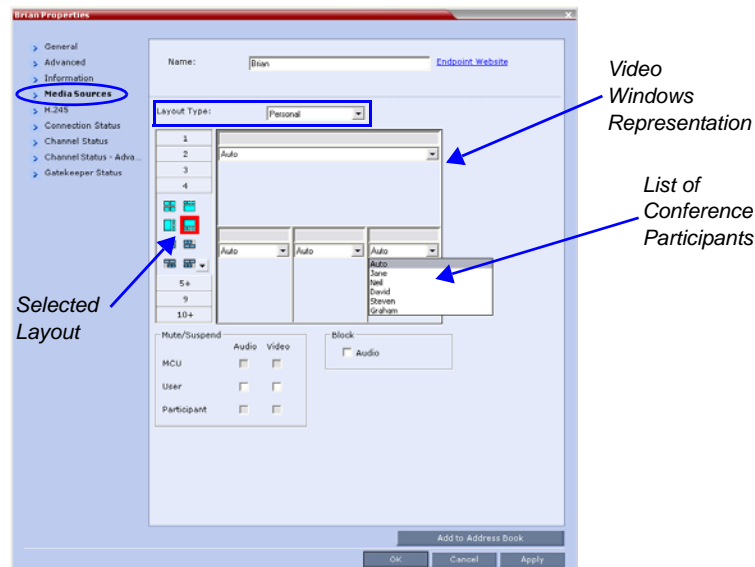
RMX users can use the *RMX Web Client* to change the *Video Layouts* of individual participants and force participants to its windows without affecting the *Video Layouts* of other participants.

### To change a participant's Video Layout and Video Forcing:

- 1 In the *Participants* list, double click the participant or right-click the participant and then click **Participant Properties**.

The *Participant Properties – Media Sources* dialog box opens.

- 2 In the *Layout Type* list, select **Personal**.



- 3 Select the number of Video Windows.
- 4 Select the required Video Layout.
- 5 To video force participants to windows in the selected video layout, in the window to which you want to force a participant, select the name of the participant to force from the list of conference participants.
- 6 Repeat step 5 to force participants to other windows.
- 7 Click **OK**.



**To cancel the Personal Video Layout selection and return to the conference layout:**

- 1 In the *Participant Properties* dialog box, select the **Media Sources** tab.
- 2 In the *Layout Type* list, select **Conference**.
- 3 Click **OK**.

The participant will now see the conference video layout with its forced participants.

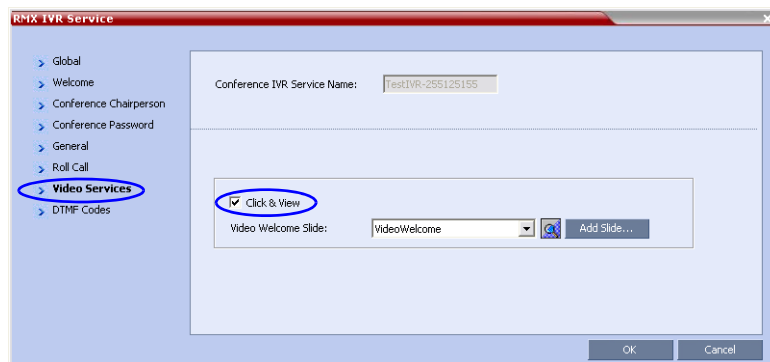
**To cancel the Personal Video Forcing for a window without returning to the conference layout:**

- 1 In the *Participant Properties – Media Sources* dialog box, in the video layout window, select **Auto** in the *Participants* list.
- 2 Click **OK**.

Switching between participants is renewed and is audio activated.

## Personal Layout Selection with **Click&View**

With the **Click&View** application, participants can change their *Personal Layouts* via *DTMF* codes entered from their endpoints. This option is available only if the **Click&View** option is selected in the *Conference IVR Service*.



**To change Personal Layout with Click&View:**

- 1 **Enable Click&View** – on the endpoint's keypad, enter .

The *Click&View* application is displayed on the screen.



When using a *Polycom VSX* endpoint, an additional must be entered to enable the remote DTMF keypad. The full *Click&View* entry sequence is: .



The Personal Layout keypad options menu is displayed on the video screen.



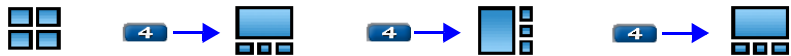
- 2** On the endpoint's remote keypad, press the number corresponding to the number of video squares you wish to select.

For example, if you want a four-square video layout, press **4**.

The video window layout of your screen changes to the first four-window layout as follows:



Repeated presses of the **4** key, within eight seconds, cycles through the following series of four-square layout options:



In any multi-square layout, pressing **#** forces the current speaker to the top left window.





















In full view, pressing **#** forces the next participant to full view.

In any video layout, pressing **0** reverts to the conference layout.



The following table summarizes the Video Layout options available via *Click&View*.

**Table 2-8** Video Layout Options

DTMF Code	Layout Options				
1					
2					
3					
4					
5					
6					
8					
9					

## Conference Control Using DTMF Codes

Participants and chairpersons can manage their connection to ongoing conferences from their endpoints, using touch-tone signals (DTMF codes) from their endpoints. Table 3-9 lists the DTMF Codes that can be used.

Chairpersons can also control an ongoing conference using DTMF codes.

Permissions for DTMF actions to be performed by all conference participants or by chairperson only are configured in the *Conference IVR Service* assigned to the conference.

For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Defining a New Conference IVR Service" on page 12-9.

To use the DTMF codes to control the conference, the DTMF input must be first enabled on the endpoint remote control (for example, entering #).



**Table 2-9** Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Mute My Line	*6	All
Unmute My Line	#6	All
Increase Broadcast Volume	*9	All
Decrease Broadcast Volume	#9	All
Mute All Except Me	*5	Chairperson
Cancel Mute All Except Me	#5	Chairperson
Change Password	*77	Chairperson
Mute Incoming Participants	*86	Chairperson
Unmute Incoming Participants	#86	Chairperson
Play Help Menu	*83	All
Enable Roll Call	*32	Chairperson
Disable Roll Call	#32	Chairperson
Roll Call Review Names	*33	Chairperson
Roll Call Stop Review Names	#33	Chairperson
Terminate Conference	*87	Chairperson
Start Click&View	**	All
Change To Chairperson	*78	All
Increase Listening Volume	*76	All
Decrease Listening Volume	#76	All
Override Mute All	Configurable	All
Secure Conference	*71	Chairperson
Unsecure Conference	#71	Chairperson
Show Participants	*88	All



# Intrusion Detection

## Network Intrusion Detection System (NIDS)

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

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

The *RMX* maintains a log that includes all unpermitted access attempts blocked by the firewall.

Unpermitted access attempts include:

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

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

For more information the *RMX 1500/2000/4000 Administrator's Guide Maximum Security Environments*, "Information Collector" on page **17-145**.







---

# Installing RMX Manager for Secure Communication Mode

The *RMX Manager* cannot be downloaded from a site, operating in *Secure Communication Mode*, without a valid TLS certificate.

The following procedure describes how to obtain a TLS certificate and download the *RMX Manager* from a site operating in *Secure Communication Mode*.



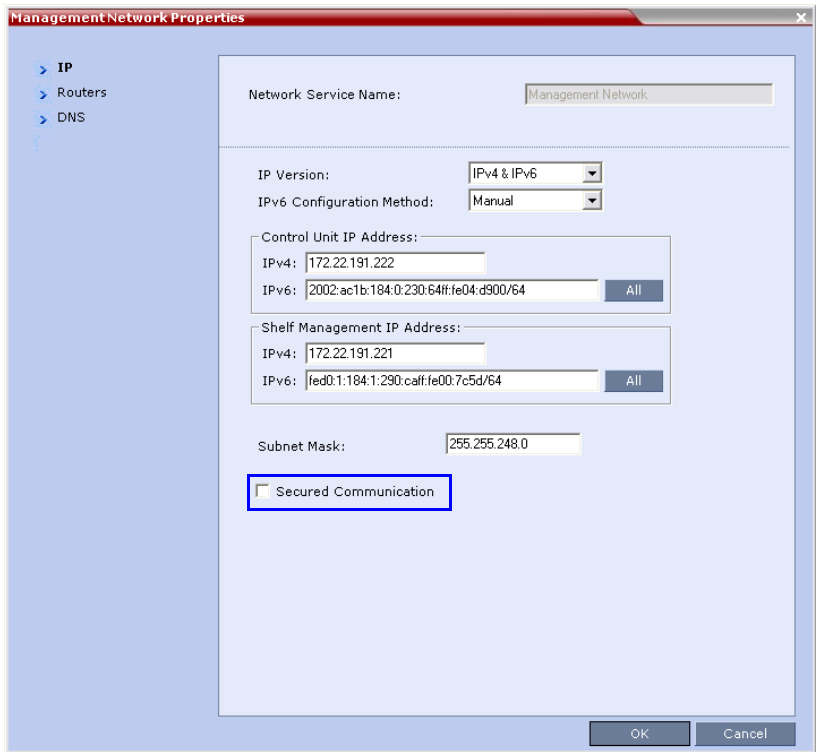
In order to install the *RMX Manager*, the workstation must have the following installed:

- *.NET Framework 3.5* or a later version of the *.NET Framework*.
- *.NET Framework 2.0* plus *Service Pack 1* or later.

- 1 Set the *RMX* to *Non Secure Communication Mode*
  - a In the *RMX Management* pane, click **IP Network Services**.
  - b In the *IP Network Services* list pane, double click the **Management Network** entry.



The *Management Network Properties* dialog box is displayed.



The image shows a screenshot of the 'Management Network Properties' dialog box. The dialog has a title bar with the text 'Management Network Properties' and a close button. On the left side, there is a tree view with three items: 'IP' (selected), 'Routers', and 'DNS'. The main area of the dialog contains several fields and sections. At the top, there is a 'Network Service Name' field with the value 'Management Network'. Below this, there are two dropdown menus: 'IP Version' set to 'IPv4 & IPv6' and 'IPv6 Configuration Method' set to 'Manual'. There are two sections for IP addresses: 'Control Unit IP Address' and 'Shelf Management IP Address'. Each section has fields for 'IPv4' and 'IPv6' addresses, with 'All' buttons next to the IPv6 fields. The 'Subnet Mask' field is set to '255.255.248.0'. At the bottom, there is a checkbox labeled 'Secured Communication' which is currently unchecked and highlighted with a blue border. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Field	Value
Network Service Name	Management Network
IP Version	IPv4 & IPv6
IPv6 Configuration Method	Manual
Control Unit IP Address - IPv4	172.22.191.222
Control Unit IP Address - IPv6	2002:ac1b:184:0:230:64ff:fe04:d900/64
Shelf Management IP Address - IPv4	172.22.191.221
Shelf Management IP Address - IPv6	fed0:1:184:1:290:caff:fe00:7c5d/64
Subnet Mask	255.255.248.0
Secured Communication	<input type="checkbox"/>

- c Clear the *Secured RMX Communication* check box.
- d Click OK.



## 2 Click the DNS tab.

The screenshot shows the 'ManagementNetwork Properties' dialog box with the 'DNS' tab selected. The 'Network Service Name' is 'Management Network'. The 'MCU Host Name' field is 'rmxido.fr.polycom.com' and is highlighted with a blue box and an arrow pointing to it from the label 'MCU Host Name'. The 'Local Domain Name' field is also 'rmxido.fr.polycom.com' and is highlighted with a blue box and an arrow pointing to it from the label 'Local Domain Name'. The 'DNS' dropdown is set to 'Specify'. The 'Register Host Names Automatically to DNS Servers' checkbox is unchecked. The 'DNS Servers Addresses' section shows 'Primary Server' as '172.22.128.27', 'Secondary Server' as '0.0.0.0', and 'Tertiary Server' as '0.0.0.0'. The 'OK' and 'Cancel' buttons are at the bottom right.

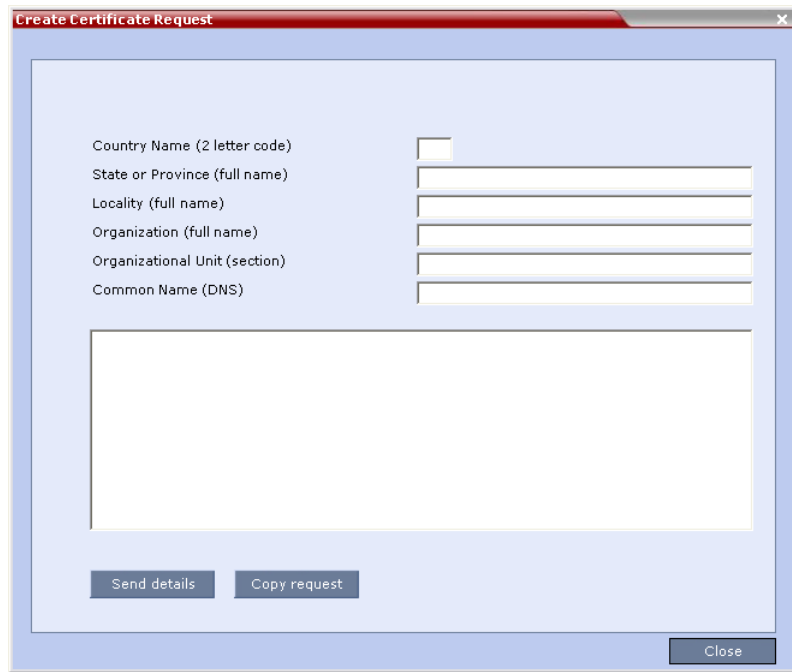
## 3 Enter the Local Domain Name.



The *Local Domain Name* must be the same as the *MCU Host Name*. If the content of these two fields are not identical an active alarm is created.



#### 4 Create a *Certificate Request*.



The screenshot shows a window titled "Create Certificate Request" with a red header bar. The window contains a light blue background with several text input fields on the right and their corresponding labels on the left. The labels are: "Country Name (2 letter code)", "State or Province (full name)", "Locality (full name)", "Organization (full name)", "Organizational Unit (section)", and "Common Name (DNS)". Below these fields is a large, empty rectangular box. At the bottom of the window, there are three buttons: "Send details", "Copy request", and "Close".

For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Purchasing a Certificate" on page [F-1](#).

Certificates can also be created and issued using an *Internal Certificate Authority*. For more information see "Using an Internal Certificate Authority" on page [8](#).



## 5 Install the certificate.



For more information, see the *RMX 1500/2000/4000 Administrator's Guide*, "Installing the Certificate" on page [F-3](#).

- 6 Set the RMX to *Secure Communication Mode*
  - a In the *RMX Management* pane, click **IP Network Services**.
  - b In the *IP Network Services* list pane, double click the **Management Network** entry.



The *Management Network Properties* dialog box is displayed.

**Management Network Properties**

> IP  
> Routers  
> DNS

Network Service Name: Management Network

IP Version: IPv4 & IPv6  
IPv6 Configuration Method: Manual

Control Unit IP Address:  
IPv4: 172.22.191.222  
IPv6: 2002:ac1b:184:0:230:64ff:fe04:d900/64 All

Shelf Management IP Address:  
IPv4: 172.22.191.221  
IPv6: fed0:1:184:1:290:caff:fe00:7c5d/64 All

Subnet Mask: 255.255.248.0

☒ Secured Communication

OK Cancel

- c Select the *Secured RMX Communication* check box.
- d Click **OK**.
- 7 Reset the RMX:
  - a In the *RMX Management* pane, click the **Hardware Monitor button**.  
The *Hardware Monitor* pane is displayed.
  - b Click the **Reset** (🔧) button.



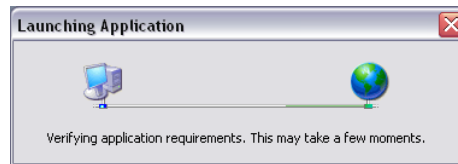
**8** Download and install the *RMX Manager*:

- a** Download the *RMX Manager* from the *Documents and Downloads* page of *Polycom's* web site:

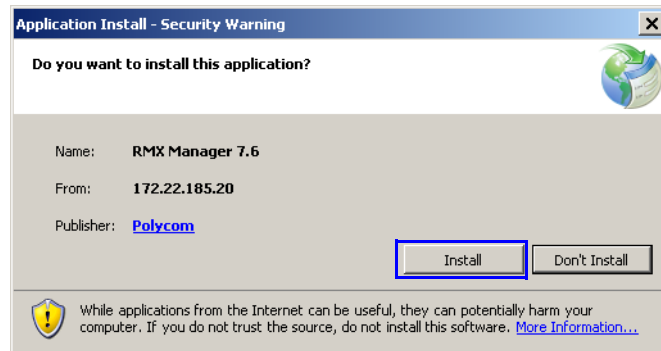
<http://support.polycom.com/PolycomService/home/home.htm>



Before installation the installer verifies the application's requirements on the workstation.



The *Install* dialog box is displayed.



- b** Click **Install**.

The installation proceeds.

When the installation completes, the application loads and the *RMX Manager – Welcome* screen is displayed.

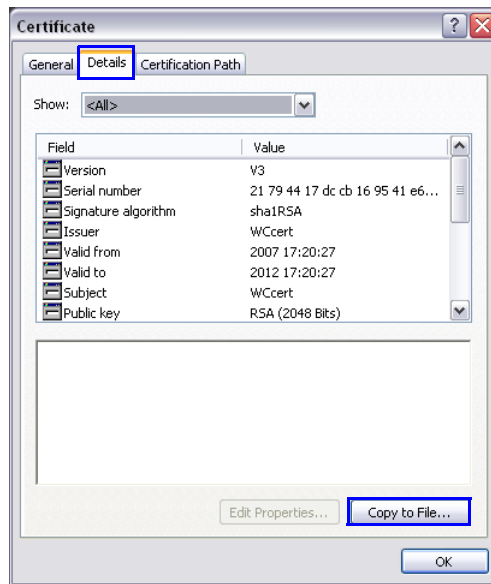


## Using an Internal Certificate Authority

If your TLS certificate was created and issued by an *Internal Certificate Authority*, it may not be seen as having been issued by a trusted *Certificate Authority*. The *RMX Manager* is not downloaded successfully and a warning is received stating that the certificate was not issued by a trusted *Certificate Authority*.

### To add the Internal Certificate Authority as a trusted Certificate Authority:

- 1 Navigate to the folder where the certificate (.cer) file is saved.
- 2 Open the certificate file.



- 3 Click the **Detail** tab.
- 4 Click the **Copy to File** button.



The *Certificate Export Wizard* is displayed.



- 5 Click the **Next** button.

The *Export File Format* dialog box is displayed.



- 6 Select **Base-64 encoded X.509 (.CER)**.
- 7 Click the **Next** button.



The *File to Export* dialog box is displayed.



- 8 In the *File Name* field, enter the file name for the exported certificate.
- 9 Click the **Next** button.
- 10 The final *Certificate Export Wizard* dialog box is displayed.



- 11 Click the **Finish** button.



The successful export message is displayed.



**12** Click the **OK** button.







# USB Operations

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

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

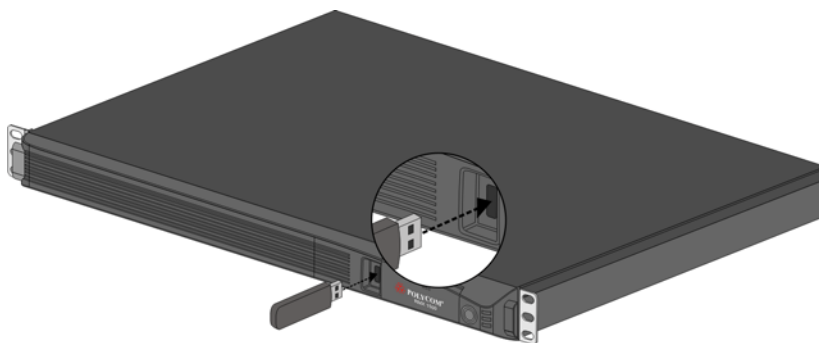
## USB Ports on RMX 1500/2000/4000



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

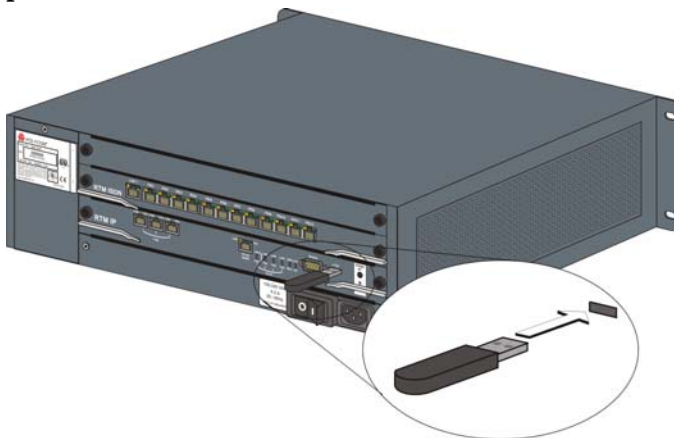
When performing *USB Operations*, the following *USB* ports are used:

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





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



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





## Restore to Factory Security Defaults

Restore to Factory Security Defaults can be performed by either:

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

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

- 1** Insert a *USB* device or a *USB* key containing a file named *RestoreFactorySecurityDefaults* into the *USB* port of the RMX.  
The *USB* port locations for RMX 1500/2000/4000 are shown in "*USB Ports on RMX 1500/2000/4000*" on page [4-1](#).
- 2** Power the RMX **Off** and then **On**.
- 3** Login using **http://<Control Unit IP Address>**.



## Comprehensive Restore to Factory Defaults

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

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

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

In addition all the conferencing entities are deleted:

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

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

## Comprehensive Restore to Factory Defaults Procedure

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

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

### **A Backup Configuration Files**

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



**B Restore to Factory Defaults**

- Restart the system with a *USB* device containing a file named *RestoreToFactoryDefault* and a *lan.cfg* file plugged into the *USB* port.
- Connect to the *RMX* using the *Alternate Management Network*.
- Apply the *Product Activation Key*.
- Unplug the *USB* device.
- Restart the *RMX*.

**C Restore the System Configuration From the Backup**

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

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

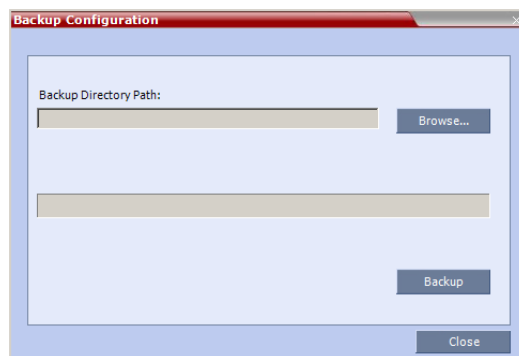
**Procedure A: Backup Configuration Files**

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

**To backup configuration files:**

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

The *Backup Configuration* dialog box opens.



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



## **Procedure B: Restore to Factory Defaults**

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

- 1** Configure a workstation for *Direct Connection*.
- 2** Connect the RMX to the workstation.
- 3** Insert a *USB* device containing a file named *RestoreToFactoryDefault* and a *lan.cfg* file into the *USB* port of the RMX.
- 4** Power the RMX **Off** and then **On**.
- 5** Connect to the *Alternate Management Network*.
- 6** Apply the *Product Activation Key*.
- 7** Unplug the *USB* device.
- 8** Restart the RMX.

### **Step 1: Configure a Workstation for Direct Connection**

The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

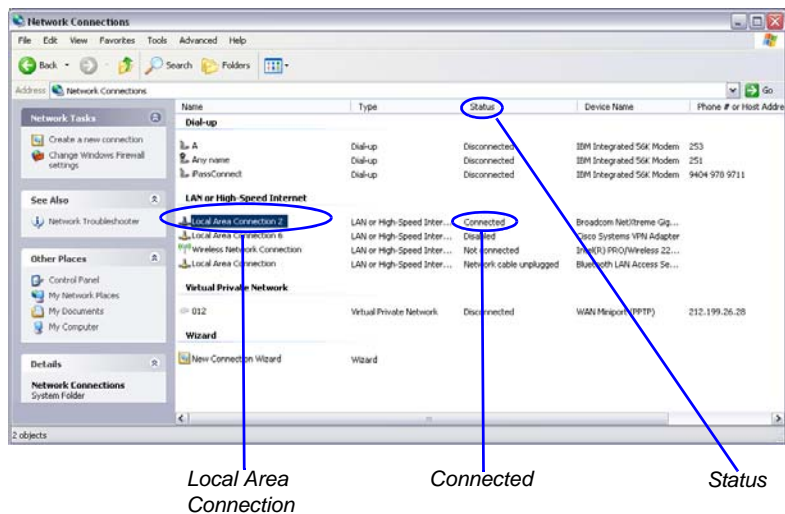
For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with the RMX's *Alternate Management Network*.

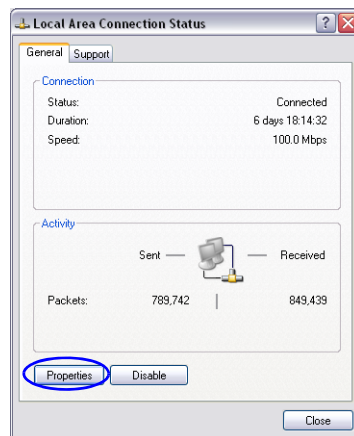
- a** On the Windows *Start* menu, select **Settings > Network Connections**.



- b** In the *Network Connections* window, double-click the **Local Area Connection** that has *Connected* status.

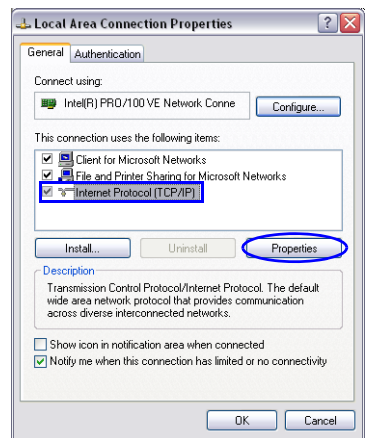


- c** In the *Local Area Connection Status* dialog box, click the **Properties** button.

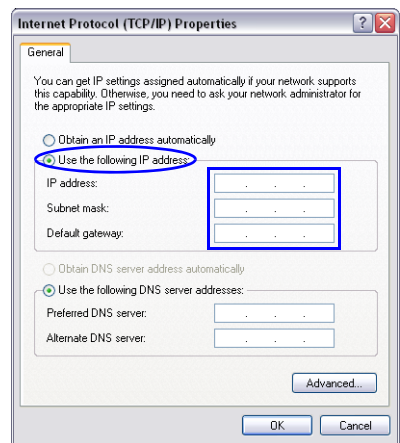




- d** In the *Local Area Connection Properties* dialog box, select **Internet Protocol [TCP/IP] > Properties**.



- e** In the *Internet Protocol (TCP/IP) Properties* dialog box, select **Use the following IP address**.
- f** Enter the *IP address*, *Subnet mask* and *Default gateway* for the workstation.





The workstation's IP address should be in the same network neighborhood as the RMX's *Control Unit* IP address.

**Example:** *IP address* – near **169.254.192.nn**



None of the reserved IP addresses listed in *Table 4-1* should be used for the IP Address.

The addresses needed for connection to the RMX's *Alternate Management Network* are listed in Table 4-1.

**Table 4-1**    *Reserved IP Addresses*

Network Entity	Alternate Network IP Address
<i>Control Unit IP Address</i>	169.254.192.10
<i>Control Unit Subnet Mask</i>	255.255.240.0
<i>Default Router IP Address</i>	169.254.192.1
<i>Shelf Management IP Address</i>	169.254.192.16
<i>Shelf Management Subnet Mask</i>	255.255.240.0
<i>Shelf Management Default Gateway</i>	169.254.192.1

**g** Click the **OK** button.

## **Step 2: Connect the RMX to the Workstation**

The *Alternate Management Network* enables direct access to the RMX for support purposes. The *Alternate Management Network* cannot be configured and operates according to factory defaults.

Access to the *Alternate Management Network* is via a cable connected to a workstation. The *Alternate Management Network* is accessible only via the



*LAN 3 port on the RMX 2000, the Modem port on the RMX 1500 and LAN 1 port on the RMX 4000.*

**RMX 1500**



**RMX 2000**



**RMX 4000**



>> Connect the cable between the RMX port and the LAN port configured on the workstation.

**Step 3: Insert a USB key containing a file named *RestoreToFactoryDefault* and a *lan.cfg* file into the USB port of the RMX**

The *USB* port locations for RMX 1500/2000/4000 are shown in "*USB Ports on RMX 1500/2000/4000*" on page 4-1.

**Step 4: Power the RMX Off and then On.**

**Step 5: Connect to the Alternate Management Network**

- Start the *RMX Web Client* application on the workstation, by entering `http://169.254.192.10` (the *Control Unit IP Address*) in the browser's address line and pressing **Enter**.



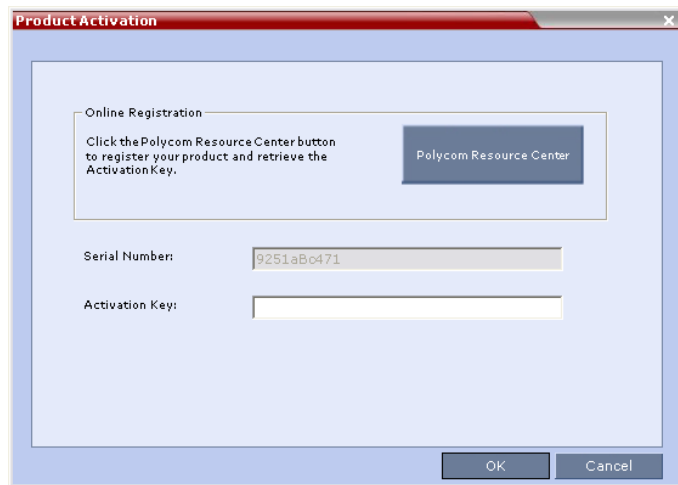
The *Login* dialog box is displayed.



- b** In the *RMX Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click **Login**.

#### Step 6: Apply the Product Activation Key

The *RMX Web Client* opens and the *Product Activation* dialog box appears with the serial number filled in.



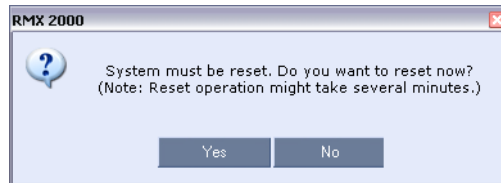
- a** In the *Activation Key* field, enter or **paste** the *Product Activation Key* obtained earlier.
- b** Click **OK**.



If you do not have an *Activation Key*, click **Polycom Resource Center** to access the *Service & Support* page of the Polycom website.

For more information, see "*Obtaining the Activation Key*" on page 1-9.

The system prompts with a restart dialog box:



#### Step 7: Unplug the USB device

>> Remove the *USB* device from the *USB* port of the *RMX*.

#### Step 8: Restart the RMX

>> In the restart dialog box, click **Yes**.

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

To restore configuration files:

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



# Emergency CRL (Certificate Revocation List) Update

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

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

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

## Emergency CRL Update Procedure



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



The *RMX* must be powered on before starting this procedure.

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

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



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

These files are saved on the workstation.



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

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

**Step 2: Disable Secure Communications mode**

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

The *USB* port locations for *RMX 1500/2000/4000* are shown in "*USB Ports on RMX 1500/2000/4000*" on page **4-1**.

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

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

Using the *RMX Manager*:

- c** In the *MCUs* list, select the *RMX* to be updated.
- d** In *MCU Properties*, change the *Port* number from **443** to **80**.
- e** Click **OK**.
- f** In the *MCUs* list, select the *RMX* to be updated.
- g** Right-click in the *MCUs* list entry and select **Connect**.
- h** Click **Accept** to accept the warning banner.
- i** Enter an administrator *Username* and *Password*.
- j** Click **OK**.

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

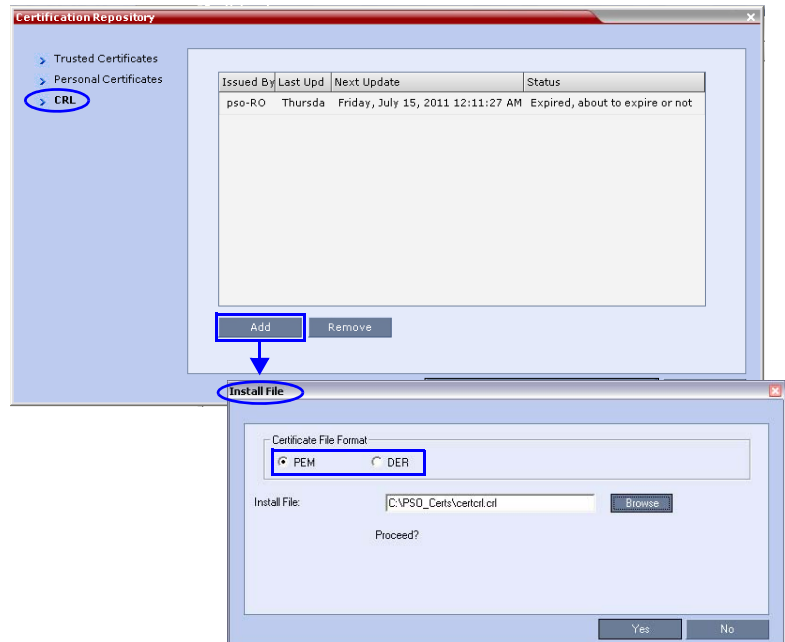
On the *RMX* menu, click **Setup > RMX Secured Communication > Certification Repository**.

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

In the *Certification Repository*:

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



**b Click Add.**

**c** In the *Install File* dialog box, select the **DER** or **PEM** format depending on which file format was chosen in *Step 1* of this procedure.

**d** Click the **Browse** button to navigate to the folder on the workstation where you saved the *CRL* files in *Step 1* of this procedure.

**e** Select the *CRL* file that you want to upload.

**f** Click **Yes** to proceed.

The system checks the *CRL* file and displays a message that the certificate was loaded successfully.

**g** Repeat Steps *d* through *f* until all of the required *CRL* files has been updated.

**Step 5: Update the repository.**

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

**a** Click **Update Repository**.

A repository update confirmation message is displayed.

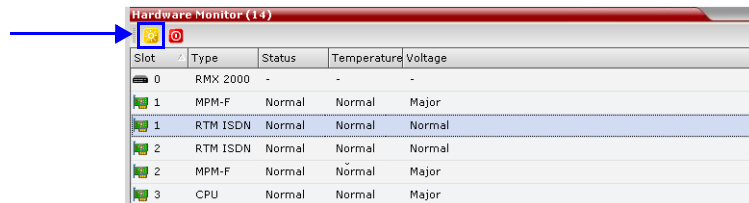


- b** Click **OK** to update the repository.

**Step 6: Re-connect to the RMX.**

- a** Remove the *USB* device that was connected in *Step 2a*.
- b** Restart the *RMX*.
- c** In the *RMX Management* pane, click the **Hardware Monitor** button.

The *Hardware Monitor* pane is displayed.



- d** Click the **Reset** button.

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

Using the *RMX Manager*:

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

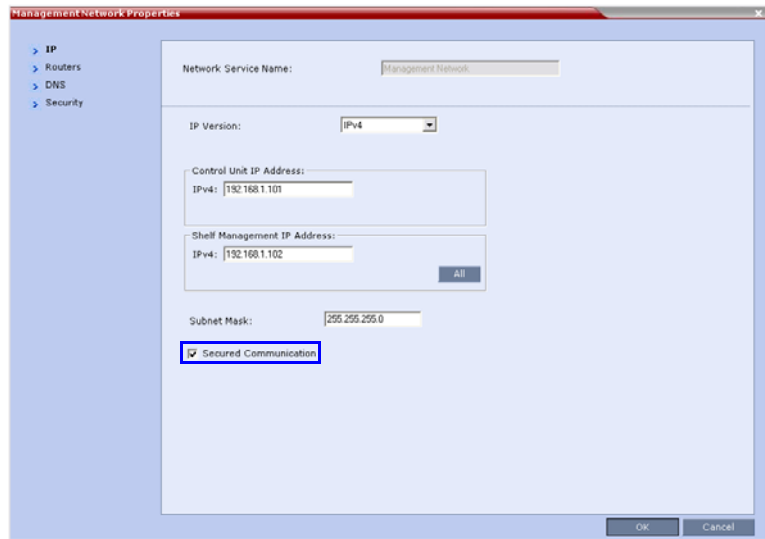
**Step 7: Re-enable Secured Communications Mode.**

Using the *RMX Manager*:

- a** In the *RMX Management* pane, click the **IP Network Services** button. (Depending on the *RMX Manager* configuration, you may have to click **Rarely Used** first.)
- b** In the *IP Network Services* list pane, double-click **Management Network**.



The *Management Network Properties* dialog box is displayed.



**c** Select the *Secured Communication* check box.

**d** Click **OK**.

A message informs you that your session will be disconnected and that you must re-connect the RMX using **https** in the browser *URL*.

**e** Click **OK**.

A system restart confirmation message is displayed.

**f** Click **Yes** to restart the RMX.

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

**g** In the *MCUs* list, select the RMX to be updated.

**h** In *MCU Properties*, change the *Port* number from **80** to **443**.

**i** Click **OK**.







The diagram illustrates a converged network architecture, divided into two main functional areas by a vertical line. The left area represents the core network and management, while the right area represents the edge network and endpoints.

**Core Network and Management (Left Side):**

- RMX 1500/2000/4000:** A central router or switch unit.
- IP Management (HTTPS):** A management workstation connected to the RMX.
- RMX Management Network (HTTPS):** A network connecting the management workstation to the RMX.
- Serial S4GW:** A serial gateway connected to the RMX.
- IP (H.323):** Connections from the RMX to the edge network.
- ISDN PRI (T1/E1):** A connection from the RMX to the DSN.

**Edge Network and Endpoints (Right Side):**

- DSN (Data Service Network):** A cloud representing the data network, connected to the RMX via ISDN PRI (T1/E1) and to the edge network via IP.
- IP Switch:** A switch connecting the DSN to the IP cloud.
- IP (H.323):** A connection from the IP cloud to the edge network.
- Endpoint:** A device (laptop or phone) connected to the edge network via IP (H.323).
- ISDN BRI:** A connection from the DSN to the edge network via ISDN BRI.
- Analog Phone Line:** A connection from the DSN to the edge network via an analog phone line.
- ISDN Phone:** A device connected to the edge network via ISDN BRI.

The diagram shows how a single network infrastructure can support multiple services, including voice (ISDN, Analog), data (IP), and management (HTTPS).

**5-1**



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

## Guidelines

- The *Serial Gateway* is supported on RMX 1500/2000/4000.
- Only one *Serial Gateway* can be connected directly to an RMX.
- The *Serial Gateway* can be associated with only one *Network Service*.
- Although the *Media* and *Signaling Network Service* on the RMX can be configured for *IPv6* addressing, the *Network Service* assigned to the *Serial Gateway* can only support *IPv4* addressing..
- The following *System Flags* must be set to **YES**:
  - **ULTRA\_SECURE\_MODE**
  - **V35\_ULTRA\_SECURED\_SUPPORT**
- When connecting the *Serial Gateway* to an RMX 2000:
  - It is essential that an *RTM LAN* card is installed.
  - The *Serial Gateway* must be physically connected to the *RTM LAN* card, *LAN 1* port.
  - The **SEPARATE\_MANAGEMENT\_NETWORK** *System Flag* must be set to **YES**.
- The **MULTIPLE\_SERVICES** *System Flag* must be set to **NO**.
- If *Content* is to be shared the conference *Profile* should have *Content Protocol* set to **H.263**.
- When the RMX is in *Ultra Secure Mode*, it requires that the *Serial Gateway* be in *Maximum Security Mode*. For more information see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments*, “*Serial Gateway S4GW - Maximum Security Mode*” on page **5-15**.
- *H.323* connections to the RMX are 1024-bit encrypted *TLS*.
- The *Certificate* installed on the *Serial Gateway* must be also be installed in the workstation that is used to run the *RMX Web Client / RMX Manager*.



## Configuring the RMX - Serial Gateway Connection

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

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

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

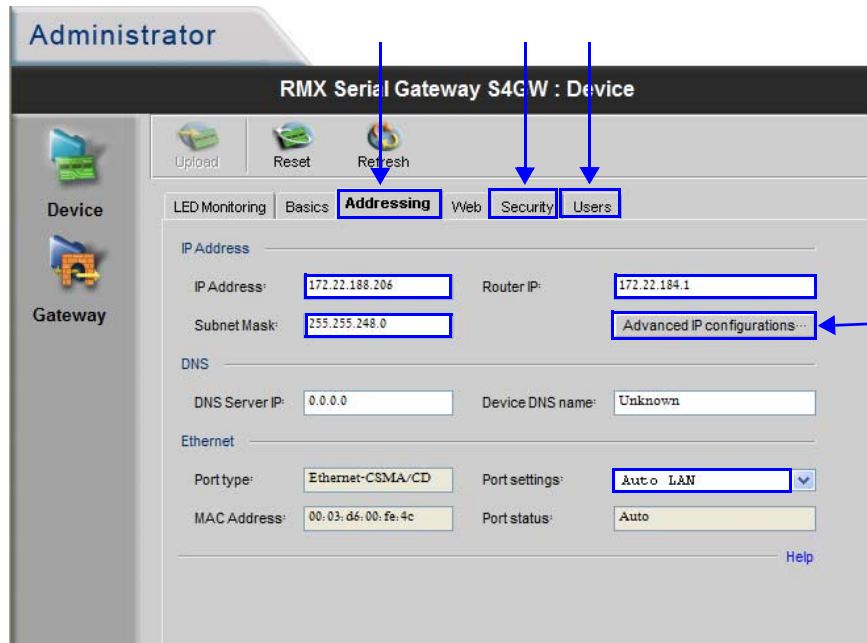
### **2 Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX**

## Procedure 1: Initial Setup of the Serial Gateway

- 1** Establish a serial connection between the *Serial Gateway* and the workstation. For more information see “*Setting Up Your Polycom RMX Serial Gateway S4GW*” in the *RMX Serial Gateway S4GW System User Guide*.
- 2** In the *Administrator > Device > Addressing* dialog box, enter IP addresses in the following fields:
  - *IP Address* (Signaling and Media). The RMX will use this IP address to connect to the *Serial Gateway's* management interface.
  - *Router IP*
  - *Subnet Mask*.



- 3 In the *Port settings* field, select **Auto LAN**. (If configured as *100 Mbps/ Full Duplex* while directly connected to the RMX, the Serial Gateway network adapter is disabled until the cable is disconnected and reconnect to the RMX.)



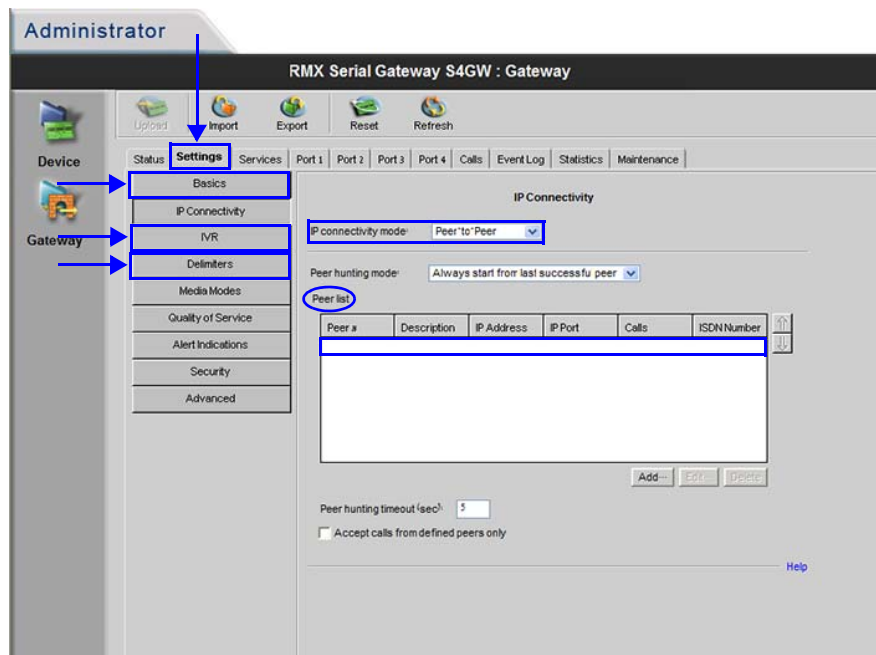
- 4 Click the **Advanced Configurations** button and verify that:
  - *VLAN Tagging* is **disabled**
  - *Use different interface for media and signaling* is **disabled**.
 If they are not disabled, disable them.
- 5 Select the **Security** tab.
- 6 Set the *Security Mode* to **Maximum**.
- 7 Select the **Users** tab.
- 8 Create the user account that the RMX will use to connect to the *Serial Gateway*.
- 9 Click **Administrator > Gateway > Settings > IP Connectivity > Peer list**.



**10** In the *Peer List*:

- a** Add the **V.35 Gateway Service Signaling Host IP Address** to the *Serial Gateway's Peer list*.
- b** Remove all other addresses.

**11** Click the **Upload** button to save the changes.



**12** Click the **Delimiters** tab.

- a** Set the delimiter to **#**.

**13** Click the **Media Modes** tab.

- a** Un-check **Enable H.263+**.
- b** Un-check **Enable T.120**.

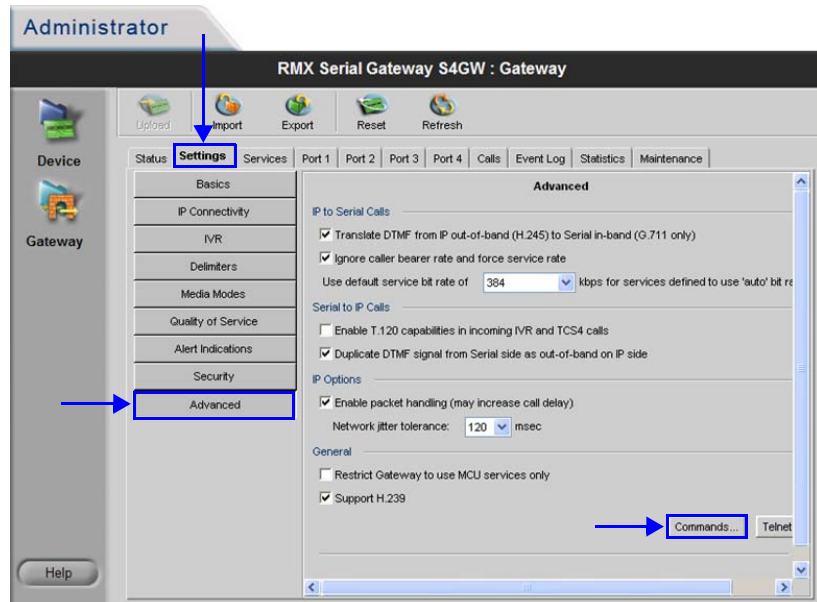
**14** Click the **Security** tab.

- a** Select **Independent**.



**15** Click the **Upload** button to save the changes.

**16** Click the **Advanced** tab.



**a** Verify the following settings:

- **IP to Serial calls:**
  - *Translate DTMF from IP...* **Selected.**
  - *Ignore caller bearer...* **Selected.**
  - *Use default service bit rate of* **384 kbps.**
- **Serial to IP calls:**
  - *Enable T.120 capabilities ...* **Cleared.**
  - *Duplicate DTMF signal ...* **Selected.**
- **IP Options:**
  - *Enable packet handling...* **Selected.**
  - *Network jitter tolerance...* **120 msec.**
- **General:**
  - *Restrict Gateway to use ...* **Cleared.**
  - *Support H.239* **Selected.**



**17** Click the **Commands** button.

Enter the advanced commands as set out in Table 5-1.

**Table 5-1** *Maximum Security - Advanced Command Settings*

<b>Advanced Command</b>	<b>Status message</b>	<b>Status After Setting/ Enable</b>
<i>advancedsecuritymode</i>	Advanced Security Mode is currently <b>DISABLED</b>	Advanced Security mode - <b>ENABLED</b>
<i>embeddedMode</i>	<b>ENABLED</b>	
<i>daysForPassword ExpireNotification</i>	Number of days till password expiration is set to <b>7</b>	<b>NO CHANGE NEEDED</b>
<i>h239OlcPatch</i>	<b>ENABLED</b>	
<i>IsdnCapsTimeout</i>	<b>15</b>	
<i>lowerCaseMinimum</i>	Minimum lower case chars in password is set to <b>2</b>	<b>NO CHANGE NEEDED</b>
<i>MinNumberOfChangedChars</i>	Minimum number of changed chars in password is set to <b>4</b>	<b>NO CHANGE NEEDED</b>
<i>NumberOfRepeatChars Allowed</i>	Number of repeated chars in password is set to <b>2</b>	<b>NO CHANGE NEEDED</b>
<i>numericalChars Minimum</i>	Minimum numerical chars in password is set to <b>2</b>	<b>NO CHANGE NEEDED</b>
<i>passwordChange MinimumTime</i>	Minimum time between password changes is <b>1</b>	<b>NO CHANGE NEEDED</b>

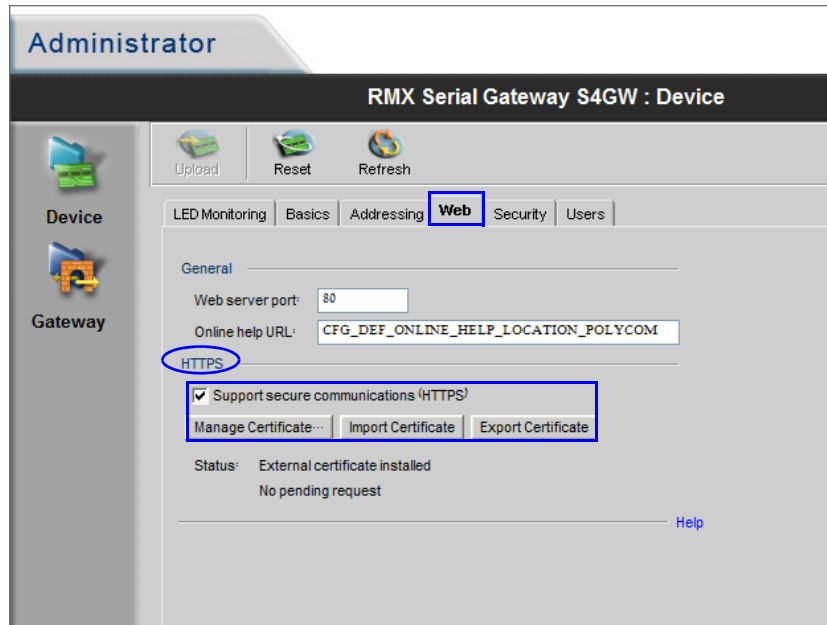


**Table 5-1** Maximum Security - Advanced Command Settings (Continued)

Advanced Command	Status message	Status After Setting/ Enable
<i>passwordReuseBuff Size</i>	The size of the re-usebuffer is <b>10</b>	NO CHANGE NEEDED
<i>SpecialCharsMinimum</i>	Minimum special chars in password is set to <b>2</b>	NO CHANGE NEEDED
<i>upperCaseMinimum</i>	Minimum upper case chars in password is set to <b>2</b>	NO CHANGE NEEDED

- a** Set the command **embeddedMode** to **Enable**
- b** Set the command **IsdnCapsTimeout** to **15**
- c** Set the command **h239OlcPatch** to **Enable**
- 18** For each port in use, clear **IVR** check box.
- 19** Click the **Upload** button to save the changes.
- 20** Click **Administrator > Device > Web**:
  - a** Use the buttons to install a *TLS Certificate*.  
For more information see the *Polycom RMX Serial Gateway S4GW User Guide*, "Enabling HTTPS" on page **54**.
  - b** Select the **Support Secure Communications (HTTPS)** check box.
- 21** Request a *Web SSL* certificate:
  - a** Click **Device > Web Tab> Manage Certificate**.
  - a** Select the **Manage Certificate** button and follow the prompts to request the certificate.
- 22** Install the *Web SSL* certificate:
  - a** Click **Device > Web > Manage Certificate**.
  - a** Select the **Manage Certificate** button



**b Select Process Pending Request.****23** Set the *Serial Gateway* to *Maximum Security Mode*:

- a** In the *Gateway* interface, on the sidebar, click **Device**.
- b** Click the **Security** tab.
- c** In the *Security mode* field, select **Maximum** (no *Telnet*, *ftp*, *SNMP* and *ICMP*)

**24** Verify the *Advanced Settings* for *Maximum Security Mode*:

- a** On the sidebar, click **Gateway**.
- b** Click the **Settings** tab.
- c** Click **Advanced >> Commands**.

The *Advanced Settings* dialog box is displayed.

- d** Enter the *Advanced Commands* in Table 5-2 and observe the returned *Status Messages*. If necessary, modify the settings to match those listed in the table.

For a full list of *Advanced Commands*, see page 5-16.



**Table 5-2** Maximum Security - Advanced Command Settings

Advanced Command	Status message	Status After Setting/ Enable
<i>advancedsecuritymode</i>	Advanced Security Mode is currently <b>DISABLED</b>	Advanced Security mode - ENABLED
<i>embeddedMode</i>	<b>ENABLED</b>	
<i>daysForPassword ExpireNotification</i>	Number of days till password expiration is set to <b>7</b>	NO CHANGE NEEDED
<i>h2390lcPatch</i>	<b>ENABLED</b>	
<i>IsdnCapsTimeout</i>	<b>15</b>	
<i>lowerCaseMinimum</i>	Minimum lower case chars in password is set to <b>2</b>	NO CHANGE NEEDED
<i>MinNumberOfChangedC hars</i>	Minimum number of changed chars in password is set to <b>4</b>	NO CHANGE NEEDED
<i>NumberOfRepeatChars Allowed</i>	Number of repeated chars in password is set to <b>2</b>	NO CHANGE NEEDED
<i>numericalChars Minimum</i>	Minimum numerical chars in password is set to <b>2</b>	NO CHANGE NEEDED
<i>passwordChange MinimumTime</i>	Minimum time between password changes is <b>1</b>	NO CHANGE NEEDED
<i>passwordReuseBuff Size</i>	The size of the re-usebuffer is <b>10</b>	NO CHANGE NEEDED



**Table 5-2** *Maximum Security - Advanced Command Settings (Continued)*

Advanced Command	Status message	Status After Setting/ Enable
<i>SpecialCharsMinimum</i>	Minimum special chars in password is set to <b>2</b>	NO CHANGE NEEDED
<i>upperCaseMinimum</i>	Minimum upper case chars in password is set to <b>2</b>	NO CHANGE NEEDED

- 25** Click the **Upload** button to save the changes.  
The *Serial Gateway* will re-start.

The *Initial Setup* of the *Serial Gateway* is complete and it is ready to be disconnected from the workstation and connected to the RMX.

- 26** Disconnect the *Serial Gateway* from the workstation.

## Procedure 2: Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX

- 1** In the RMX menu, click **Setup > System Configuration**.
- 2** Set the following *System Flags*:
  - **ULTRA\_SECURE\_MODE = YES**
  - **SEPARATE\_MANAGEMENT\_NETWORK = YES**  
(RMX 2000 only)
  - **V35\_ULTRA\_SECURED\_SUPPORT = YES**
  - **ENABLE\_EPC = NO** (If this *System Flag* doesn't exist it must be manually added.)
  - **MULTIPLE\_SERVICES = NO**
- 3** Re-start the RMX.



- 4 Connect the *LAN* cable from the front of the *Serial Gateway* to the *LAN 1* port on the *RTM LAN* card.
- 5 In the *RMX Management* pane, click **Rarely Used** and click **IP Network Services**.
- 6 In the *IP Network Services* list pane click the **New IP Service** icon. The *New IP Service* dialog box is displayed.

The screenshot shows the 'Properties' dialog box for IP Network Services. The left pane has 'IP' selected under 'Networking'. The main area contains the following fields:

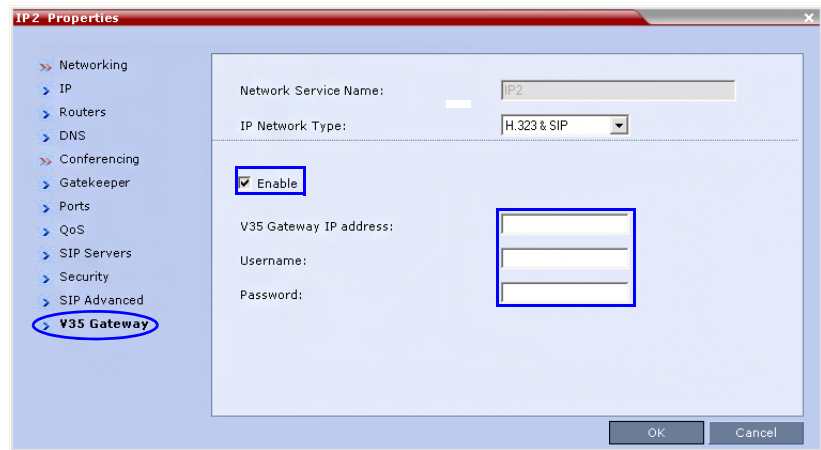
- Network Service Name: SerialGW
- IP Network Type: H.323
- Signaling Host IP Address: IP v4: 10.1.150, IP v6: [empty]
- Media Card 1 Port 1 IP Address: IP v4: 0.0.0.0, IP v6: [empty]
- Media Card 2 Port 1 IP Address: IP v4: 10.1.151, IP v6: [empty]
- Subnet Mask: 255.255.255.0
- Media Card 1 Port 2 IP Address: IP v4: 0.0.0.0, IP v6: [empty]
- Media Card 2 Port 2 IP Address: IP v4: 0.0.0.0, IP v6: [empty]

At the bottom, there is a 'Service Configuration' button and 'OK' and 'Cancel' buttons.

- 7 In the *IP* tab:
  - a Enter an *IP Network Service Name*.
  - b Enter a *Signaling Host IP Address* that is on the same *VLAN* as the *Serial Gateway Management* address.
  - c Enter a *Media Card 2 Port 1 IP Address* that is on the same *VLAN* as the *Serial Gateway Management* address.
- 8 Click the **Routers** tab.
- 9 Enter a *Default Router IP Address* that is on the same *VLAN* as the *Serial Gateway Management* address.
- 10 Click the **V35 Gateway** tab.



The network service *Properties* dialog box is displayed. The *Enable* field is selected and cannot be un-checked.



**11** Modify the following fields:

**Table 5-3** Network Service - V35 tab

Field	Description
<i>V35 Gateway IP Address</i>	Enter the <i>Management IP</i> address of the management interface of the <i>Serial Gateway</i> .
<i>Username</i>	Enter the <i>User Name</i> that the <i>RMX</i> uses to log in to the management interface of the <i>Serial Gateway</i> .
<i>Password</i>	Enter the <i>Password</i> that the <i>RMX</i> uses to log in to management interface of the <i>Serial Gateway</i> .

**12** Click **OK**.

A *Reset Confirmation* dialog box is displayed

**13** Click **Yes**.

**14** After the *RMX* has restarted, log in.

**15** Modify the *Video Quality* tabs of all conference *Profiles*, by changing the *Content Video Definition - Content Protocol* setting of all conferences to **H.263**.



## Testing

The following procedure can be used to test dialing procedures when using an *Adtran Gateway* for *ISDN* to *V.35*.



When using an *Adtran Gateway* the *Conference Profile* should have *Content Protocol* set to *H.263*, not *H.264*.

### Dialing to the RMX from an ISDN Endpoint

To dial to the RMX from an ISDN endpoint:

**Dial String:** <ISDN Number of AdTran>##<Conference\_Room\_Number>

**Example:** 5556789##4000



- The *Conference Profile* should have *Content Protocol* set to *H.263*, not *H.264*.
- The password can be entered via DTMF from the endpoint (HDX).

### Dialing to an ISDN Endpoint from the RMX

To dial to an ISDN endpoint from the RMX

**IP Address:** The IP address of the *Serial Gateway*

**Alias Name /Type:** <service prefix><ISDN Number><AdTran suffix> and select **Participant Number**

The first number in the *AdTran* suffix is the bit rate (#3 for 56kbps, #4 for 64kbps).

The second number in *AdTran* suffix is the number of *B Channels*.



**Example:** The dial string 38468824003#4#6 indicates **6 B Channels** of **64kbps** for a 384kbps call.

The screenshot shows the 'V.35 EP Properties' dialog box. On the left is a sidebar with three expandable sections: 'General', 'Advanced', and 'Information'. The 'General' section is currently expanded. The main area contains several fields: 'Name' (with 'V.35 EP' entered), 'Dialing Direction' (set to 'Dial out'), 'Type' (set to 'H.323'), 'IP Address' (set to '10.1.1.10'), 'Alias Name / Type' (containing '3846824003#4#6' and a 'Participant Number' dropdown), 'Website IP Address' (empty), an 'Audio Only' checkbox (unchecked), and 'Extension/Identifier String' (empty). The 'Alias Name / Type' field is highlighted with a blue border.



# Advanced Commands

**Table 5-4** Advanced Commands

Command	Parameters	Description	Default
<i>Advanced Security Mode</i>	ENABLE	<p>This command puts the Gateway in MAXIMUM security mode. Used by: CS</p> <p>Available Since V5.7.2.0.7</p>	The default of the Gateway will be in MINIMUM security mode , but once the user sets the Gateway to Maximum security the only way to go back to Standard security is by the 'Setting Factory Defaults' procedure.
<i>Session Inactivity Enabled Timeout</i>	5-60 minutes	<p>Sets the Inactivity timeout value. Web will disconnect from GW if user is inactive for this period of time.</p> <p>Available Since V5.7.2</p>	10 minutes
<i>password Change Minimum Time</i>	1-30 days	<p>Sets the minimum number of days needed to pass before User can change his/her own password. This value is not valid for administra-tors</p> <p>Available Since V5.7.2</p>	1 day



**Table 5-4** Advanced Commands (Continued)

Command	Parameters	Description	Default
<i>minimum Password Length</i>	8-15	Sets the minimum length of a valid password  Available Since V5.7.2	15
<i>upperCase Minimum</i>	1-2	Sets the minimum number of upper case characters needed for a valid password.  Available Since V5.7.2	2
<i>lowerCase Minimum</i>	1-2	Sets the minimum number of lower case characters needed for a valid password.  Available Since V5.7.2	2
<i>Numerical Chars Minimum</i>	1-2	Sets the minimum number of numerical characters needed for a valid password.  Available Since V5.7.2	2
<i>Special Chars Minimum</i>	1-2	Sets the minimum number of special characters needed for a valid password.  Available Since V5.7.2	2
<i>NumberOf Repeat Chars Allowed</i>	1-4	Sets the number of repeated characters allowed in valid password.  Available Since V5.7.2	2
<i>Min NumberOf Changed Chars</i>	1-4	Sets the minimum number of characters needed to change when setting new password.  Available Since V5.7.2	4



**Table 5-4** Advanced Commands (Continued)

Command	Parameters	Description	Default
<i>daysFor Password Expire Notification</i>	1-7	Sets the number of days before password expires that a 'password expiration notice' will be shown to user.  Available Since V5.7.2	7
<i>password ReuseBuff Size</i>	8-16	Sets the number of passwords saved to check for reuse. i.e. if the buffer is set to 10, then the user cannot re-use any of the last 10 passwords.  Available Since V5.7.2	10
<i>user LockedOut Duration</i>	0-480 minutes	Sets the number of minutes before user that was locked out will be automatically released. Value of 0 – means indefinite.  Available Since V5.7.2	0
<i>user Session Limit</i>	1-10 sessions	Sets the number of simultaneous sessions per user allowed.  Available Since V5.7.2	5
<i>auditLog Threshold</i>	10 -100 percent of log capacity	Sets the audit log threshold, so that when this value is reached an audit log overflow trap is sent.  Available Since V5.7.2	70
<i>Password Expiration Timeout</i>	30-180 days	Sets the number of days till password will expire.  Available Since V5.7.2	60



**Table 5-4** *Advanced Commands (Continued)*

Command	Parameters	Description	Default
<i>User Lockout Failures Interval</i>	60-1440 minutes. (1440 = 24 hours)	Period of time in which the failed login threshold must be exceeded the lock the users account.  Available Since V5.7.2	60
<i>User Lockout MaxFailure</i>	2-10	Sets the number of login failures needed to lockout user. Failed login threshold.  Available Since V5.7.2	3



