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

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

This software has achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 8.5.10 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

Support Information
For support on your Polycom systems, contact Polycom Global Services at 1-888-248-4143 or go to the Polycom Support Contact page (http://support.polycom.com/PolycomService/support/us/support/Contact_Us.html).

Documentation Feedback
Polycom appreciates your help as we work to improve its product documentation. Send your comment to videoinformationdesign@polycom.com.

© 2013-2016 Polycom, Inc. All rights reserved.
Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
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.
Document Change History

This information is required for listing on the US Department of Defence (DoD) Unified Capabilities (UC) Approved Products List (APL):

<table>
<thead>
<tr>
<th>Doc Version</th>
<th>Release Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>January 2014</td>
<td>Initial approved release</td>
</tr>
<tr>
<td>2.0</td>
<td>June 2014</td>
<td>RMX 8.3 update</td>
</tr>
<tr>
<td>3.0</td>
<td>July 2015</td>
<td>RMX 8.4.2 update</td>
</tr>
<tr>
<td>4.0</td>
<td>April 2016</td>
<td>RMX 8.5.10 update</td>
</tr>
</tbody>
</table>

CONDITION OF FIELDING.

When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites’ Designated Approving Authority:

a  The system must be incorporated in the site’s PKI. If PKI is not incorporated, the following findings will be included in the site’s architecture:
   ◆  APP3305, CAT I (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000
   ◆  APP3280, CAT II (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000
   ◆  APP3290, CAT II (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000
   ◆  APP3300, CAT II (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000
   ◆  DSN13.17, CAT II (x4), RMX 1500, RMX 2000, RMX 4000
   ◆  NET0445, CAT II (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000

b  The system must be integrated into the site’s AD environment for authentication and authorization requirements.
   ◆  APP3390, CAT I (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000
   ◆  APP3400, CAT II (x5), RMX 1500, RMX 2000, RMX 4000, DMA 7000

c  The site must use a STIG-compliant, PK-enabled workstation for management of the solution.

d  The configuration must be in compliance with the Polycom RMX Family military-unique features deployment guide.

Contents

First Time Installation and Configuration ........................................... 1
  Workstation Requirements ......................................................... 1
  Required IT Infrastructure ....................................................... 2
    DNS .................................................................................. 2
    NTP Servers ...................................................................... 2
    Certificate Authority Server ................................................. 3
  RMX Hardware ....................................................................... 3
  First Time Installation and Configuration ..................................... 3
  Upgrading to Version 8.5.10 ....................................................... 4
  Procedure 1: Hardware Installation and Setup ................................ 4
    Installing the Telescopic Rail Runners on the Rack ...................... 5
    Telescopic Rail Runners Accessory Kit ...................................... 5
    Telescopic Rail Runner Assembly .......................................... 6
    Installing the RMX 1500 ......................................................... 10
    Installing the RTM ISDN 1500 Card on the RMX 1500 (Optional) ... 10
    Mounting the Collaboration Server 1500 in a Rack ..................... 12
    Connecting Cables to the RMX 1500 ........................................ 12
    Installing the RMX 2000 ......................................................... 13
    Installing the RTM ISDN Card on the RMX 2000 ......................... 14
    Mounting the Collaboration Server 2000 in a Rack ..................... 14
    Connecting Cables to the RMX 2000 ........................................ 15
    Installing the RMX 4000 ......................................................... 16
      Optional. Installing the RTM ISDN Card on the RMX 4000 ............ 16
      Mounting the Collaboration Server 4000 in a Rack .................... 17
      Connecting the RMX 4000 to the Power Sources ...................... 19
      Connecting Cables to the RMX 4000 ...................................... 20
  Procedure 2: Gather Network Equipment and Address Information ........ 22
  IP Services ........................................................................ 22
    Management Network .......................................................... 22
    Signaling Network ............................................................... 22
    ISDN/PSTN Services ............................................................ 23
  First Time Setup Worksheet ....................................................... 23
<p>| Procedure 3: First Entry Configuration | 27 |
| Register the RMX | 27 |
| Obtain Product Activation Key for the RMX | 27 |
| Download and Install the RMX Manager Onto a Workstation | 27 |
| Connect the Workstation to the Default Management Network | 29 |
| Configuring the workstation for direct connection | 29 |
| Connect the Workstation to the RMX | 31 |
| Power up the RMX | 32 |
| Login to the RMX | 32 |
| Activate the RMX Product | 33 |
| Modify the Default Management Network | 34 |
| Modifying the Signaling Network Service | 35 |
| Fast Configuration Wizard | 36 |
| Configure the ISDN/PSTN Network Service | 42 |
| Configure the DNS for the Management Network: | 51 |
| Procedure 4: Enable Ultra Secure Mode | 52 |
| Connecting to the RMX | 53 |
| Procedure 5: Enable Network Separation (RMX 2000) | 54 |
| Enabling Network Separation | 55 |
| Procedure 6: Enable Secured Communication | 56 |
| Installing Certificates and Enabling Secure Communications | 56 |
| Installing a Certificate | 57 |
| Installing Certificates for the Management Network Service | 58 |
| Installing Certificates for the IP Network Service | 63 |
| Installing the Certificates | 63 |
| Installing the RMX Certificates | 64 |
| Installing the Trusted Certificate(s) | 65 |
| Installing the CRLs | 66 |
| Certificate Revocation | 67 |
| Switching to Secure Communication Mode | 69 |
| Procedure 7: Optional. Configure SIP/AS-SIP for the Signaling Network | 70 |
| Procedure 8: Set System Configuration Flags | 72 |
| Modifying Flag Values | 77 |
| Procedure 9: Optional. Configure 802.1X Authentication | 78 |
| Procedure 10: Configure Precedence (DSCP) and QOS | 80 |
| Procedure 11: Configure IVR Settings | 81 |
| Procedure 12: Optional. Modify Default Login and Main Screen Banner Text | 83 |
| Login Screen Banner | 83 |
| Main Screen Banner | 84 |
| Customizing Login and Main Screen Banners | 84 |</p>
<table>
<thead>
<tr>
<th>Procedure 13: Rename the Default POLYCOM User</th>
<th>85</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure 14: Disable Inline AutoComplete Option in Web Browser</td>
<td>86</td>
</tr>
<tr>
<td>Procedure 15: Configure Whitelist Access</td>
<td>87</td>
</tr>
<tr>
<td>Procedure 16: Configure Gateway Services</td>
<td>89</td>
</tr>
</tbody>
</table>

**Basic Operation**

- Starting the RMX Manager: 90
- Connecting to the MCU: 92
- Login Record: 93

**RMX Manager Screen Components**

- MCUs Pane: 95
- Conferences List: 97
- List Pane: 97
- RMX Management: 97
- Status Bar: 97
- System Alerts: 98
- Participant Alerts: 98
- Port Usage Gauges: 99
- MCU State: 100

**Address Book**

- Displaying and Hiding the Address Book: 101

**Conference Templates**

- Displaying and Hiding Conference Templates: 101

**Adding MCUs to the MCUs List**

- Customizing the Main Screen: 104

**Starting a Conference**

- Starting a Conference from the Conferences Pane: 106
- General Tab: 107
- Participants Tab: 108
- Information Tab: 111

**Starting a Reservation**

- Starting an Ongoing Conference From a Template: 114

**Connecting to a Conference**

- Direct Dial-in: 116
- H.323 Participants: 116
- Entry Queue Access: 117
- H.323 Participants: 118
- ISDN and PSTN Participants: 118
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialing to the RMX from an ISDN Endpoint</td>
<td>156</td>
</tr>
<tr>
<td>Dialing to an ISDN Endpoint from the RMX</td>
<td>156</td>
</tr>
<tr>
<td>Serial Gateway S4GW - Maximum Security Mode</td>
<td>157</td>
</tr>
<tr>
<td>Advanced Commands</td>
<td>159</td>
</tr>
<tr>
<td><strong>Restoring the RMX Using the USB Port</strong></td>
<td>161</td>
</tr>
<tr>
<td>Recovery Operations Performed Using a USB Device</td>
<td>162</td>
</tr>
<tr>
<td>Comprehensive Restore to Factory Defaults</td>
<td>163</td>
</tr>
<tr>
<td>Procedure Summary for Performing a Comprehensive Restore to Factory Defaults:</td>
<td>163</td>
</tr>
<tr>
<td>Detailed Procedure for Performing a Comprehensive Restore to Factory Defaults:</td>
<td>164</td>
</tr>
<tr>
<td>Emergency CRL (Certificate Revocation List) Update</td>
<td>169</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>174</td>
</tr>
<tr>
<td>Collaboration Server Web Client Installation - Troubleshooting Instructions</td>
<td>174</td>
</tr>
<tr>
<td>Procedure 1: Ending all Internet Explorer Sessions</td>
<td>175</td>
</tr>
<tr>
<td>Procedure 2: Deleting the Temporary Internet Files, RMX Cookie and RMX Object</td>
<td>176</td>
</tr>
<tr>
<td>Deleting the Temporary Internet Files</td>
<td>176</td>
</tr>
<tr>
<td>Deleting the RMX/Collaboration Server Cookie</td>
<td>178</td>
</tr>
<tr>
<td>Deleting the RMX/Collaboration Server ActiveX Object</td>
<td>180</td>
</tr>
<tr>
<td>Procedure 3: Managing Add-ons Collisions</td>
<td>181</td>
</tr>
<tr>
<td>Procedure 4: Add the Collaboration Server to the Internet Explorer Trusted Sites List</td>
<td>181</td>
</tr>
<tr>
<td>Procedure 5: Browser Hosting Controls (Optional)</td>
<td>183</td>
</tr>
</tbody>
</table>
First Time Installation and Configuration

This software, when configured per the guidance provided in this guide, is designed to meet the latest U.S. Department of Defense (DoD) security requirements for listing on the Unified Capabilities (UC) Approved Products List (APL) as maintained by the Defense Information Systems Agency (DISA) Unified Capabilities Connection Office (UCCO). For more information about the UC APL process, please visit the UCCO website.

This document provides guidance for configuring and using software version 8.5.10 to be consistent with the conditions for deployment as listed in the UC APL listing for the Polycom Realpresence Collaboration Server (RMX) product. For a listing of certified software versions in addition to version 8.5.10, refer to http://www.polycom.com/solutions/solutions-by-industry/us-federal-government/certification-accreditation.html

Do not insert a USB device into the RMX’s USB port unless it is your intention to disable Secured Mode or perform a Comprehensive Restore to Factory Defaults.

Workstation Requirements

The RMX Manager application 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.
- 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 added to Internet Explorers Local Intranet Zone or added to the trusted sites list. In both cases, the ActiveX control will install properly.
Management of the RMX using the RMX Web Client (not recommended) requires the installation of ActiveX. In deployments were ActiveX is prohibited, administrators must use the RMX Manger.

For users deploying a RMX Serial Gateway S4GW, the VIEW_RVGW_ACTIVEX System Flag can be added and its value modified to determine if ActiveX controls are used to display the RMX Serial Gateway S4GW web site. If the flag value is set to NO (default) an external Internet Explorer browser is launched to display the RMX Serial Gateway S4GW web site. For more information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide.

## Required IT Infrastructure

The following IT infrastructure components are required to secure the RMX conferencing (audio and video) solution.

- External Domain Name Server (DNS)
- Network Time Protocol (NTP) server
- Certificate Authority server.
- Certificate Revocation List (CRL) distribution point for each Certificate Authority (CA) used in the configuration
- Online Certificate Status Protocol (OCSP)

### DNS

All systems that are part of the secure solution, whether IT infrastructure or Polycom devices, must be configured with the capability to resolve all other Polycom and other IT infrastructure device Host Names on the network. This includes all workstations used to access the RMX Management Network using the RMX Manager.

The easiest way to do this is to use a DNS server to ensure that each device in the deployment can be identified by a Fully Qualified Domain Name (FQDN).

- Devices must have FQDNs in order to use security certificates.
- In dual stack network configurations that support both IPv4 and IPv6, both IP addresses must be included in the DNS configuration.
- When connecting to devices within the IT infrastructure from Polycom devices, the FQDN of the respective machines should be used.

### NTP Servers

In order to meet Maximum Security requirements, a secure audio and video conferencing environment must include at least two NTP servers. Security certificates are not required for NTP servers.

The RealPresence Server will not use a time source such as a Windows-based, W32Time service (SNTP) time service. Only full-featured (Stratum 16 or below) NTP Servers are considered sufficiently reliable for high-accuracy timing environments.
Certificate Authority Server

A certificate authority (CA) server is used to issue and manage security credentials. A CA server is an integral part of a (Public Key Infrastructure) PKI security system and is a required component of a Maximum Security Environment.

- Polycom products must be able to resolve the CA server using its Fully Qualified Domain Name (FQDN).
- With the exception of the NTP servers, all networked components within the Maximum Security Environment must have a valid certificate or certificate chain. A Certificate Revocation policy and a Certificate Revocation method for all networked components must also be established.
- Certificates issued for Polycom devices within a Maximum Security Environment must meet the specific requirements as described in Polycom® RMX® 1500/2000/4000 Administrator’s Guide.
- For certificate management, networked components within the Maximum Security Environment can use either an Online Certificate Status Protocol (OCSP) responder or Certificate Revocation Lists (CRLs). For more information see Polycom® RMX® 1500/2000/4000 Administrator’s Guide.

RMX Hardware

Version 8.5.10 requires that MPMx cards are installed in the RMX.

First Time Installation and Configuration

First Time Installation and Configuration of the Collaboration Server 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.
   - Obtain Product Activation Key for the RMX.
   - Download and install the RMX Manager onto a workstation.
   - Connect workstation to the Default Management Network.
   - Power up the RMX.
   - Activate the RMX product.
   - Modify the Default Management Network.
   - Configure the IP (Signaling) Network Service.
   - Configure the ISDN/PSTN Network Service.

4 Enable Ultra Secure Mode

5 Enable Network Separation (RMX 2000)
6 Enable Secured Communication
   ➢ Purchase and Install the SSL/TLS certificate
   ➢ Modify the Management Network settings
   ➢ Create/Modify the relevant System Flags
7 Configure SIP/AS-SIP for the Signaling Network
8 Set System Configuration Flags
9 Configure 802.1X Authentication (Optional)
10 Configure Precedence (DSCP) and QOS
11 Configure IVR Settings
12 Modify Default Login Banner Text (Optional)
13 Rename the default POLYCOM user
14 Disable Inline AutoComplete Option in Web Browser
15 Configure White List Access
16 Configure Gateway Services

Upgrading to Version 8.5.10

If you are upgrading to version 8.5.10 from a previous version, see the Polycom® RealPresence®
Collaboration Server (RMX) 1500/2000/4000 Release Notes for Maximum Security Environments,
“Upgrade Procedures”.

Procedure 1: Hardware Installation and Setup

In a well ventilated area, mount the RMX 1500/RMX 2000/RMX4000 unit in a 19” rack. It is important to
adhere to the Site Requirements as described in the RMX 2000/4000 Hardware Guides, “Site
Requirements”.

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

The following procedures have to be performed to install the RMX System in your site:
   • Installing the RMX in a rack or as a standalone. When installing the RMX unit on a rack, this process
is done in two stages:
      ➢ Installing the telescopic rail runners on the rack. This stage is identical to all RMX system types.
      ➢ Mounting the RMX on the rack using the previously installed rail runners
   • Connecting the RMX to the power source
   • Connecting the network (LAN and ISDN) cables to the RMX.
Installing the Telescopic Rail Runners on the Rack

Telescopic Rail Runners Accessory Kit

Before installing the telescopic rail runners in the rack, make sure that the kit has the following parts:

**Rail Runners Kit Contents**

<table>
<thead>
<tr>
<th>Part/Kit no.</th>
<th>Item</th>
<th>Item No.</th>
<th>Item Sample</th>
<th>Item Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASY2716A-L0</td>
<td>Left rail runner (two types available: item (a) with or (b) without rail runner clip)</td>
<td>1</td>
<td>Rail runner end views:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Note: The rail runner clip is designed to attach and clip onto the chassis runner frame.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Right rail runner (two types available: with or without rail runner clip)</td>
<td>2</td>
<td>See Figure 1-1.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Note: The rail runner clip is designed to attach and clip onto the chassis runner frame.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack spacer assembly kit</td>
<td>Rack spacer</td>
<td>3</td>
<td>Front &amp; Rear:</td>
<td>4</td>
</tr>
<tr>
<td>Flat head screw - M5*10mm</td>
<td></td>
<td>4</td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>
Telescopic Rail Runner Assembly

Rack Rail Runners require a minimum of 48cm and a maximum of 80cm within the rack for installation.

1. Determine the location of the RMX on the rack:
   - Allow for a 1U gap above and below the system for ventilation.
   - Use the Rack Spacer (3) to predetermine its position on the rack post, making sure that square studs of the spacer fit into the rack post’s square/rounded mounting holes. Mark the spacer’s location on the rack post. Repeat this process for the 3 remaining vertical posts ensuring that the system can be horizontally seated.

### Rail Runners Kit Contents

<table>
<thead>
<tr>
<th>Part/Kit no.</th>
<th>Item</th>
<th>Item No.</th>
<th>Item Sample</th>
<th>Item Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail runner assembly kit</td>
<td>Flat head screw - M3*8mm</td>
<td>5</td>
<td><img src="sample.jpg" alt="Sample" /></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Flat washer M3</td>
<td>6</td>
<td><img src="sample.jpg" alt="Sample" /></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Nut spring M3</td>
<td>7</td>
<td><img src="sample.jpg" alt="Sample" /></td>
<td>4</td>
</tr>
<tr>
<td>RMX chassis assembly kit</td>
<td>Pan head screw - M5*12mm</td>
<td>8</td>
<td><img src="sample.jpg" alt="Sample" /></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Flat washer M5</td>
<td>9</td>
<td><img src="sample.jpg" alt="Sample" /></td>
<td>2</td>
</tr>
</tbody>
</table>
Position the Rack Spacer (item no. 3) onto the marked rack post together with rack rail runner (item no. 1 which is labeled LEFT) and fasten the flat head screws 3*10mm (4) as shown in the following figure.
Detail of Front Rack Spacer Assembly for all RMX types

RMX 1500 rack assembly view without rail runner clip

RMX 1500 rack assembly view with rail runner clip

RMX 2000 rack assembly view without rail runner clip

RMX 2000 rack assembly view with rail runner clip
3 Adjust the telescopic rack rail runner to the rack opening and mount it onto the marked position of the rear post as described in step 2.

4 Repeat steps 2 and 3 for the right rack rail runner.

5 Install the flat head screw (5), flat washer (6) and nut spring (7) in the middle of the telescopic rack rail runner for added stability as shown in the figure below.

On the RMX1500/4000 the center hole on the Rack Spacer must be left clear as it is required for fixing the RMX to the rack post. See .

On the RealPresence Collaboration Server (RMX) 2000 the top hole on the Rack Spacer must be left clear as it is required for fixing the RMX to the rack post. See .
6 Repeat step 5 for the right rack rail runner.

Installing the RMX 1500

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

The following procedures have to be performed to install the RMX 1500 in your site:

- Optional. Installing the RTM ISDN card on the RMX (Optional)
- Installing the RMX in a rack or as a standalone
- Connecting the RMX to the power source
- Connecting the network (LAN, IP and ISDN) cables to the RMX.

Installing the RTM ISDN 1500 Card on the RMX 1500 (Optional)

If the ISDN option was purchased with your RMX, the ISDN card is shipped separately and must be manually installed into the rear of the RMX 1500. It is recommended to install the ISDN card before the RMX 1500 is placed in a rack.

Removing the blank cover from the rear of the RMX 1500

1 Ensure that the power switch on the Collaboration Server is turned OFF (O).
2 Remove the cover by unscrewing the captive screws that fasten the card to the MCU.
3 Slide out the cover.

Installing the RTM ISDN 1500 Card
1 Slide in the RTM ISDN 1500 card.

2 Insert the card into the slot and tighten the captive screws on each side of the rear panel of the card, securing the RTM ISDN card to Collaboration Server.

A Software License is included with the ISDN card. This license must be registered as part of the Product Registration and Product Activation process.
Mounting the Collaboration Server 1500 in a Rack

There are two methods for installing the Collaboration Server in a 19" rack:

- Using the rack rail runners on the RMX 1500
  - Install the telescopic rail runners, as described in Installing the Telescopic Rail Runners on the Rack.
  - Mount the Collaboration Server 1500 on top of the rail runners.
  - Fasten the Collaboration Server to the rack spacers using the flat head screw (8) with flat washer (9) through the two holes in the Collaboration Server’s front mounting brackets.

- Using a shelf
  - Install the shelf, supplied by the rack manufacturer, in the rack.
  - Mount the Collaboration Server unit on the shelf.
  - Fasten the Collaboration Server unit to the rack with screws through the four holes in the Collaboration Server’s front mounting brackets.

Connecting Cables to the RMX 1500

Before plugging network cables in, ensure sure that the network infrastructure containing all the devices (including the RMX) has two different networks: one for Management; the other for Signaling & Media. Separation can be achieved either by two physical networks or by two virtual networks (VLANs).
➢ To connect the cables:

● Connect the Media cable to LAN 2 port.

➢ Optional. If LAN Redundancy or Multiple Networks options are used, connect the LAN cable to LAN 1. For more information, see RMX 1500/2000/4000 Administrator’s Guide “LAN Redundancy”.

● Connect the Network cables to:

➢ the MNG (Signaling) port

➢ the MNGB (Management Network) port

When an NTP Server is used for the RMX Time, the Shelf Management cable must be connected to the shelf port.

➢ For ISDN/PSTN connections, connect the E1/T1 cables to their PRI (1-4) ports (Optional).

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

* With Multiple network and LAN redundancy configurations, LAN 1 port is used. For more information, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrators Guide, Multiple Services and LAN Redundancy.

Installing the RMX 2000

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

The following procedures have to be performed to install the RMX 2000 in your site:

● Installing the RTM ISDN card on the RMX (Optional)

● Installing the RMX in a rack or as a standalone
• Connecting the RMX to the power source
• Connecting the network (LAN and ISDN) cables to the RMX

Installing the RTM ISDN Card on the RMX 2000

If the ISDN option was purchased with your RMX, the ISDN card is shipped separately and must be manually installed into the rear of the RMX 2000. It is recommended to install the ISDN card before the RMX 2000 is placed in a rack.

Removing the blank cover from the rear of the RMX 2000

Use the following procedure to remove the blank cover:

1. Ensure that the power switch/circuit switch on the Collaboration Server is turned OFF (O).
2. Unscrew the captive screws on the rear panel of the Collaboration Server that secure the blank panel.
3. Use the metal ejector levers to pull the blank panel.

Installing the RTM ISDN 2000 Card

A Software License is included with the ISDN card. This license must be registered as part of the Product Registration and Product Activation process.

Mounting the Collaboration Server 2000 in a Rack

There are two methods for installing the Collaboration Server in a 19” rack:

• Using rack rail runners on the RMX 2000:
  ➢ Install the telescopic rail runners, as described in Installing the Telescopic Rail Runners on the Rack.
  ➢ Mount the Collaboration Server 2000 on top of the rail runners.
  ➢ Fasten the Collaboration Server to the rack spacers using the flat head screw (item 8) with flat washer (item 9) through the two holes in the Collaboration Server’s front mounting brackets.
Using a shelf:
- Install the shelf, supplied by the rack manufacturer, in the rack.
- Mount the Collaboration Server on the shelf.
- Fasten the Collaboration Server to the rack with screws through the four holes in the Collaboration Server’s front mounting brackets.

Refer to Detail of Front Rack Spacer Assembly for all RMX types on page 8 for installation instructions.

Connecting Cables to the RMX 2000

Do not remove the protective caps from LAN1, LAN3 and ShMG ports.

Ensure that the network infrastructure containing all the devices (including the RMX) has two different networks: one for Management; the other for Signaling & Media. Separation can be achieved either by two physical networks or by two virtual networks (VLANs). These separated networks will be used after Network Separation is performed.

Connect the following cables to the back panel:
- Power cable
- On the RTM IP card connect the LAN cable to LAN 2 Port.
- On the RTM LAN card connect the LAN cable to LAN 2.
Connect the LAN cable to LAN 1.

With Multiple Networks and LAN Redundancy configurations, LAN 1 port is used. For more information, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide. "LAN Redundancy" and "Multiple Networks".

- On the RTM ISDN card connect the E1/T1 Cables to PRI Ports (Optional).

Installing the RMX 4000

The following procedures have to be performed to install the RMX 4000 at your site:

- Optional. Installing the RTM ISDN card on the RMX
- Mounting the RMX in a rack
- Connecting the RMX to the power source
- Connecting the network (LAN and ISDN) cables to the RMX

Optional. Installing the RTM ISDN Card on the RMX 4000

If the ISDN option was purchased with your RMX, the ISDN card is shipped separately and must be manually installed into the rear of the RMX 2000. It is recommended to install the ISDN card before the RMX 2000 is placed in a rack.

Removing the RTM LAN Card or the blank cover from the rear of the RMX 4000

1. Ensure that the power switch on the RealPresence Collaboration Server 4000 is turned OFF.
2. Remove the RTM LAN or blank cover by unscrewing the captive screws that fasten the card or the cover to the RMX. When removing a card, use the metal ejector levers to pull the RTM LAN card out of its slot from the backplane.
3. Slide out the RTM LAN or RTM ISDN card.
Installing the RTM ISDN 4000 Card

1. On the RTM ISDN card move the ejector levers to their fully open position.
2. Slide the new RTM ISDN card into its slot.

An RTM ISDN card must connect directly to an MPMx card in the opposite facing front slot.

3. Push the card into the slot until the ejector levers touch the front edge of the card cage. Push the ejector levers to their fully closed position.
4. Tighten the captive screws on each side of the rear panel of the card, securing the RTM ISDN card to the MCU.

A Software License is included with the ISDN card. This license must be registered as part of the Product Registration and Product Activation process.

Mounting the Collaboration Server 4000 in a Rack

Either place the RMX 4000 on a hard, flat surface such as a desktop or mount it on a 19” rack.

For a detailed description of the safety requirements and precautions and the installation of the RMX 4000 as a standalone, or reverse mounting the RMX 4000 on a 19” rack, see the RealPresence Collaboration Server (RMX) 4000 Hardware Guide.

To install the Collaboration Server 4000 in a 19” rack:

- Using rack rail runners on the RMX 4000
  - Install the telescopic rail runners, as described in Installing the Telescopic Rail Runners on the Rack.
  - Mount the Collaboration Server 4000 on top of the rail runners.
  - Fasten the Collaboration Server to the rack spacers using the flat head screw (item 8) with flat washer (item 9) through the two holes in the Collaboration Server’s front mounting brackets.
Using a shelf

- Install the shelf, supplied by the rack manufacturer, in the rack.
- Mount the Collaboration Server on the shelf.
- Fasten the Collaboration Server to the rack with screws through the eight holes in the Collaboration Server’s front mounting brackets.

Refer to Detail of Front Rack Spacer Assembly for all RMX types on page 8 for installation instructions.
Connecting the RMX 4000 to the 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).

**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 RealPresence Collaboration Server (RMX) 4000 Hardware Guide.

2. Ensure that the cables from the Main that supplies electricity to the DC power units are **OFF** or 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.
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.

**Connecting Cables to the RMX 4000**

- To connect the cables (AC and DC systems):
- 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.

Before plugging network cables in, ensure sure that the network infrastructure containing all the devices (including the RMX) has two different networks: one for Management; the other for Signaling & Media. Separation can be achieved either by two physical networks or by two virtual networks (VLANs).

- Connect the LAN cable to LAN 2.

When an NTP Server is used for the RMX Time, the Shelf Management cable must be connected to the shelf port.

- For each installed RTM LAN - Connect the LAN cable to LAN 2.
  - Optional. Connect the LAN cable to LAN 1. With Multiple networks and LAN redundancy configurations, LAN 1 port is used.
    - For more information see the Administrator’s Guide for Maximum Security Environments, "LAN Redundancy" and "Multiple Networks".
  - Optional. When deploying a Serial Gateway S4GW, connect a LAN cable from the S4GW to either LAN 1 or LAN 2.
    - For more information see Deploying a Polycom RMX™ Serial Gateway S4GW on page 144.

- Optional. If RTM ISDN is installed, for each installed RTM ISDN:
  - Connect the E1/T1 cables to their PRI Ports.
  - Connect the LAN cable to LAN 1.
Procedure 2: Gather Network Equipment and Address Information

IP Services

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

- Management Network (Control Unit)
- IP (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 Collaboration Server Control Unit and the RMX Manager and is used to manage the Collaboration Server.

The RMX is shipped with default IP addresses as listed in .

Signaling Network

The Signaling Network is used to configure and manage communications between the Collaboration Server and conferencing devices.
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 Collaboration Server.

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.

First Time Setup Worksheet

When installing an RMX system, these default system parameters, must be modified to your local network settings and site requirements. It is therefore important to obtain the information needed to complete the First Time Setup Worksheet from your network administrator before powering up the RMX for the first time.

First Time Setup Worksheet

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default</th>
<th>Local Network Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Key</td>
<td>–</td>
<td>IP Network Service / Default PSTNService</td>
<td>Before the Collaboration Server can be used, it is necessary to register the product and obtain an Activation Key, available from <a href="http://portal.polycom.com">http://portal.polycom.com</a></td>
</tr>
<tr>
<td>Network Service Name</td>
<td>IP Network Service / Default PSTNService</td>
<td></td>
<td>Network Service Name(s) are required for H.323 and ISDN/PSTN Network Services. The default name can be changed and can contain character sets that use Unicode encoding.</td>
</tr>
<tr>
<td>Control Unit IP Address</td>
<td>192.168.1.254</td>
<td>192.168.1.254</td>
<td>Default IP addresses with which the system is shipped to enable direct connection.</td>
</tr>
<tr>
<td>Control Unit Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Default Router IP Address</td>
<td>192.168.1.1</td>
<td>192.168.1.1</td>
<td></td>
</tr>
<tr>
<td>Shelf Management IP Address</td>
<td>192.168.1.252</td>
<td>192.168.1.252</td>
<td></td>
</tr>
<tr>
<td>Shelf Management Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Shelf Management Default Gateway</td>
<td>192.168.1.1</td>
<td>192.168.1.1</td>
<td></td>
</tr>
<tr>
<td>Signaling Host IP address</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>The address to be used by IP endpoints when dialing into the RMX.</td>
</tr>
</tbody>
</table>
### First Time Setup Worksheet

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default</th>
<th>Local Network Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Board IP address (MPM 1)</td>
<td>0.0.0.0</td>
<td></td>
<td>The network administrator should allocate:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4 IP addresses in the local network for an MCU with one MPMx card,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Up to seven IP addresses for an MCU with up to 4 MPMx cards.</td>
</tr>
<tr>
<td>Media Board IP address (MPM 2)</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMX 2000/4000 only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Board IP address (MPM 3)</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMX 4000 only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Board IP address (MPM 4)</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMX 4000 only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Router IP Address</td>
<td>0.0.0.0</td>
<td></td>
<td>The default router is used whenever the defined static routers are not able to route packets to their destination.</td>
</tr>
<tr>
<td>Service Host Name</td>
<td>PolycomMCU.</td>
<td></td>
<td>DNS:</td>
</tr>
<tr>
<td>DNS</td>
<td>Specify</td>
<td></td>
<td>The Service Host Name is the FQDN (Fully Qualified Domain Name) of the RMX in the network. The IP address fields are enabled only if Specify is selected. Local Domain Name is the FQDN where the MCU is installed.</td>
</tr>
<tr>
<td>Register Host Names Automatically to DNS Server</td>
<td>Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Domain Name</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server Address</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Type</td>
<td>H.323</td>
<td></td>
<td>H.323, SIP, H.323 &amp; SIP may be selected. If AS-SIP is to be used, H.323 &amp; SIP must be selected.</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>Off</td>
<td></td>
<td>Gatekeeper:</td>
</tr>
<tr>
<td>IP Address or Name</td>
<td>–</td>
<td></td>
<td>When Off is selected, all gatekeeper options are disabled.</td>
</tr>
<tr>
<td>MCU Prefix in Gatekeeper</td>
<td>–</td>
<td></td>
<td>The gatekeeper’s host name as registered in the DNS or IP address can be entered.</td>
</tr>
<tr>
<td>Alias</td>
<td>–</td>
<td></td>
<td>The Prefix is the number with which this Network Service registers with the gatekeeper, used by H.323 endpoints as the first part of their dial-in string. Up to five aliases can be defined for each RMX.</td>
</tr>
<tr>
<td>Alias Type</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Authentication</td>
<td>Off</td>
<td></td>
<td>H.323 Authentication and User Name are specified in the Security dialog box.</td>
</tr>
<tr>
<td>User Name</td>
<td>–</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### First Time Setup Worksheet

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default</th>
<th>Local Network Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Server</td>
<td>Off</td>
<td></td>
<td>SIP Server:</td>
</tr>
<tr>
<td>SIP Server IP address (optional)</td>
<td>–</td>
<td></td>
<td>The IP address of the preferred SIP server or its host name (if a DNS server is used).</td>
</tr>
<tr>
<td>SIP Server IP Address or Name</td>
<td>0.0.0.0</td>
<td></td>
<td>The domain name is that is the SIP domain. (The SIP domain may be different to the DNS domain.)</td>
</tr>
<tr>
<td>Server Domain Name</td>
<td>DomainName</td>
<td></td>
<td>Select the transport type and protocol that is used for signaling between the MCU and the SIP Server or the endpoints according to the protocol supported by the SIP Server:</td>
</tr>
<tr>
<td>Transport Type</td>
<td>TCP</td>
<td></td>
<td>TLS should be selected for Maximum Security Environment deployments.</td>
</tr>
<tr>
<td>SIP Authentication</td>
<td>Off</td>
<td></td>
<td>SIP Authentication and User Name are specified in the Security dialog box.</td>
</tr>
<tr>
<td>User Name</td>
<td>–</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Do you want to create an ISDN/PSTN service**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Yes</th>
<th></th>
<th>ISDN/PSTN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Span Type</td>
<td>E1</td>
<td></td>
<td>During the initial Collaboration Server 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. A new ISDN/PSTN Network Service can be defined even if no RTM ISDN card is installed in the system but only using the ISDN/PSTN Network Service -&gt;Add New Service dialog box.</td>
</tr>
<tr>
<td>Service Type</td>
<td>PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Num Type</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Num Plan</td>
<td>ISDN/PSTN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Specific</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial-out Prefix</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Framing</td>
<td>ESF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Side</td>
<td>User side</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line Coding</td>
<td>B8ZS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Type</td>
<td>EURO-ISDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Number</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Number</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU CLI</td>
<td>–</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### First Time Setup Worksheet

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default</th>
<th>Local Network Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use NTP Server</td>
<td>–</td>
<td>1:</td>
<td>The IP addresses of up to 3 NTP Servers can be specified.</td>
</tr>
<tr>
<td></td>
<td>–</td>
<td>2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–</td>
<td>3:</td>
<td></td>
</tr>
<tr>
<td>Conference ID Length (MCU)</td>
<td>5</td>
<td></td>
<td>The initial System Flag values can be configured.</td>
</tr>
<tr>
<td>Minimum Conference ID Length (User)</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Conference ID Length (User)</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU Display Name</td>
<td>Polycom RMX</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1500/2000/4000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminate Conference when Chairperson Exits</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Extend Conferences</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator User</td>
<td>POLYCOM</td>
<td></td>
<td>In Maximum Security Environments the Administrator User Name and Password are configured after Secured Communication has been enabled.</td>
</tr>
</tbody>
</table>

### Workstation for Direct Connection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The workstation’s IP address should be in the same network neighborhood as the RMX’s Control Unit IP address, but should not use any of the default IP addresses with which the RMX system is shipped to enable direct connection. See Default IP addresses with which the system is shipped to enable direct connection. on page 23.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 3: First Entry Configuration

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

1. Register the RMX.
2. Obtain Product Activation Key for the RMX.
3. Download and install the RMX Manager onto a workstation.
5. Power up the RMX.
6. Login to the RMX.
7. Activate the RMX product.
8. Modify the Default Management Network.
9. Configure the IP (Signaling) Network Service.
10. Configure the ISDN/PSTN Network Service.

Register the RMX

Before the Collaboration Server 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.

Obtain Product Activation Key for the RMX

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.

Download and Install the RMX Manager Onto a Workstation

The RMX Manager is the recommended option for accessing the RMX's management console.

The RMX Manager specific to version 8.5.10 can be downloaded from the Federal Accreditation and Certification section of the Polycom website at http://www.polycom.com/federal.

To install the RMX Manager:

1. Obtain the RMX Manager specific to Version 8.5.10 from the Polycom Software Distribution website.
2. Install the RMX Manager on the workstation:
   a. Using Windows, navigate to the folder where the downloaded RMX Manager has been saved.
b Double-click on the downloaded install file and follow the on-screen instructions to complete the installation.

3 When the install of the RMX Manager is completed, launch the RMX Manager using the Windows Start menu.

4 If needed, add the MCU to the RMX Manager’s MCUs list if it was not pre-populated during installation.
   a Right-click in the RMX Manager window.
   b Select Add MCU.
   c Enter the MCU Name.
   d Enter the IP Address of the MCU.
   e Leave the port as Port 80 until such time that the RMX is placed into Secure Mode.
   f Click OK.
   The Username and Password dialog box is displayed.

5 Enter the default Username - POLYCOM and default Password – POLYCOM.

6 Click OK.
Connect the Workstation to the Default Management Network

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 Collaboration Server and the workstation and the Default Management Network parameters are modified using the Fast Configuration Wizard in the RMX Manager.

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 Collaboration Server’s Default Management Network.

To modify the workstation’s IP addresses:

(It is recommended that workstation’s settings be documented in order to reset it back to its original settings after it has been used for direct connection to the RMX.)

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.


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
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 Collaboration Server’s Default Management Network are listed in the table below.

### Reserved IP Addresses

<table>
<thead>
<tr>
<th>Network Entity</th>
<th>Default Management Network IP Addresses (Factory Default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Unit IP Address</td>
<td>192.168.1.254</td>
</tr>
<tr>
<td>Control Unit Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Router IP Address</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Shelf Management IP Address</td>
<td>192.168.1.252</td>
</tr>
<tr>
<td>Shelf Management Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Shelf Management Default Gateway</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

7. Click the OK button.

### Connect the Workstation to the RMX

» 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.

---

None of the reserved IP addresses listed in the table should be used for the IP Address.
Power up the RMX

- Connect the power cable and power the RMX ON.

Login to the RMX

In the RMX Manager’s main screen:

1. Connect to the RMX using the RMX Manager’s MCUs list, by one of the following methods:
   a. Double-click the MCU icon.
   b. Select the RMX to connect and click the Connect MCU button.
   c. Right-click the MCU icon and then click Connect MCU.

The Username / Password dialog box is displayed.

2. Enter the default Username (POLYCOM) and Password (POLYCOM) and click OK.
Activate the RMX Product

The *RMX Manager* and the Product Activation dialog box is displayed with the serial number filled in:

1. In the Activation Key field, enter or paste the Product Activation Key obtained earlier.
2. 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 *Obtain Product Activation Key for the RMX* on page 27.
   
   The system prompts with a restart dialog box:

3. In the dialog box, click Yes.
Modify the Default Management Network

After the RMX resets, the Fast Configuration Wizard starts.

Both IPv4 and IPv6 are supported. For IPv6 addressing information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, "IP Network Services".

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:

1. 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

2. Click the Save & Close button.
   The system prompts you to sign in with the new Control Unit IP Address.

3. Disconnect the LAN cable between the workstation and the LAN 2 port on the RMX’s back panel.
   (The workstation can be configured back to its original network settings.)

4. Connect LAN 2 port on the RMX’s back panel to the local network using a LAN cable.
5 Connect to the RMX using the RMX Manager's MCUs list, by one of the following methods:
   a Double-click the MCU icon.
   b Select the RMX to connect and click the Connect MCU button.
   c Right-click the MCU icon and then click Connect MCU.
   The Username / Password dialog box is displayed.

6 Enter the default Username (POLYCOM) and Password (POLYCOM) and click OK.

Modifying the Signaling Network Service

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 RMX 1500/2000/4000 Administrator’s Guide, "IP Network Services".
Fast Configuration Wizard

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

**Signaling Network Service – IP Signaling**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Service Name</td>
<td>The name Default IP Service is assigned to the Signaling Network Service by the Fast Configuration Wizard. This name can be changed. Note: This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.</td>
</tr>
<tr>
<td>Signaling Host IP Address</td>
<td>Enter the address to be used by IP endpoints when dialing into the MCU. Dial out calls from the Collaboration Server are initiated from this address. This address is used to register the Collaboration Server with a Gatekeeper or a SIP Proxy server.</td>
</tr>
<tr>
<td>Media Card 1-4 IP Addresses</td>
<td>Enter the IP address(es) of the media card(s) (MPMx 1 and 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.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask of the MCU. Default value: 255.255.255.0.</td>
</tr>
</tbody>
</table>
2 Click the Next button.
3 Enter the required Routers information in the dialog box.

![Image]

Signaling Network Service – Routers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Router IP Address</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Settings in this dialog box pertain to the Signaling Network.

Fast Configuration Wizard – DNS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Host Name</td>
<td>Enter the FQDN of the MCU on the network. Default: PolycomMCU.</td>
</tr>
</tbody>
</table>
| DNS           | Select:  
  • Off – if DNS servers are not used in the network.  
  • Specify – to enter the IP addresses of the DNS servers.  
  Note: The IP address fields are enabled only if Specify is selected. |
| Register Host Names Automatically to DNS Server | Select this option to automatically register the MCU Signaling Host with the DNS server. |
Fast Configuration Wizard – DNS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Domain Name</td>
<td>Enter the FQDN where the MCU is installed.</td>
</tr>
<tr>
<td>DNS Server IP Address</td>
<td>The static IP address of the primary DNS server.</td>
</tr>
</tbody>
</table>

6 Click the Next button.

7 Enter the required Network Type information in the dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Network Type</td>
<td>Select a Network Type:</td>
</tr>
<tr>
<td></td>
<td>• H.323</td>
</tr>
<tr>
<td></td>
<td>• SIP</td>
</tr>
<tr>
<td></td>
<td>• H.323 &amp; SIP</td>
</tr>
<tr>
<td></td>
<td>Note: If AS-SIP is to be used, select H.323 &amp; SIP</td>
</tr>
</tbody>
</table>

8 Click the Next button.

9 If you selected SIP only, go to Step 13.
Enter the required Gatekeeper information in the dialog box.

### Signaling Network Service – IP

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper</td>
<td>Select Specify to enable configuration of the gatekeeper IP address. When Off is selected, all gatekeeper options are disabled.</td>
</tr>
<tr>
<td>Primary Gatekeeper IP Address or Name</td>
<td>Enter either the gatekeeper’s host name as registered in the DNS or IP address.</td>
</tr>
<tr>
<td>MCU Prefix in Gatekeeper</td>
<td>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.</td>
</tr>
</tbody>
</table>
11 Click the Next button.
12 If you selected H.323, click Save & Continue; otherwise click Next and go to Step 13.
   If you have selected Save and Continue, the IP Network Service is created and confirmed.

➢ Go to Step 17.
13 Leave the SIP Server field configured to Off - this will be changed later once the Fast Configuration Wizard has completed.

14 Click Next.

15 Enter the required Security information in the dialog box.
Default IP Network Service – Security (SIP Digest)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>These fields can contain up to 20 ASCII characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Authentication</td>
<td>Click this check box to enable SIP proxy authentication. Select this check box only if the authentication is enabled on the SIP proxy, to enable the Collaboration Server to register with the SIP proxy. If the authentication is enabled on the SIP proxy and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the SIP proxy.</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name the Collaboration Server will use to authenticate itself with the SIP proxy. This name must be defined in the SIP proxy.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password the Collaboration Server will use to authenticate itself with the SIP proxy. This password must be defined in the SIP proxy.</td>
<td></td>
</tr>
<tr>
<td>H.323 Authentication</td>
<td>Click this check box to enable H.323 server authentication. Select this check box only if authentication is enabled on the gatekeeper, to enable the Collaboration Server to register with the gatekeeper. If the authentication is enabled on the gatekeeper and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name the Collaboration Server will use to authenticate itself with the gatekeeper. This name must be defined in the gatekeeper.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password the Collaboration Server will use to authenticate itself with the gatekeeper. This password must be defined in the gatekeeper.</td>
<td></td>
</tr>
</tbody>
</table>

16 Click Save & Continue.

The IP Network Service is created and confirmed.

17 Click OK.

Configure the ISDN/PSTN Network Service

During the initial Collaboration Server 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 15.

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:

1. Define the following parameters:

**Fast Configuration Wizard – ISDN Service Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Service Name</td>
<td>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. Note: This field is displayed in all ISDN/PSTN Network Properties tabs and can contain character sets that use Unicode encoding.</td>
</tr>
<tr>
<td>Span Type</td>
<td>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: • T1 (U.S. – 23 B channels + 1 D channel) • E1 (Europe – 30 B channels + 1 D channel) Default: T1 Note: Only one Span Type (E1 or T1) is supported on the Collaboration Server. If you define the first span as type E1 all other spans that you may later define must also be of type E1.</td>
</tr>
<tr>
<td>Service Type</td>
<td>PRI is the only supported service type. It is automatically selected.</td>
</tr>
</tbody>
</table>
2 Click Next.

The PRI Settings dialog box is displayed.

3 Define the following parameters:

### Fast Configuration Wizard – PRI Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Num Type</td>
<td>Select the Default Num Type from the list. 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. 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 Unknown. Default: Unknown Note: For E1 spans, this parameter is set by the system.</td>
</tr>
<tr>
<td>Num Plan</td>
<td>Select the type of signaling (Number Plan) from the list according to information given by the service provider. Default: ISDN Note: For E1 spans, this parameter is set by the system.</td>
</tr>
<tr>
<td>Net Specific</td>
<td>Select the appropriate service program if one is used by your service provider (carrier). Some service providers may have several service programs that can be used. Default: None</td>
</tr>
<tr>
<td>Dial-out Prefix</td>
<td>Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required. The field can contain be empty (blank) or a numeric value between 0 and 9999. Default: Blank</td>
</tr>
</tbody>
</table>
4 Click Next.
The Span Definition dialog box is displayed.

5 Define the following parameters:

### Fast Configuration Wizard – Spans Definition

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framing</td>
<td>Select the Framing format used by the carrier for the network interface from the list.</td>
</tr>
<tr>
<td></td>
<td>• For T1 spans, default is SFSF.</td>
</tr>
<tr>
<td></td>
<td>• For E1 spans, default is FEBE.</td>
</tr>
<tr>
<td>Side</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• User side (default)</td>
</tr>
<tr>
<td></td>
<td>• Network side</td>
</tr>
<tr>
<td></td>
<td>• Symmetric side</td>
</tr>
<tr>
<td></td>
<td>Note: If the PBX is configured on the network side, then the Collaboration Server unit must be configured as the user side, and vice versa, or both must be configured symmetrically.</td>
</tr>
<tr>
<td>Line Coding</td>
<td>Select the PRI line coding method from the list.</td>
</tr>
<tr>
<td></td>
<td>• For T1 spans, default is B8ZS.</td>
</tr>
<tr>
<td></td>
<td>• For E1 spans, default is HDB3.</td>
</tr>
<tr>
<td>Switch Type</td>
<td>Select the brand and revision level of switch equipment installed in the service provider’s central office.</td>
</tr>
<tr>
<td></td>
<td>• For T1 spans, default is AT&amp;T 4ESS.</td>
</tr>
<tr>
<td></td>
<td>• For E1 spans, default is EURO ISDN.</td>
</tr>
<tr>
<td></td>
<td>Note: For T1 configurations in Taiwan, Framing must be set to ESF and Line Coding to B8ZS.</td>
</tr>
</tbody>
</table>
6 Click Next.
   The Phones dialog box is displayed.

7 Click Add to define dial-in number ranges.
   The Add Phone Number dialog box is displayed.

8 Define the following parameters:

**Fast Configuration Wizard – Add Phone Numbers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Number</td>
<td>The first number in the phone number range.</td>
</tr>
<tr>
<td>Last Number</td>
<td>The last number in the phone number range.</td>
</tr>
</tbody>
</table>

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

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

10 Repeat steps 7 to 8 to define additional dial-in ranges (Optional).

11 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.
12 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.

13 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 MPMx 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.
14 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 Manager.

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 Manager.

- RMX 2000/4000 - Each ISDN RTM card can support either 7 E1 or 9 T1 PRI lines.
- RMX 1500 - Either 4 E1 or 4 T1 PRI lines are supported.

E1 and T1 connections cannot be used simultaneously.

15 Click Next.

The RMX Time dialog box is displayed.

16 Set the RMX Time using one of the three available options: setting the RMX Time manually, clicking the Retrieve Client Time button, or using the NTP Servers options.

**Fast Configuration Wizard - Collaboration Server Time**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT Date</td>
<td>The date at Greenwich, UK.</td>
</tr>
<tr>
<td>Local Time</td>
<td>The MCU's local time settings, are calculated from the GMT Time and the GMT Offset.</td>
</tr>
<tr>
<td>GMT Time</td>
<td>Displays the MCU's current GMT Time settings. Option 1: Manually setting the Collaboration Server time:</td>
</tr>
<tr>
<td></td>
<td>• Using the Up or Down arrows alter the GMT Time and the GMT Offset to set the Collaboration Server time.</td>
</tr>
<tr>
<td>GMT Offset</td>
<td>The time zone difference between Greenwich and the MCU's physical location.</td>
</tr>
<tr>
<td></td>
<td>• Using the Up or Down arrows manually modify the GMT Offset time on the Collaboration Server.</td>
</tr>
<tr>
<td>Retrieve Client Time</td>
<td>Option 2: Automatically setting the MCU time:</td>
</tr>
<tr>
<td></td>
<td>• Click this button to automatically update the MCU's GMT Date, Time and Offset to match that of the workstation.</td>
</tr>
</tbody>
</table>
17 Click Next.

The Administrator User dialog box is displayed.

The Administrator User Name and Password are configured in Procedure 12, after Secured Communication has been enabled.

If the default POLYCOM user is defined, an active alarm is displayed and the MCU status changes to Major until the administrator changes the default username and password.

18 Click Next.

The System Flags dialog box is displayed

19 Enter the required System Flags information in the dialog box.
### Signaling Network Service – System Flags

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description / Default</th>
<th>Note: Selecting 2 digits limits the number of simultaneous ongoing conferences to 99.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference ID Length (MCU)</td>
<td>The number of digits of the Conference ID to be assigned by the MCU. Range: 2-16 (Default: 5)</td>
<td></td>
</tr>
<tr>
<td>Minimum Conference ID Length (User)</td>
<td>The minimum number of digits that the user must enter when manually assigning a numeric ID to a conference. Range: 2-16 (Default: 4)</td>
<td></td>
</tr>
<tr>
<td>Maximum Conference ID Length (User)</td>
<td>The maximum number of digits that the user can enter when manually assigning a Numeric ID to a conference. Range: 2-16 (Default: 8)</td>
<td></td>
</tr>
<tr>
<td>MCU Display Name</td>
<td>The MCU name is displayed on the endpoint’s screen. Default name: RMX 1500, Polycom RMX 2000 or Polycom RMX 4000.</td>
<td></td>
</tr>
<tr>
<td>Terminate Conference when Chairperson Exits</td>
<td>When Yes is selected (default), the conference ends when the chairperson exits even if there are other participants connected. When No is selected, the conference automatically ends at the predefined end time, or when all the participants have disconnected from the conference.</td>
<td></td>
</tr>
<tr>
<td>Auto Extend Conferences</td>
<td>When Yes 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.</td>
<td></td>
</tr>
</tbody>
</table>

20 Click Save & Close.

The RMX confirms successful configuration.

21 In the Success Message box, click OK.

22 In the Reset Confirmation dialog box, click Yes.

23 In the Please wait for system reset message box, click OK.

System restart may take up to five minutes.

24 In the RMX Manager’s MCUs list, periodically highlight the RMX and then select Connect MCU. When the system has restarted and is back online the Login Banner will be displayed and you will be able to logon.

25 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.
Configure the DNS for the Management Network:

1. In the RMX Management pane, click the IP Network Services button.
2. In the IP Network Services list pane, double-click Management Network.
   When the Management Network Properties - IP dialog box opens, click the DNS tab.

3. Modify the following fields:

Default Management Network Service – DNS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Host Name</td>
<td>Enter the FQDN of the MCU on the network.</td>
</tr>
<tr>
<td>DNS</td>
<td>Select Specify. Note: The IP address fields are enabled only if Specify is selected.</td>
</tr>
<tr>
<td>Register Host Names Automatically to DNS Servers</td>
<td>Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.</td>
</tr>
<tr>
<td>Local Domain Name</td>
<td>Enter the FQDN of the domain where the MCU is installed.</td>
</tr>
<tr>
<td>DNS Servers Addresses:</td>
<td></td>
</tr>
<tr>
<td>Primary Server</td>
<td>The static IP addresses of the DNS servers.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>A maximum of three servers can be defined.</td>
</tr>
<tr>
<td>Tertiary Server</td>
<td></td>
</tr>
</tbody>
</table>

The MCU Host Name and Local Domain Name must be the same.
If the content of these two fields are not identical an Active Alarm is created.
Procedure 4: Enable Ultra Secure Mode

The Ultra Secure Mode is disabled by default and can be enabled by adding the ULTRA_SECURE_MODE System Flag and setting its value 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 add and enable ULTRA_SECURE_MODE System Flag:

1. On the RMX menu, click Setup > System Configuration.
   The System Flags dialog box is displayed.
2. In the System Flags dialog box, click the New Flag button.
   The New Flag dialog box is displayed.
3. In the New Flag field enter the flag name: ULTRA_SECURE_MODE.
4. In the Value field enter the flag value: YES.
5. Click the OK button to close the Update Flag Value dialog box.
6. Click the Close 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.
Connecting to the RMX

1. After the system has restarted, log back into the RMX using the RMX Manager and connect to the RMX.
   (In the MCUs list, periodically highlight the RMX and then select Connect MCU. When the system has restarted and is back online the Login Banner will be displayed and you will be able to logon.)

The DoD warning banner is displayed.

2. Click Accept
   The Username / Password dialog box is displayed.

3. Enter the Username and Password.
4. Click OK.
   The system will notify you that you must change the password.
Click OK.

Enter the new Username.

Enter the old Password.

Enter the New Password.

Confirm the New Password.

Click OK.

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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “Secure Communication Mode”.

Procedure 5: Enable Network Separation (RMX 2000)

This procedure is only applicable to the RMX 2000 - Network Separation on the RMX 1500 and RMX 4000 is done differently and will have been already done in a previous procedure.

For more information see Connecting Cables to the RMX 1500 and Connecting Cables to the RMX 4000.

If you are installing an RMX 1500 or RMX 4000 skip to Procedure 6: Enable Secured Communication.

The the SEPARATE_MANAGEMENT_NETWORK System Flag is not relevant to RMX 1500 and RMX 4000 systems which are designed with separate ports and networks for signaling, management and media.

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 is set to YES, media and signaling traffic between IP endpoints and the RMX is hosted via the LAN 2 port, while RMX management sessions are hosted via the LAN 3 port.

Before plugging network cables in, ensure sure that the network infrastructure containing all the devices (including the RMX) has two different networks: one for Management; the other for Signaling & Media. Separation can be achieved either by two physical networks or by two virtual networks (VLANs).
Enabling Network Separation

To enable network separation:

1. On the RMX menu, click Setup > System Configuration. The System Flags dialog box is displayed.
2. Locate and double-click on the SEPARATE_MANAGEMENT_NETWORK System Flag entry. The Update Flag Name dialog box is displayed.
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 Collaboration Server 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 Manager 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 53.

Procedure 6: 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 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 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.

Installing Certificates and Enabling Secure Communications

Participation in a Public Key Infrastructure requires the RMX system to have been configured with at least one CA certificate, and a digital certificate signed by that CA which identifies the RMX.

Often, however, additional CA certificates will be needed to allow the system to properly validate a received certificate.

Using the following checklist, work with your network administrator to gather all required certificates needed for use in the environment:

- RMX Identity Certificates - One for the Management interface and one for the Signaling interface created by the system via the Certificate Signing Request (CSR) procedure described below and signed by a CA within your network infrastructure.
- CA Certificate - For the CA that signs the RMX Identity Certificates.
- Root CA Certificate - This is the certificate for the root of the CA hierarchy.
- Intermediate CA Certificates - For all CAs between the root CA and the CA that signs the RMX certificates.
● OCSP Responder Certificate - Used to validate responses from the OCSP responder. For more information see Certificate Revocation.

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

The RMX uses a separate certificate for the:
● Management Network interface
● Signaling Network interface
It is important that both certificates are installed.

RMX certificates are used for both:
● TLS client connections
● TLS server connections

It is important that the certificate template used on the CA enables both clientAuth and serverAuth use in the Extended Key Usage (EKU) field of the certificate. The related bits in the Key Usage extension should be set accordingly. Using RFC 5280 for more information, work with the administrator of the CA to assure that these parameters are set correctly.

● Purchase and install the necessary SSL/TLS certificates:
  ➢ Certificate
  ➢ CA Certificate(s)
  ➢ CRL
    Certificates are managed using the Certification Repository dialog box accessed through the RMX Manager, Setup menu.
● Modify the Management Network settings

For more information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Release Notes for Maximum Security Environments.

Installing a Certificate

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

Certificates must be installed for both the Management and IP Network Services.
To install a certificate:

1. In the RMX menu, click Setup > RMX Secured Communications > Certificate Repository. The Certificate Repository dialog box is displayed.

2. Click the Personal Certificates tab.

Installing Certificates for the Management Network Service

1. In the Certification Repository dialog box, select Management Network Service.
2 Click Add.
   The Create Personal Certificate dialog box is displayed:

   ![Create Personal Certificate dialog box]

3 Click Create Certificate Request.
   The Create Certificate Request details dialog box is displayed:

   ![Create Certificate Request details dialog box]

4 Enter information in all the following fields:

   **Create Certificate Request**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>Enter any 2 letter code for the country name.</td>
</tr>
<tr>
<td>State or Province</td>
<td>Enter the full name of the state or province.</td>
</tr>
<tr>
<td>Locality</td>
<td>Enter the full name of the town/city/location.</td>
</tr>
<tr>
<td>Organization</td>
<td>Enter the full name of your organization for which the certificate will be issued.</td>
</tr>
</tbody>
</table>
## Create Certificate Request

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Unit</td>
<td>Enter the full name of the unit (group or division) for which the certificate will be issued.</td>
</tr>
<tr>
<td>Common Name (DNS/IP)</td>
<td>Enter the DNS MCU Host Name. This MCU Host Name must also be configured in the Management Network Properties dialog box.</td>
</tr>
<tr>
<td>Subject Alternative Name (SAN)</td>
<td>This field is optional and enabled by default. It is used when using EAP-TLS in conjunction with a Network Policy Server (MS-NPS). It allows the optional inclusion of:</td>
</tr>
<tr>
<td></td>
<td>• Principle Name</td>
</tr>
<tr>
<td></td>
<td>• DNS Name</td>
</tr>
<tr>
<td></td>
<td>• Long – FQDN</td>
</tr>
<tr>
<td></td>
<td>• IP Address (IPv4 and IPv6)</td>
</tr>
<tr>
<td></td>
<td>If DNS/MCU host name is configured, the name will be populated automatically. The configured IP address (IPv4, IPv6 or both) will be automatically populated. Additional IPv6 addresses can be added manually.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>Principal Name=<a href="mailto:user@example.com">user@example.com</a></td>
</tr>
<tr>
<td></td>
<td>DNS Name=myhost.example.com.COM</td>
</tr>
<tr>
<td></td>
<td>IP Address=10.11.12.13</td>
</tr>
<tr>
<td></td>
<td>IP Address=fe80::592f:6a4c:87b:b69a</td>
</tr>
<tr>
<td></td>
<td>IP Address=fe80::2e0:dbff:fe0b:f9e4</td>
</tr>
<tr>
<td></td>
<td>The user can add up to 20 different SANs. If an incorrect SAN type is entered, an error message, Unsupported SAN type, is displayed when the Send Details button is clicked.</td>
</tr>
<tr>
<td>Notes:</td>
<td>• The SAN field, DNS Name (FQDN) is not used for Machine Account validation. For example, when using a DMA, the DMA will not validate the RMX unless the FQDN field in the User Properties (New User) dialog box is correctly filled in.</td>
</tr>
<tr>
<td></td>
<td>• The SAN field should not be used when configuring the RMX for use in MS Lync Environments.</td>
</tr>
<tr>
<td>Hash Method</td>
<td>Select SHA-256 (in compliance with UC APL, FIPS 140-2).</td>
</tr>
<tr>
<td></td>
<td>Note: For backward compatibility, with previous versions, SHA-1 is selectable as the hash algorithm used in the creation of CSRs (Certificate Signing Requests).</td>
</tr>
</tbody>
</table>
5 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.

6 Click Copy Request to copy the New Certificate Request to the workstation’s clipboard.

7 Click Close.

8 Connect to your preferred Certificate Authority’s website using the web browser.

9 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 Certificates for the IP Network Service**

1 In the Certification Repository dialog box, select IP Network Service.

2 Repeat steps 2 to 9 above for the IP Network Service.

**Installing the Certificates**

TLS certificates can be generated using the following methods: CSR, PFX and PEM; each giving different options for Encryption Key length. The table below lists the SIP TLS Encryption Key length support for the various system components.
Polycom, Inc. 62

The specific security certificate requirements for Collaboration Servers used in Maximum Security Environments are:

- Support of 2048-bit encryption keys.
- Support of Extended Key Usage (EKU) for both:
  - Client Authentication
  - Server Authentication

The certificate template used by your CA server may need modification to meet the Collaboration Server requirements.

In Ultra Secure Mode, each Polycom device must have security certificates for the entire Chain Of Trust.

The Collaboration Server must have:

- The public certificate of each server in the CA Chain or hierarchy that issued its certificate. For example: RootCA « IntermediateCA « SubCA
- The public certificates of the chain that issued the administrator’s identity certificate. For example: UserRootCA « UserIntermediateCA « UserSubCA

**Certificate Expiry**

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.

**Installing the RMX Certificates**

After you have received the Certificates, Trusted (CA) Certificate(s), and CRL (if needed - OCSP is the preferred method for certificate maintenance) from the Certificate Authority, continue with the following installation procedures.
To install the certificate:

The following Steps 1 - 4 must be executed for both the Management Network and the IP Network Certificates.

1. Select (Ctrl + A) and 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.

   Steps 1 - 4 above must have been executed for both the Management Network and the IP Network Certificates before closing and updating the repository.

5. Click Close

6. Click Update Repository.

7. Re-boot the MCU.
Installing the Trusted Certificate(s)

To add a Trusted Certificate to the repository:
This procedure is performed for each CA Certificate that is to be added to the Certification Repository.
Two options are available for sending the certificate to the RMX:

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

Option. Paste Certificate and Send Certificate
After you have received the certificate from the Certificate Authority:
1. Copy (Ctrl + C) the certificate information from the Certificate Authority’s e-mail to the clipboard.
2. Click Paste Certificate to paste the clipboard content into the Send Certificate dialog box.
3. Click the Send Certificate button to send the certificate to the RMX.

Option. Send Certificate File
After you have received the certificate file from the Certificate Authority:
1. Click Send Certificate File.
   The Install File dialog box is displayed.
2. Select the Certificate File Format: PEM, DER, PKCS#7/P7B or PKCS#12/PFX.
3. Enter the certificate file name in the Install File field or click the Browse button.
   The Open file dialog box is displayed. The files are filtered according to the Certificate File Format selected in Step 2.
4. Enter the certificate file name in the File name field or click to select the certificate file entry in the list.

5. Click the Open button.

6. In the Install File dialog box, click the Yes button to proceed.
   The certificate is added to the Trusted Certificate List in the Certification Repository.

7. Optional. If there are additional Trusted Certificates to be added to the Certification Repository, repeat the above procedure.

**Installing the CRLs**

Use this procedure if CRL is the chosen method and OCSP is not to be used:

**CRL -** Requires at least one CRL file be installed, failing which an error message, At least one CRL should be installed, is displayed.

This procedure is performed for each CRL that is to be added to the Certification Repository.

**To add a CRL to the repository:**

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

1. In the CRL List tab, click the Add button.

2. The Install File dialog box is displayed.

3. Select the Certificate File Format: PEM or DER.

4. Enter the certificate file name in the Install File field or click the Browse button.

5. The Open file dialog box is displayed. The files are filtered according to the file type selected in Step 2.
6 Enter the Certificate file name in the File name field or click to select the certificate file entry in the list.

7 Click the Open button.

The certificate is added to the CRL List in the Certification Repository.

8 Optional. If there are additional Trusted Certificates to be added to the Certification Repository, repeat the above procedure.

When the Update Repository button is clicked, all added Trusted Certificates and CRLs are installed and the RMX displays an RMX Manager connection termination confirmation dialog box.

9 Click the OK button.

10 Login to the RMX to proceed with further management tasks.

Certificate Revocation

Certificate Revocation of IP Network and peer SIP TLS certificates for each defined IP Service can be enabled, disabled and configured. OCSP and CRL are the two Certificate Revocation methods available. OCSP is the preferred method.

To configure Certificate Revocation:

1 In the Revocation Method drop down menu select OCSP.

OSCP is the preferred method, and when selected, additional configuration options are displayed.
2 In the Global Responder URL field, type the URL of the Global Responder to be used. The format of the URL is validated and must be of the format: http(s)://responder.example.com/ocsp. The URL can be either http or https. If the Global Responder URL does not respond an Active Alarm is raised.

3 Optional. Clear the Use Responder Specified in Certificate check box. Optional. If it is required that the Responder URL is taken from the Authority Information Access (AIA) element of the Certificate, select the Use Responder Specified in Certificate check box. If the certificate does not contain a Responder URL, the Global Responder URL will be used.

4 Clear the Allow Incomplete Revocation Checks check box to ensure that all checks are performed. If the check box is and left unchecked and the Global Responder or the Responder Specified in the Certificate do not respond correctly, the certificate is considered revoked and system lock-out is possible. It is therefore important that the user pings the Global Responder or the Responder Specified in the Certificate to verify correct operation.

If the check box is checked and the Global Responder or the Responder Specified in the Certificate does not respond for any reason the certificate is not considered revoked.

System Flag:

Network latency or slow WAN links can cause login problems when logging in to the RMX's Management Network. The OCSP_RESPONDER_TIMEOUT System Flag can be added, and its value set to the number of seconds the MCU is to wait for an OCSP response from the OCSP Responder before failing the connection.

Default: 3 (seconds)

Range: 1-20 (seconds)
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 or RMX Manager 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.
3. Click the Security tab.
   The Security tab dialog box is displayed.
4. Configure Secured Communication:
   a. Select the Secured Communication check box.
   b. Un-Check the Skip certificate validation for user logging session check box.
   c. Select the Revocation Method - OCSP is preferred.
   d. In the Global Responder URL field, add a Global Responder URL if needed.
   e. Select the Use Responder Specified in Certificate check box.
   f. Un check the Allow Incomplete Revocation Checks check box.
   g. Un check the Skip Certificate Verification of OCSP Responder check box.
5. Click OK.
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 In the RMX Manager’s MCUs list, periodically highlight the RMX and then select Connect MCU.
   When the system has restarted and is back online the Login Banner will be displayed and you will be able to logon.

Procedure 7: Optional. Configure SIP/AS-SIP for the Signaling Network

Once all certificate configuration has been completed, the SIP/AS-SIP IP Network Service can be configured (if needed).
If SIP is not being used, skip to Procedure 8: Set System Configuration Flags.

To Configure AS-SIP for the Signaling Network:

1 In the RMX Management pane, click the IP Network Services button.
2 In the IP Network Services list pane, double-click IP Network Service.
3 When the IP Network Service Properties dialog box opens, click the SIP Servers tab.

4 Modify the following fields for UC APL compliance:

**IP Network Service - SIP Servers: AS-SIP**

<table>
<thead>
<tr>
<th>Field</th>
<th>Required Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Network Type</td>
<td>Select H323 &amp; SIP.</td>
</tr>
<tr>
<td>SIP Server</td>
<td>Select Specify.</td>
</tr>
<tr>
<td>Note: The IP address fields are enabled only if Specify is selected.</td>
<td></td>
</tr>
<tr>
<td>SIP Server Type</td>
<td>Select Generic.</td>
</tr>
<tr>
<td>Refresh Registration Every</td>
<td>Enter 3600.</td>
</tr>
<tr>
<td>Note: This value may be varied to accommodate specific environment requirements.</td>
<td></td>
</tr>
<tr>
<td>Transport Type</td>
<td>Select TLS.</td>
</tr>
<tr>
<td>Skip Certificate Validation</td>
<td>Unchecked.</td>
</tr>
<tr>
<td>Revocation Method</td>
<td>Select OCSP.</td>
</tr>
</tbody>
</table>
Procedure 8: 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

5 Click OK.
When the Maximum Security Environment is enabled by adding the ULTRA_SECURE_MODE System Flag and setting its value to YES using the Setup > System Configuration menu, YES, the enhanced security features are enforced.

The table below lists the default and recommended values of these flags in Ultra Secure Mode.

### System Flags and their default values

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOW_NON-ENCRYPT_PARTY_IN_ENCRYPT_CONF</td>
<td>If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No</td>
<td>NO</td>
</tr>
<tr>
<td>ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN</td>
<td>Enables the forwarding of all DTMF codes sent by participants in a Gateway Session to all PSTN and ISDN participants. Note: This System Flag must be added using the Setup &gt; System Configuration menu.</td>
<td>YES</td>
</tr>
<tr>
<td>ANAT_IP_PROTOCOL</td>
<td>When the RMX is configured for IPv4 and IPv6 addressing, the addition of the sdp-anat option tag in the SIP Require and SIP Supported headers allows a mixture of IPv4 and IPv6 addressing to be specified by the Session Description Protocol (SDP). For a full description of ANAT see IETF RFCs 4091 and 4092 and the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, &quot;Alternative Network Address Types (ANAT)&quot;. Default: Auto (In Ultra Secure Mode) Possible Values: DISABLED, AUTO, PREFER_IPv4, PREFER_IPv6</td>
<td>AUTO</td>
</tr>
<tr>
<td>DISABLE_INACTIVE_USER</td>
<td>Determines the number of consecutive days a user can be inactive before being disabled. Default: 30 Range: 1-90</td>
<td>30</td>
</tr>
<tr>
<td>ENABLE_CYCLIC_FILE_SYSTEM_ALARMS</td>
<td>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</td>
<td>YES</td>
</tr>
<tr>
<td>FORCE_STRONG_PASSWORD_POLICY</td>
<td>Enables or disables all password related flags. This flag cannot be set to NO when the RMX is in Ultra Secure Mode. Default: YES</td>
<td>YES</td>
</tr>
<tr>
<td>HIDE_CONFERENCE_PASSWORD</td>
<td>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</td>
<td>YES</td>
</tr>
</tbody>
</table>
## System Flags and their default values

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAST_LOGIN_ATTEMPTS</td>
<td>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</td>
<td>YES</td>
</tr>
<tr>
<td>MAX_KEEP_ALIVE_REQUESTS</td>
<td>The number of KeepAliveTimeout request intervals for the Apache server. In a Maximum Security Environment this value must be set to a value of 1814400 to ensure that the RMX Web Client / RMX Manager will remain connected for several hours, but not indefinitely. The exact time period depends on the type of client that is connected and the number of requests. Default: 0 (This value should never be used as the connection time is unlimited.) (If the SESSION_TIMEOUT_IN_MINUTES System Flag if configured, the RMX Web Client / RMX Manager will disconnect after the specified period if there is no keyboard or mouse activity.)</td>
<td>1814400</td>
</tr>
<tr>
<td>MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM</td>
<td>Determines the maximum number of management sessions per system. Default: 80 Range: 4-80</td>
<td>80</td>
</tr>
<tr>
<td>MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER</td>
<td>Determines the maximum number of management sessions per user. Default: 20 Range: 4-80</td>
<td>10</td>
</tr>
<tr>
<td>MIN_PASSWORD_LENGTH</td>
<td>Determines the minimum length of a user password. Default: 15 Range: 15-20</td>
<td>15</td>
</tr>
<tr>
<td>MIN_PWD_CHANGE_FREQUENCY_IN_DAYS</td>
<td>Determines the minimum number of days that users must retain passwords. Default: 1 Range: 1-7</td>
<td>1</td>
</tr>
<tr>
<td>NUMERICCHAIR_PASS_MIN_LEN</td>
<td>Determines the minimum length of a user chairperson password. Default: 9 Range: 9-16</td>
<td>9</td>
</tr>
<tr>
<td>NUMERIC_CONF_PASS_MIN_LEN</td>
<td>Determines the minimum length of a conference password. Default: 9 Range: 9-16</td>
<td>9</td>
</tr>
</tbody>
</table>
### System Flags and their default values

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP_RESPONDER_TIMEOUT</td>
<td>The number of seconds the RMX is to wait for an OCSP response from the OCSP Responder before failing the connection. Network latency or slow WAN links can cause login problems when logging in to the RMX's Management Network. This System Flag's value determines the number of seconds the MCU is to wait for an OCSP response from the OCSP Responder before failing the connection. Default: 3 (seconds) Range: 1-20 (seconds)</td>
<td>3</td>
</tr>
<tr>
<td>PASSWORD_EXPIRATION_N_DAYS</td>
<td>Determines the number of days that passwords remain valid. Default: 60 Range: 7-90</td>
<td>60</td>
</tr>
<tr>
<td>PASSWORD_EXPIRATION_N_WARNING_DAYS</td>
<td>Determines how many days before password expiration a warning of pending password expiration will be displayed to the users. Default: 7 Range: 7-14</td>
<td>7</td>
</tr>
<tr>
<td>PASSWORD_HISTORY_SIZE</td>
<td>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</td>
<td>10</td>
</tr>
<tr>
<td>QOS_IP_AUDIO</td>
<td>The default priority for audio packets.</td>
<td>0xb8 *</td>
</tr>
<tr>
<td>QOS_IP_SIGNALING</td>
<td>The default priority for Signaling Network packets.</td>
<td>0xA0 *</td>
</tr>
<tr>
<td>QOS_IP_VIDEO</td>
<td>The default priority for video packets.</td>
<td>0x68 *</td>
</tr>
<tr>
<td>QOS_MANAGEMENT_NETWORK</td>
<td>The default priority for Management Network packets.</td>
<td>0x10 *</td>
</tr>
<tr>
<td>REDUCE_CAPS_FOR_REDCOM_SIP</td>
<td>To accommodate deployments where some devices have limits on the size of the SDP payload in SIP messages (such as LSCs from Redcom running older software versions), when the flag value = YES the SDP size is less than 2kb and includes only one audio and one video media line. Default: NO Range: YES, NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
### System Flags and their default values

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEND_SRTP_MKI</td>
<td>Enables or disables the inclusion of the MKI field in SRTP packets sent by the RMX. Setting the value to NO to disables the inclusion of the MKI field in SRTP packets sent by the RMX. Set this flag to:</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>• NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▲ When all conferences on the RMX will not have MS-Lync clients participating and will have 3rd party endpoints participating.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▲ When using endpoints (eg. CounterPath Bria 3.2 Softphone) that cannot decrypt SRTP-based audio and video streams if the MKI (Master Key Identifier) field is included in SRTP packets sent by the RMX.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▲ When any conferences on the RMX will have both MS-Lync clients and Polycom endpoints participating.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▲ Some 3rd party endpoints may be unsuccessful in participating in conferences with this setting.</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td>• This System Flag must be added and set to YES (default) when Microsoft Office Communicator and Lync Clients are used as they all support SRTP with MKI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The system flag must be added and set to NO when Siemens phones (Openstage and ODC WE) are used in the environment as they do not support SRTP with MKI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Polycom endpoints function normally regardless of the setting of this flag.</td>
<td></td>
</tr>
<tr>
<td>Default:</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>SESSION_TIMEOUT_IN_MINUTES</td>
<td>The number of minutes after which, if there is no input from the user, the user’s connection to the RMX is terminated.</td>
<td>10</td>
</tr>
<tr>
<td>Default:</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Range:</td>
<td>1-999</td>
<td></td>
</tr>
<tr>
<td>SIP_FORMAT_GW_HEADERS_FOR_REDCOM</td>
<td>Controls whether the RMX adds special gateway prefix and postfix characters to the user portion of the SIP URI expressed in the “From” and “Contact” headers of SIP messages sent during calls involving Gateway Services. The addition of these characters can result in call failures with some SIP call servers. It is recommended to set this flag to YES whenever the RMX is deployed such that it registers its conferences to a SIP call server.</td>
<td>YES</td>
</tr>
<tr>
<td>Default:</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>
The relationship between the hexadecimal settings of the QoS System flags and the DSCP values is detailed in Procedure 10: Configure Precedence (DSCP) and QOS.

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 is displayed.
2 Locate and double-click on the System Flag to be modified. The Update Flag Name dialog box is displayed.
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 In the RMX Manager’s MCUs list, periodically highlight the RMX and then select Connect MCU. When the system has restarted and is back online the Login Banner will be displayed and you will be able to logon.

10 Connect to the RMX. See Connecting to the RMX.

Procedure 9: Optional. Configure 802.1X Authentication

- Perform this procedure if required within the environment.
- If 802.1X is being used on the production network, then it is possible that previous steps may have failed due to the RMX not being on the production network yet (and thus being unable to reach remote servers). After completing this step any such failures should not reoccur.

802.1X Authentication must be enabled for each Network Interface Controller (NIC).
To enable 802.1X Authentication:

1. In the RMX Menu, click Setup > Ethernet Settings
   The Ethernet Settings dialog box is displayed.

2. For each NIC, modify the Ethernet Settings table fields as set out in the table below.

### 802.1X Authentication - Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Authentication</td>
<td>For each NIC, click the arrow to open the drop-down menu and select the 802.1X Authentication method:</td>
</tr>
<tr>
<td></td>
<td>• EAP-TLS</td>
</tr>
<tr>
<td></td>
<td>• PEAPv0</td>
</tr>
<tr>
<td></td>
<td>Note: EAP-MD5 and MSCHAPv2 are also available as options. Selecting Off disables 802.1X Authentication.</td>
</tr>
<tr>
<td>User</td>
<td>Enter the User name that the RMX will use to register with the 802.1X Authentication Server. If the Domain Name (DC) field was completed in the Certificate Request, the User must be: &lt;Common Name (DNS)&gt;@&lt;Domain Name (DC)&gt; as set out in the Certificate Request.</td>
</tr>
<tr>
<td>Password (EAP-MD5, PEAPv0 and MSCHAPv2 only)</td>
<td>Enter the Password, that the RMX will use to register with the 802.1X Authentication Server. Up to 256 Unicode characters can be used. The Password is always displayed as four asterisks.</td>
</tr>
</tbody>
</table>

3. When 802.1X Authentication is configured for all NICs, click OK.
   A warning message is displayed:
4. Click OK.
   The RMX is disconnected from the network.
5. Disconnect the RMX’s LAN cables from the existing network and re-connect them to the 802.1X Authentication-enabled network.
6. Login to the RMX from the 802.1X Authentication-enabled network.

Procedure 10: Configure Precedence (DSCP) and QOS

Precedence is disabled by default and must be enabled and configured for AS-SIP deployments.

When enabling Precedence the Signaling DSCP value is considered as part of the full Diffserv Field. Its value of 40 relates to the hexadecimal value 0xA0 entered for the QOS_IP_SIGNALING System Flag value configured in Procedure 8: Set System Configuration Flags, as follows:

**Signaling DSCP value**

<table>
<thead>
<tr>
<th>Signaling DSCP Value</th>
<th>DSCP Signaling Value (Standalone)</th>
<th>Diffserv Field</th>
<th>DSCP Signaling Value (As part of Diffserv field)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>Binary</td>
<td>Hex</td>
<td>Decimal</td>
</tr>
<tr>
<td>40</td>
<td>101000</td>
<td>0x28</td>
<td>160</td>
</tr>
</tbody>
</table>

* The QOS/IP_SIGNALING System Flag value is set as the hexadecimal equivalent of four times the Signaling DSCP’s decimal value.

**To enable Precedence:**

1. On the RMX menu, click Setup > Precedence Settings.
   The Precedence Settings dialog box is displayed.

2. Select the Use Precedence check box.
3. In the Precedence Domain drop-down menu select 1.
4 In the Domain Name field, enter uc-000000.
5 In the Signaling DSCP field enter 40.
6 Optional. Modify the Audio DSCP and Video DSCP values for each of the Precedence Levels according to local site requirements.
7 Optional. Modify the r-priority values for each of the Precedence Levels according to local site requirements.
8 In the Precedence Domain drop-down menu select 2.
9 In the Domain Name field, enter dsn-000000.
10 In the Signaling DSCP field enter 40.
11 Optional. Modify the Audio DSCP and Video DSCP values for each of the Precedence Levels according to local site requirements.
12 Optional. Modify the r-priority values for each of the Precedence Levels according to local site requirements.
13 Click OK.

Procedure 11: 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 12: Optional. Modify Default Login and Main Screen Banner Text

The Login and Main Screens of 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:

![Login Screen Banner Example]

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

![Main Screen Banner Image]

Customizing Login and Main Screen Banners

The Login and Main Screen banners can be customized when the RMX is in either .

To customize the banners:

1. In the RMX menu, click Setup > Customize Display Settings > Banners Configuration.
2. Customize the banners by modifying the following fields:
Procedure 13: 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.

Banner Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Page Banner</td>
<td>Select or clear the check box to enable or disable the display of the banner. Banner display cannot be disabled in .</td>
</tr>
<tr>
<td></td>
<td>Edit the text in this field to meet local requirements:</td>
</tr>
<tr>
<td></td>
<td>• Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used.</td>
</tr>
<tr>
<td></td>
<td>• Maximum banner size is 100KB.</td>
</tr>
<tr>
<td></td>
<td>• The banner may not be left blank in .</td>
</tr>
<tr>
<td>Main Page Banner</td>
<td></td>
</tr>
</tbody>
</table>

3. Click the OK button.
5 Enter a new User Name in the New User Name field and click OK.
6 Logout of the RMX.
7 Login, using the new User Name.
8 Click Login.
   The Change Password/Login - Welcome screen is displayed:
   The system will notify you that you must change the password.
9 Click OK.

10 Enter the new Username.
11 Enter the old Password.
12 Enter the New Password.
13 Confirm the New Password.
14 Click OK.

Procedure 14: 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 15: Configure Whitelist Access

For security reasons it is important that a list of devices permitted to connect to the RMX is configured. The Whitelist contains the addresses of all IP devices permitted to connect to the RMX.

To view or modify the Whitelist:

1 In the RMX Management pane, click the IP Network Services.
2 In the IP Network Services list pane, double-click the Management Network entry.
3 In the Management Network Properties dialog box click the WhiteList tab.
   The Whitelist dialog box is displayed.
   ➢ If there are no entries in the Whitelist, it is disabled to prevent lock out.
   ➢ If the Whitelist is disabled none of the IP addresses in the list are displayed.
   ➢ The Add and Remove buttons are only active if the Enable Whitelist check box is selected.
4  Select the Enable Whitelist check box.

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

5  Modify the Whitelist.

Both IPv4 and IPv6 addresses are supported and the system will only allow entry of the type of IP addresses for which it is configured according to the table below.

### IP Address Modes

<table>
<thead>
<tr>
<th>IP Address Modes</th>
<th>RMX</th>
<th>Workstation / Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv4 &amp; IPv6</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv4 &amp; IPv6</td>
</tr>
<tr>
<td>IPv4 &amp; IPv6</td>
<td>IPv4</td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv4 &amp; IPv6</td>
</tr>
</tbody>
</table>

- If the system changes its IP addressing mode (e.g. from IPv4 only to both IPv4 &6) while the Whitelist is enabled, the Whitelist is disabled and a message, Whitelist has been disabled please reconfigure, is displayed.
- IPv4 addresses can be added as a range by substituting the 3rd and 4th dotted decimal numbers of the IP address with * characters, e.g. 11.10.*.*
6 Add IP addresses to the Whitelist:
   For each IP address to be added to the Whitelist:
   a In the Add IP Address field enter an IP address to be added to the Whitelist and click the Add button to add the IP address to the Whitelist.
      If an invalid IP address is entered, an error message is displayed and the administrator is prompted to enter a correct IP address.
   b When all the IP addresses have been added, click OK.
      A message is displayed: Applying Whitelist will limit RMX web access to the configured IP list, are you sure you want to continue?
   c Click Yes to apply the modified Whitelist.

Procedure 16: Configure Gateway Services

RMX Gateway Services provide connectivity between the following protocol combinations:

- PSTN ↔ H.320
- PSTN ↔ H.323
- PSTN ↔ SIP
- PSTN ↔ AS-SIP
- H.320 ↔ H.323
- H.320 ↔ SIP
- H.320 ↔ AS-SIP
- H.323 ↔ SIP
- H.323 ↔ AS-SIP

This connectivity is facilitated by special conference acting as a Gateway Session, created on the RMX. It includes one dial-in connection of the endpoint initiating the Gateway Session and one or several dial-out connections to endpoints.

These Gateway Services are internal to the RMX, not to be confused with the V.35 Serial Gateway capabilities detailed in Deploying a Polycom RMX™ Serial Gateway S4GW on page 144.

Configuring the Gateway Components on the RMX

To enable Gateway Calls in the RMX, the following components have to be configured:

- Conference IVR Service to be used with the Conference Profile assigned to the Gateway Profile. The IVR Services are used for Gateway IVR connections.
- Conference Profile that includes the IVR Service for the Gateway Session and the settings to automatically terminate the Gateway Session when one participant is still connected or when no participants are connected
- Gateway Profile for call routing.

For more information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, "Gateway Calls".
Basic Operation

The RMX Manager is the recommended option for accessing the RMX's Management Console.

The RMX Manager can only be downloaded to the workstation from the link in the Welcome screen before the RMX is placed into Ultra Secure Mode. Subsequent downloads of the RMX Manager, if necessary, must be obtained from the Polycom website at http://www.polycom.com/federal.

The most common operations performed via the RMX Manager 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 Manager

Once installed, the RMX Manager is started using the https:// (secured) command in the browser’s address line from the Windows Start menu.

To use the browser:

1. In the browser’s command line, enter:
   
   https://<MCU Control Unit IP Address>/RMXManager.html

2. Press Enter.

To use the Windows Start menu:

1. Click Start > Programs.
   a. If the RMX Manager is displayed in the recently used programs list, click RMX Manager in the list to start the application.
   
   or
b Click All Programs > Polycom > RMX Manager.

The MCUs screen is displayed, listing the MCUs currently defined in the RMX Manager.

This screen enables you to add additional MCUs or connect to any of the MCUs listed. For each listed MCU, the system displays the following information:

- MCU Display Name (as defined in the Add MCU dialog box).
- IP Address of the MCU’s control unit
- Product Type - The MCU type: RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000, or RealPresence Collaboration Server (RMX) 4000. Before connecting to the MCU for the first time, the RMX type is unknown so “RMX” is displayed instead as a general indication.
Connecting to the MCU

Once an MCU is defined, the RMX Manager can be connected to it. This allows you to set up conferences, make reservations, monitor On Going Conferences and perform other activities on several MCUs.

The first RMX unit that is connected to the RMX Manager dictates the Authorization Level of Users that can connect to the other MCUs on the list. For example, if the Authorization level of the User POLYCOM is Administrator, all Users connecting to the other MCUs on the list must be Administrators. Each user can have a different login name and password for each of the listed MCUs and they must be defined in the Users list of each of the listed MCUs.

To connect the RMX Manager to an MCU:

1. In the MCUs list, use one of the following methods:
   a. Double-click the MCU icon.
   b. Select the RMX to connect and click the Connect MCU button.
   c. Right-click the MCU icon and then click Connect MCU.

2. Click Accept.

   The Username / Password dialog box is displayed.

3. Enter the Username and Password.
4 Click OK.

The RMX Manager - Main Screen is displayed.

If you are connecting to any MCU from the MCUs pane in the RMX Manager Main Screen and have defined the Username and Password for the connecting MCU, the MCU icon changes to connected and its status, type and number of audio and video resources are displayed in the MCUs pane.

Login Record

The system can display a record of the last Login of the user. It is displayed in the Main Screen of the RMX Manager. The user Login Record display is enabled when the LAST_LOGIN_ATTEMPTS System Flag is set to YES, which is the default when the ULTRA_SECURE_MODE System Flag is set to YES.
Both lists display the:

- Date and Time of the Login attempt.
- IP Address of the workstation initiating the Login attempt.

The list of unsuccessful Logins can contain up to ten records.

Failed Login attempts are written to the system Log Files and are recorded as Audit Events. The Audit files can be retrieved by the Administrator User.

**RMX Manager Screen Components**

The *RMX Manager* Main Screen is displayed only when at least one MCU is connected.
Only one MCU can be selected in the MCUs pane. If only one MCU is connected, it is automatically selected. The selected MCU is highlighted.

The menu items, the RMX Management features, the Address Book and the Conference Templates are all properties of the selected MCU and apply to it.

**MCUs Pane**

The MCUs pane includes a list of MCUs and a toolbar.

For each listed MCU, the system displays the following information:
- MCU Display Name - the name of the MCU and its icon according to its type and connection status. The following icons are available:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 1500, disconnected.</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 1500, connected.</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 2000, disconnected.</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 2000, connected.</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 4000, disconnected.</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td>RealPresence Collaboration Server (RMX) 4000, connected.</td>
</tr>
</tbody>
</table>

- IP Address of the MCU’s control unit.
- Status - The status of the MCU:
  - Connected - the MCU is connected to the RMX Manager and can be managed by the RMX Manager user.
  - Disconnected - The MCU is disconnected from the RMX Manager
  - Major - The MCU has a major problem. MCU behavior could be affected and attention is required.
- Product Type - The MCU type: RealPresence Collaboration Server 1500/2000/4000. Before connecting to the MCU for the first time, the RMX type is unknown so RMX is displayed instead as a general indication.
- Monitored - When checked indicates that the conferences running on this MCU are automatically added to the Conferences list and monitored. To stop monitoring the conferences running on this MCU and their participants, clear the Monitored check box.
- Video Resources - The number of video resources that are available for conferencing.
- Audio Resources - The number of audio resources that are available for conferencing.

**MCUs Toolbar**
The MCUs toolbar contains the following buttons:
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).

If Conference Recording is enabled the following are displayed in color:

- **Start/Resume Recording** – start/resume recording.
- **Stop Recording** – stop recording.
- **Pause** – toggles with the Start/Resume button.

When right-click on a specific conference, lock and unlock conference options are available:

- **Lock Conference** – lock the conference. Participants of the conference become invisible, and other users cannot join the conference.
- **Unlock Conference** – unlock the conference.

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 Manager 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.

For more information about Active Alarms and Faults List, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, "System and Participant Alerts”.

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.
**Port Usage Gauges**

The Port Usage gauge indicates:

- 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.

The MCUs toolbar contains the following buttons:
**MCU State**

The MCU State indicator displays one of the following:

- **Starting up (15:25)** – 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.

- **NORM** – The MCU is functioning normally.

- **MAJOR** – 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.

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 Collaboration Server Manager, the Address Book pane is displayed as a closed tab. You can open 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.

**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 Manager main window. You can open it by clicking the anchor pin ( ) button. 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.

**Adding MCUs to the MCUs List**

The *RMX Manager* can connect to one or several *RMXs* simultaneously. If the site’s configuration includes more than one MCU, or when a new MCU is added to your configuration, and you want to monitor and control all MCUs from within the same window, you must add the MCU to the MCUs list.

The *RMX* must be installed and its IP addresses properly configured in the Management Network Service before defining its connection parameters in the *RMX Manager* application.

To add the MCU to the list of MCUs being managed, define the MCU’s connection parameters.

**To add a *RMX* unit:**

1. On the MCUs toolbar, click the **Add MCU** button to add an MCU to the MCU list. The Add MCU dialog box opens.
2. Define the following parameters:

**MCU Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Name</td>
<td>Enter the name of the MCU on the network.</td>
</tr>
<tr>
<td><strong>MCU IP</strong></td>
<td>Enter the IP address of the MCU’s Control Unit. The IP address must be</td>
</tr>
<tr>
<td></td>
<td>identical to the one configured in the MCU during first entry Configuration.</td>
</tr>
<tr>
<td></td>
<td>For more details, see <em>Procedure 2: Gather Network Equipment and Address Information</em> on page 22.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port used for communication and data transactions between the <em>RMX</em> unit and the <em>RMX Manager</em>. For standard connection, enter 80. For a Secured connection (using TLS or SSL).</td>
</tr>
</tbody>
</table>
### MCU Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the user name with which you will login to the MCU. A User with this name must be defined in the RMX Users list. The system is shipped with a default User whose name is POLYCOM.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password as defined for the user name with which you will login to the MCU. The system is shipped with a default User whose password is POLYCOM.</td>
</tr>
<tr>
<td>Secure Mode</td>
<td>(Optional) Select this check box to connect to the RMX with SSL and work in Secure Mode</td>
</tr>
<tr>
<td>Remember Login</td>
<td>This check box is automatically selected, and it enables the usage of the user name and password entered in this dialog box when connecting to the RMX. If this check box is cleared, the user is prompted for the user name and password when connecting to this RMX unit.</td>
</tr>
<tr>
<td>Auto Reconnection</td>
<td>Select this check box to automatically reconnect to the RMX if the connection between the RMX Manager and the MCU is broken.</td>
</tr>
<tr>
<td>Interval</td>
<td>Enter time in seconds between reconnect ion attempts to the RMX. For example, if you enter 10, the system will wait 10 seconds between the connection attempts.</td>
</tr>
<tr>
<td>Max Time</td>
<td>Enter the maximum amount of time in seconds that the RMX is allowed to try to reconnect. If the RMX reconnects before the allotted time frame the count down timer is halted. For example, if you enter 100, the system will stop trying to reconnect if it has failed to do so within 100 seconds.</td>
</tr>
</tbody>
</table>

3. Click **OK**. The MCU is added to the MCUs pane.
4. If required, repeat steps 1-3 to define additional RMX units.

The MCUs pane contains the list of all defined MCUs.
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 Manager 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 2000 display window to its default configuration:

- On the RMX 2000 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.
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 Manager. 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 106.
- 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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “Meeting Rooms”.
- 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 Collaboration Server 1500/2000/4000 Administrator’s Guide, “Entry Queues, Ad Hoc Conferences and SIP Factories”.
- 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.
- Start from any Conference Template saved in the Conference Templates list.

Although SVC Conferencing Mode options are available in Conference Profiles, it is advised that they not be used with Version 8.5.10

Starting a Conference from the Conferences Pane

To start a conference from the Conference pane:

1. In the MCUs pane, select the MCU to run the conference.
2. 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.

   If you are the meeting chairperson or organizer using the RMX Manager to start your own meeting, you need to communicate the default conference ID (or the one you created) to the other conference participants so they can dial in.

   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

1. Define the following parameters:

## General Tab Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Manager.</td>
</tr>
<tr>
<td></td>
<td>In conferences, Meeting Rooms and Entry Queues the system automatically generates an ASCII name for the Display Name field that can be modified using Unicode encoding.</td>
</tr>
<tr>
<td></td>
<td>• English text uses ASCII encoding and can contain the most characters (length varies according to the field).</td>
</tr>
<tr>
<td></td>
<td>• European and Latin text length is approximately half the length of the maximum.</td>
</tr>
<tr>
<td></td>
<td>• Asian text length is approximately one third of the length of the maximum.</td>
</tr>
<tr>
<td></td>
<td>The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII).</td>
</tr>
<tr>
<td></td>
<td>Maximum field length in ASCII is 80 characters.</td>
</tr>
<tr>
<td></td>
<td>If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is displayed in all tabs.</td>
</tr>
<tr>
<td>Duration</td>
<td>Define the duration of the conference in hours using the format HH:MM (default 01:00).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is displayed in all tabs.</td>
</tr>
<tr>
<td>Routing Name</td>
<td>Routing Name 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 defined using ASCII characters.</td>
</tr>
<tr>
<td></td>
<td>Comma, colon and semicolon characters cannot be used in the Routing Name.</td>
</tr>
<tr>
<td></td>
<td>The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows:</td>
</tr>
<tr>
<td></td>
<td>• If ASCII characters are entered as the Display Name, it is used also as the Routing Name</td>
</tr>
<tr>
<td></td>
<td>• If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the Display Name, the ID (such as Conference ID) is used as the Routing Name.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Profile</td>
<td>The system displays the name of the default Conference Profile. Select the required Profile from the list.</td>
</tr>
<tr>
<td></td>
<td>The Conference Profile includes the Conference line rate, media settings and general settings.</td>
</tr>
</tbody>
</table>
2 If all participants are undefined, dial-in and no additional information is required for the new conference, click OK.

3 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.

1 Click the Participants tab.

The Participants tab opens.
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.

### New Conference — Participants Tab

<table>
<thead>
<tr>
<th>Column / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Participants List</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A Unicode field that displays the participant’s name and an icon representing the endpoint type: Audio Only or Video.</td>
</tr>
<tr>
<td>IP Address/Phone</td>
<td>Indicates the IP address or phone number of the participant’s endpoint.</td>
</tr>
<tr>
<td></td>
<td>• For dial-out connection, displays the IP address or phone number of the endpoint called by the RMX.</td>
</tr>
<tr>
<td></td>
<td>• For dial-in connection, displays the participant’s IP address or phone number used to identify and route the participant to the appropriate conference.</td>
</tr>
<tr>
<td>Alias Name (IP Only)</td>
<td>Displays the alias name of an H.323 endpoint.</td>
</tr>
<tr>
<td>Network</td>
<td>The network communication protocol used by the endpoint to connect to the conference: H.323 or ISDN/PSTN.</td>
</tr>
<tr>
<td>Dialing Direction</td>
<td>Dial-in – The participant dials in to the conference</td>
</tr>
<tr>
<td></td>
<td>Dial-out – The Collaboration Server dials out to the participant</td>
</tr>
</tbody>
</table>
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.

To add participants from the Address Book:

1. In the Participants List, click the Add from Address Book button to open the Participants Address Book.
2 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.

3 The selected participants are assigned to the conference and appear in the Participant List.

4 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.
To add information to the conference:

1. Click the Information tab.
   
The Information tab opens.

2. Enter the following information:

   **Information Tab Parameters**
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info1, 2, 3</td>
<td>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.</td>
</tr>
<tr>
<td>Billing</td>
<td>Enter the conference billing code if applicable.</td>
</tr>
</tbody>
</table>

3. 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 MCUs pane, select the MCU to run the conference.

2. In the RMX Management pane, click the Reservation Calendar button ( ). The Reservation Calendar is displayed.

3. Click the New Reservation button. The New Reservation – General tab dialog box opens.
4  **(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.

5  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.

6  Click the **OK** button.

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

7  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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, "Reservations".

### Starting an Ongoing Conference From a Template

An ongoing conference or a Reservation can be started from any Conference Template saved in the Conference Templates list of the selected MCU.
To start an ongoing conference or a reservation from a Template:

1. In the MCUs pane, select the MCU to run the conference.
2. In the Conference Templates list, select the Template you want to start as an ongoing conference.
3. Click the **Start Conference from Template** button to start a conference or **Schedule Reservation from Template** button to schedule a reservation.
   or
   Right-click and select **Start Conference from Template** to start an ongoing conference or **Schedule Reservation from Template** to schedule a reservation.

   ![Image of MCU and Conference Templates]

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 *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "Conference Templates".
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 gatekeeper925
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.

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 gatekeeper925
Entry Queue ID 1000
   - The participant dials9251000

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

H.323 participants can also bypass the conference IVR voice messages by adding the Conference Password to the initial dial string:

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

Example:
Conference ID 1001
Conference Password 34567
   - H.323 participants dial 9251000##1001##34567

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 number9251000
   - ISDN/PSTN participants dial9251000

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 Manager, 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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “System Configuration”.

**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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “System Configuration”

**Monitoring Ongoing Conferences**

When MCUs are connected to the *RMX Manager* they are automatically monitored, that is, any ongoing conference that is started on that MCU is automatically added to the Conferences pane and its participants are monitored.
To list participants from several conferences (running on the same or different MCUs):

- In the Conferences pane, using Windows multiple selection methods, select the conferences whose participants you want to list. The participants are displayed in the Participants list pane. By default, the participants are grouped by conferences, and the name of the MCU is displayed in the first column of the properties table, enabling sorting according to MCU name.

**Grouping the Participants by MCU**

The Participants can be grouped by MCU and then by conferences.

To change the display mode for the Participants pane:

- On the RMX Menu, click View > Group by MCU. The Participants pane display changes accordingly.

**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. When Conference Recording is enabled in a conference’s Profile, the Conference Recording buttons are enabled.
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 the following table may appear in the Status column.

### Conferences — Monitoring Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name    | Displays conference name and type of conference:  
• 🎤 – Video Conference (including HD CP conferences).  
• 🎥 – High Definition Video Conference running in Video Switching mode.  
• 📋 – The conference has been secured using the *71 DTMF code. |
| Status  | Displays the status of the ongoing conference.  
If there is no problem with the participant’s connection no indication is displayed.  
If one of the following statuses occurs, the appropriate indication is displayed, proceeded by a warning icon (⚠️).  
• **Audio** – There is a problem with the participant’s audio.  
• **Empty** – No participants are connected.  
• **Faulty Connection** – Participants are connected, but the connection is problematic.  
• **Not Full** – Not all the defined participants are connected.  
• **Partially Connected** – The connection process is not yet complete; the video channel has not been connected.  
• **Single Participant** – Only one participant is connected.  
• **Video** – There is a problem with the participant’s video. |
| ID      | The Conference ID assigned to the conference. |
| Start Time | Conference start time. |
| End Time | 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 RealPresence Collaboration Server (RMX) 2000/4000 Administrator’s Guide.

**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:

**Participant Connection Details**

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Icon/Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name and type (icon) of the participant:</td>
</tr>
<tr>
<td>Audio Participant</td>
<td>Connected via IP phone or ISDN/PSTN.</td>
</tr>
<tr>
<td>Video Participant</td>
<td>Connected with audio and video channels.</td>
</tr>
</tbody>
</table>
## Participant Connection Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Icon/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Displays the connection status (text and icon) of the participant. If there is no problem with the participant's connection no indication is displayed.</td>
</tr>
<tr>
<td><strong>Connected</strong></td>
<td>The participant is successfully connected to the conference.</td>
</tr>
<tr>
<td><strong>Disconnected</strong></td>
<td>The participant is disconnected from the conference. This status applies only to defined participants.</td>
</tr>
<tr>
<td><strong>Waiting for Dial-in</strong></td>
<td>The system is waiting for the defined participant to dial into the conference.</td>
</tr>
<tr>
<td><strong>Partially Connected</strong></td>
<td>The connection process is not yet complete; the video channel has not been connected.</td>
</tr>
<tr>
<td><strong>Faulty Connection</strong></td>
<td>The participant is connected, but problems occurred in the connection, such as synchronization loss.</td>
</tr>
<tr>
<td><strong>Secondary Connection</strong></td>
<td>The endpoint's video channel cannot be connected to the conference and the participant is connected only via audio.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Displays the participant's role or function in the conference:</td>
</tr>
<tr>
<td><strong>Chairperson</strong></td>
<td>The participant is defined as the conference chairperson. The chairperson can manage the conference using touch-tone signals (DTMF codes).</td>
</tr>
<tr>
<td><strong>Lecturer</strong></td>
<td>The participant is defined as the conference Lecturer.</td>
</tr>
<tr>
<td><strong>Lecturer and Chairperson</strong></td>
<td>The participant is defined as both the conference Lecturer and Chairperson.</td>
</tr>
<tr>
<td><strong>Cascade Enabled Dial-out Participant</strong></td>
<td>A special participant functioning as a link in a cascaded conference.</td>
</tr>
<tr>
<td><strong>Recording</strong></td>
<td>A special participant functioning as a Recording Link.</td>
</tr>
<tr>
<td><strong>IP Address/Phone</strong></td>
<td>The IP participant's IP address or the ISDN/PSTN participant's phone number.</td>
</tr>
<tr>
<td><strong>Alias Name</strong></td>
<td>The participant's Alias Name. The alias of an RSS 2000 Recording System if the participant is functioning as a recording link.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>The participant's network connection type – H.323 or ISDN/PSTN.</td>
</tr>
<tr>
<td><strong>Dialing Direction</strong></td>
<td><strong>Dial-in</strong> – The participant dialed the conference.</td>
</tr>
<tr>
<td></td>
<td><strong>Dial-out</strong> – The MCU dialed the participant.</td>
</tr>
</tbody>
</table>
### Starting Monitoring / Stopping Monitoring

By default, all conferences running on connected RMXs are monitored.

You can stop the automatic monitoring of conferences on a specific MCU in one of the following methods:

- By clearing the check box in the Monitored column in the MCUs pane.

---

For more information, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “Participant Level Monitoring”.

---

### Participant Connection Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Icon/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><img src="muted.png" alt="Muted" /> – Participant’s audio channel is muted. The participant can still hear the conference.</td>
</tr>
<tr>
<td></td>
<td><img src="blocked.png" alt="Blocked" /> – Transmission of audio from the conference to the participant is blocked.</td>
</tr>
<tr>
<td></td>
<td><img src="muted_blocked.png" alt="Muted and Blocked" /> - Audio channel is muted and blocked.</td>
</tr>
<tr>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><img src="suspended.png" alt="Suspended" /> – Video transmission from the endpoint to the conference is suspended.</td>
</tr>
<tr>
<td></td>
<td><img src="secondary.png" alt="Secondary" /> – Participant is connected only through the audio channel due to problems with the video channel.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Indicates that the endpoint is connected to the conference using encryption.</td>
</tr>
<tr>
<td>FECC Token</td>
<td><img src="fecc_token.png" alt="FECC Token" /> 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.</td>
</tr>
<tr>
<td>Content Token</td>
<td><img src="content_token.png" alt="Content Token" /> Participant is the holder of the Content token and has content sharing permission. The Content token can be allocated to only one participant at a time and remains un-allocated if no participant requests it. For more information, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “H.239”.</td>
</tr>
</tbody>
</table>
Right-clicking the MCU icon and selecting Stop Monitoring.

The check box is cleared in the Monitored column.

To start monitoring again, click the check box in the Monitored column in the MCUs pane, or right-clicking the MCU icon and selecting Start Monitoring.

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** 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.

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.

- Participant level video forcing overrides conference level video forcing.

- A participant can view him/herself in a layout window, by selecting the Same Layout option.

- When different size video windows are used in video layouts such as 1+2, 1+3, 1+4, etc., a participant can only be forced, in Personal Layout, to a video window of the same size as that selected for him/her in Conference Layout.

- When changing the Video Layout at the conference level, the video forcing settings are not applied to a new layout, and switching between participants is audio-activated. The video forcing setting are saved and applied the next time the layout is selected.

- Windows that are not assigned any participant display the current speaker and last speakers.

**To video force a participant to a window:**

1. In the Conference Properties dialog box, select the Video Settings tab.
2. If Auto Layout check box is selected, clear it.
3. Select the required video layout.
4. In the window to which you want to force a participant, select the participant's name from the list of conference participants.
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 the following table.

### Participant Information

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Participant</td>
<td><img src="image" alt="Definition" /></td>
<td>Define a new participant. For more information about the New Participant dialog box tab, see New Conference — Participants Tab on page 109.</td>
</tr>
<tr>
<td>Add Participant From Address Book</td>
<td><img src="image" alt="Open Address Book" /></td>
<td>Open the Address Book to select the participant for the conference. For more information about the Address Book, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “Address Book” on page.</td>
</tr>
<tr>
<td>Connect Participant</td>
<td><img src="image" alt="Connect" /></td>
<td>Connect a disconnected defined dial-out participant to the conference.</td>
</tr>
<tr>
<td>Disconnect Participant</td>
<td><img src="image" alt="Disconnect" /></td>
<td>Disconnect the participant from the conference.</td>
</tr>
<tr>
<td>Delete Participant</td>
<td><img src="image" alt="Delete" /></td>
<td>Delete the selected participants from the conference.</td>
</tr>
<tr>
<td>Mute Audio</td>
<td><img src="image" alt="Mute" /></td>
<td>Mute the audio transmission from the participant to the conference. The Audio Muted indicator appears in the Participants List and the Unmute Audio button becomes active.</td>
</tr>
<tr>
<td>Unmute Audio</td>
<td><img src="image" alt="Unmute" /></td>
<td>Resume the participant’s audio transmission to the conference. The Mute Audio button becomes active.</td>
</tr>
<tr>
<td>Suspend Video</td>
<td><img src="image" alt="Suspend" /></td>
<td>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 Suspend Video indicator appears in the Participants List and the Resume Video button becomes active.</td>
</tr>
<tr>
<td>Resume Video</td>
<td><img src="image" alt="Resume" /></td>
<td>Resume the participant’s video transmission to the conference. The Suspend Video button becomes active.</td>
</tr>
<tr>
<td>Block Audio</td>
<td><img src="image" alt="Block" /></td>
<td>Block the audio transmission from the conference to the participant. When blocked, the participant can still be heard by the conference. The Audio Blocked indicator appears in the Participants List and the Unblock Audio button becomes active.</td>
</tr>
<tr>
<td>Unblock Audio</td>
<td><img src="image" alt="Unblock" /></td>
<td>Resume the audio transmission from the conference to the participant. The Block Audio button becomes active.</td>
</tr>
</tbody>
</table>
Personal Layout Control with the RMX Manager

RMX users can use the RMX Manager 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**.

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Participant to Address Book</td>
<td><img src="image" alt="Add Participant to Address Book" /></td>
<td>Add selected participant’s details to the Participant Address Book.</td>
</tr>
<tr>
<td>Abort H.239 Session</td>
<td></td>
<td>To withdraw the Content Token from the participant back to the MCU for re-assignment.</td>
</tr>
<tr>
<td>Change to Chair-person</td>
<td></td>
<td>Define the selected participant as the conference leader/chairperson.</td>
</tr>
<tr>
<td>Change to Regular Participant</td>
<td></td>
<td>Define the chairperson as a regular participant without chairperson privileges.</td>
</tr>
<tr>
<td>Connect to Website</td>
<td></td>
<td>Connect directly to the internal website of the participant’s endpoint to perform administrative, configuration and troubleshooting activities.</td>
</tr>
<tr>
<td>AGC (Auto Gain Control)</td>
<td><img src="image" alt="AGC (Auto Gain Control)" /></td>
<td>Enable AGC for the participant with weak audio signal during ongoing conferences.</td>
</tr>
<tr>
<td>Participant Properties</td>
<td></td>
<td>To view all Participant Properties.</td>
</tr>
</tbody>
</table>

For more information, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, “**Participant Level Monitoring**” on.
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.

A 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

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>
<thead>
<tr>
<th>DTMF Code</th>
<th>Layout Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

**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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide, “Defining a New Conference IVR Service”.

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

### DTMF Codes

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

### Modifying the MCU Properties

You can view the currently defined MCU settings, and modify them when required, for example, change the MCU name, IP address or Secured mode.
Use this procedure to add the Username and Password to the properties of the MCU that was automatically added to the MCU list when installing the RMX Manager. This enables automatic login when connecting the MCU to the RMX Manager.

You can modify the MCU properties when the MCU is connected or disconnected.

**To view and/or modify the MCU Properties:**

1. Use one of the following methods:
   a. Select the MCU to disconnect and click the [MCU Properties] button.
   b. Right-click the MCU icon and then click [MCU Properties]

   The MCU Properties dialog box opens.

2. Define/modify the required parameters. For details, see [MCU Properties] on page 102.

3. Click [OK].

**Disconnecting an MCU**

An MCU can be disconnected from the RMX Manager, without removing it from the MCUs list.

**To disconnect an MCU:**

1. Use one of the following methods:
   a. Select the MCU to disconnect and click the [Disconnect MCU] button.
   b. Right-click the MCU icon and then click [Disconnect MCU].

   The MCU icon changes to disconnected and any ongoing conference running on that MCU will not be monitored in this RMX Manager; they are removed from the Conferences pane. This MCU can still be monitored and controlled by other users.

**Removing an MCU from the MCUs Pane**

An MCU can be removed from the RMX Manager. This function should be used if the MCU hardware was disconnected and removed from the network.
To Remove an MCU from the list:

1 Use one of the following methods:
   a Select the MCU to disconnect and click the Delete button.
   b Right-click the MCU icon and then click Remove MCU.

   ![RMX Manager menu](image)

   A confirmation message is displayed.

2 Click OK to confirm or Cancel to abort the operation.

   The MCU icon is removed from the MCUs pane.

Changing the RMX Manager Language

You can change the language of the RMX Manager menus and dialog boxes. Only one language can be selected at a time and the RMX Manager application must be restarted after changing the display language.

To select a language:

1 On the RMX Manager menu, click Setup > Customize Display Settings > Multilingual Settings.

   The Multilingual Settings dialog box opens, displaying the current language selection.

   ![Multilingual Settings](image)

2 Click the check box of the required language. Only one language can be selected.

3 Click OK.

4 Restart the RMX Manager application to implement the language change.
Import/Export RMX Manager Configuration

The RMX Manager configuration that includes the MCU list and the multilingual selection can be save to any workstation/PC on the network and imported to any Multi-RMX Manager installed in the network. This enables the creation of the MCUs list once and distributing it to all RMX Manager installations on the network.

In addition, when upgrading to a previous version, the MCU list is deleted, and can be imported after upgrade.

The exported file is save in XML format and can be edited in any text editor that can open XML files.

To Export the RMX Manager Configuration:

1. In the Multi-RMX Manager, click the Export RMX Manager Configuration button in the toolbar, or right-click anywhere in the MCUs pane and then click Export RMX Manager Configuration.

The Export RMX Manager Configuration dialog box opens.

2. Click the Browse button to select the location of the save file, or enter the required path in the Export Path box.

The selected file path is displayed in the Export Path box.

3. Click OK to export the RMX Manager configuration.

To Import the RMX Manager Configuration:

1. In the Multi-RMX Manager, click the Import RMX Manager Configuration button in the toolbar, or right-click anywhere in the MCUs pane and then click Import RMX Manager Configuration.

The Import RMX Manager Configuration dialog box opens.

Are you sure you want to merge the two MCU lists?

OK  Cancel
2 Click the **Browse** button to select the saved file, or enter the required path in the Export Path box. The Open dialog box is displayed.

3 Select the XML file previously saved, and click the **Open** button. The selected file path is displayed in the Import Path box.

4 Click **OK** to import the file.
Deploying a Polycom RMX™ Serial Gateway S4GW

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

Network Infrastructure

Network infrastructure with direct connection to Serial Gateway S4GW

After initial setup, the Serial Gateway is configured, managed and monitored via the 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 systems.
- A 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.
- For all RMX platforms:
  - The following System Flags must be set to YES:
    - ULTRA_SECURE_MODE
    - V35_ULTRA_SECURED_SUPPORT
- In addition, for RMX 2000, when connecting a Serial Gateway:
  - It is essential that an RTM LAN card is installed.
  - The Serial Gateway must be physically connected to a RTM LAN card, LAN 1 port.
  - The SEPARATE_MANAGEMENT_NETWORK System Flag must be set to YES.
  - The RMX2000_RTM_LAN System Flag must be set to YES.
- Beginning with Version 7.5.2.J, a Serial Gateway can be connected directly to any available RTM-LAN port on the RMX that is associated with a Network Service.
- 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 RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments, Serial Gateway S4GW - Maximum Security Mode.
- H.323 connections to the RMX are 1024-bit encrypted TLS.
- RTP traffic between the RMX and the Serial Gateway are not encrypted.
- If the certificates installed on the Serial Gateway and the RMX are signed by the same Certificate Authority, that Certificate Authority must be trusted. If the certificate installed on the Serial Gateway was issued by a different Certificate Authority to the one that issued the RMX certificate, the Certificate Authority trust that signed the Serial Gateway certificate must be added to the Trusted Certificate Repository on the workstation.
- An RTM LAN card must be installed in the RMX2000 or RMX4000 if an RMX Serial Gateway S4GW is to be directly connected to the RMX.

Configuring the RMX - Serial Gateway Connection

To configuring the connection between the Serial Gateway and the RMX:

1. Initial Setup of the Serial Gateway:
   - Initial Setup must be completed for each of the Serial Gateways to be deployed.
   - 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 each of the Serial Gateways and Connect the Serial Gateways to the RMX.
Procedure 1: Initial Setup of the Serial Gateway

The IP Addresses on the RMX that match those described in this procedure are described in Procedure 2: Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX.

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 > Settings > IP Connectivity > Peer List**, enter the Signaling Host IP Address (Signaling and Media). The RMX will use this IP address to connect to the Serial Gateway's management interface.

Remove all other addresses from the Peer list. Each Serial Gateway uses the address of the LAN port on the RTM-LAN card that is assigned to its Network Service.

3. In the **Device > Addressing > IP Address** Dialog Box:
   - In the **Router IP** field, enter the Default Router IP Address.
   - In the **Subnet Mask** field, enter the Subnet Mask address.
4 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 and until the cable is disconnected and reconnect to the RMX.)

5 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.

6 Select the Security tab.

7 Set the Security Mode to Maximum.

8 Select the Users tab.

9 Create the user account that the RMX will use to connect to the Serial Gateway.
10 Click the Delimiters tab.
   a Set the delimiter to #.
11 Click the Media Modes tab.
   a Un-check **Enable H.263+.**
   b Un-check **Enable T.120.**
12 Click the Security tab.
   a Select Independent.
13 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 ...Un-selected.
       - Duplicate DTMF signal ... Selected.
   ♦  IP Options:
       - Enable packet handling... Selected.
       - Network jitter tolerance... 120 msec.
   ♦  General:
       - Restrict Gateway to use ... Un-selected.
       - Support H.239 Selected.

14  Click the Commands button.
   a  Enter the Advanced Commands as set out in Maximum Security - Advanced Command Settings.
   b  Set command embeddedMode to Enable
c Set command IsdnCapsTimeout to 15

d Set command h239OlcPatch to Enable

15 For each port in use un-check IVR.

16 In the HTTPS section of the Administrator > Device > Web dialog box:

a Use the buttons to install a TLS Certificate.

b Select the Support Secure Communications (HTTPS) check box.


17 Save the changes to the Serial Gateway configuration.

The Serial Gateway will re-start.

18 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**
- **SEPERATE_MANAGEMENT_NETWORK = YES** (RMX 2000 only)
- **V35_ULTRA_SECURED_SUPPORT = YES**
- **ENABLE_EPC = NO** (If this System Flag doesn’t exist it must be created)

3. Re-start the RMX.

4. For versions prior to Version 7.5.2.J, connect the LAN cable from the front of the Serial Gateway to the **LAN 1** port on the **RTM LAN** card.
   If Version 7.5.2.J is being used, connect the Serial Gateway to any available RTM-LAN port on the RMX that is associated with a Network Service.

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.

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. (This address was configured in Step 3 of Procedure 2: Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX.)

10 Click the V35 Gateway tab.

The network service Properties dialog box is displayed. The Enable field is selected and cannot be un-checked.
Modify the following fields:

**Network Service - V35 Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V35 Gateway IP Address</td>
<td>Enter the Management IP address of the management interface of the Serial Gateway.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the User Name that the RMX uses to log in to the management interface of the Serial Gateway.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Password that the RMX uses to log in to management interface of the Serial Gateway.</td>
</tr>
</tbody>
</table>

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.

**Management of Serial Gateways**

After initial setup, if necessary, Serial Gateways can be further configured, managed and monitored using the RMX Manager. Clicking the **Launch V35 GateWay Site** button in the **Network Properties - V35 Gateway** dialog box opens the **Serial Gateway's Administrator** console.
For more information see Setting Up Your Polycom RMX Serial Gateway S4GW in the RMX Serial Gateway S4GW System User Guide.

The administrator may also use the following URL for administration of the RMX Serial Gateway:

URL: https://[rmx FQDN]/admin/gw/login.asp

For users deploying a RMX Serial Gateway S4GW, the VIEW_RVGW_ACTIVEX System Flag can be added and its value modified to determine if ActiveX controls are used to display the RMX Serial Gateway S4GW web site. If the flag value is set to NO (default) an external Internet Explorer browser is launched to display the RMX Serial Gateway S4GW web site.

For more information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide, ActiveX Bypass.
Testing

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 password can be included in the dial string by adding #<password> at the end of the dial string.
- The password can be entered via DTMF from the endpoint (HDX) if including it in the dial string would create a security concern.

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: For a 384kbps call:
Serial Gateway S4GW - Maximum Security Mode

In Ultra Secure Mode, it is required that the S4GW Serial Gateway operates in Maximum Security Mode.

To enable Maximum Security Mode:

1. Login to the Gateway as an administrator:
   a. In your browser type the URL of the Gateway.
      If HTTPS is enabled, a Security Alert screen is displays.
   b. Click Yes to proceed and display the Administrator login screen. Click No to cancel the current operation.
   c. Type a user name and password.
   d. Click Login.

2. Enable 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)

3. Verify the Advanced Settings for Maximum Security Mode:
   a. In the Gateway interface, 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 the table below, and observe the returned Status Messages.
      If necessary, modify the settings to match those listed in the table.
      For more information see Advanced Commands.

Maximum Security - Advanced Command Settings

<table>
<thead>
<tr>
<th>Advanced Command</th>
<th>Status Message</th>
<th>Status After Setting/Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>advancedsecuritymode</td>
<td>Advanced Security Mode is currently DISABLED</td>
<td>Advanced Security mode - ENABLED</td>
</tr>
<tr>
<td>embeddedMode</td>
<td>ENABLED</td>
<td></td>
</tr>
<tr>
<td>daysForPassword ExpireNotification</td>
<td>Number of days till password expiration is set to 7</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>h239OlcPatch</td>
<td>ENABLED</td>
<td></td>
</tr>
<tr>
<td>IsdnCapsTimeout</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>lowerCaseMinimum</td>
<td>Minimum lower case chars in password is set to 2</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>MinNumberOfChangedChars</td>
<td>Minimum number of changed chars in password is set to 4</td>
<td>NO CHANGE NEEDED</td>
</tr>
</tbody>
</table>
Log out.

4 Request a Web SSL certificate:
   a Click Device >> Web Tab> Manage Certificate.
   b Select the Manage Certificate button and follow the prompts to request the certificate.

5 Install the Web SSL certificate:
   a Click Device > Web Tab > Manage Certificate.
   b Select the Manage Certificate button
   c Select Process Pending Request

### Maximum Security - Advanced Command Settings

<table>
<thead>
<tr>
<th>Advanced Command</th>
<th>Status Message</th>
<th>Status After Setting/Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>NumberOfRepeatCharsAllowed</td>
<td>Number of repeated chars in password is set to 2</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>numericalCharsMinimum</td>
<td>Minimum numerical chars in password is set to 2</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>passwordChangeMinimumTime</td>
<td>Minimum time between password changes is 1</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>passwordReuseBuffSize</td>
<td>The size of the re-usebuffer is 10</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>SpecialCharsMinimum</td>
<td>Minimum special chars in password is set to 2</td>
<td>NO CHANGE NEEDED</td>
</tr>
<tr>
<td>upperCaseMinimum</td>
<td>Minimum upper case chars in password is set to 2</td>
<td>NO CHANGE NEEDED</td>
</tr>
</tbody>
</table>
### Advanced Commands

Below, is the Advance Commands table.

#### Advanced Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdvancedSecurity Mode</td>
<td>ENABLE</td>
<td>This command puts the Gateway in MAXIMUM security mode. Used by: CS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>SessionInactivity</td>
<td>5-60 minutes</td>
<td>Sets the Inactivity timeout value. Web will disconnect from GW if user is inactive for this period of time.</td>
<td>10 minutes</td>
</tr>
<tr>
<td>EnabledTimeout</td>
<td></td>
<td>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</td>
<td>1 day</td>
</tr>
<tr>
<td>passwordChange Minimum</td>
<td>1-30 days</td>
<td>Sets the minimum number of days needed to change when setting new password.</td>
<td></td>
</tr>
<tr>
<td>passwordMinimumTime</td>
<td></td>
<td>Sets the minimum number of days needed to change when setting new password.</td>
<td></td>
</tr>
<tr>
<td>minimum PasswordLength</td>
<td>8-15</td>
<td>Sets the minimum length of a valid password</td>
<td>15</td>
</tr>
<tr>
<td>upperCase Minimum</td>
<td>1-2</td>
<td>Sets the minimum number of upper case characters needed for a valid password.</td>
<td>2</td>
</tr>
<tr>
<td>lowerCase Minimum</td>
<td>1-2</td>
<td>Sets the minimum number of lower case characters needed for a valid password.</td>
<td>2</td>
</tr>
<tr>
<td>NumericalChars Minimum</td>
<td>1-2</td>
<td>Sets the minimum number of numerical characters needed for a valid password.</td>
<td>2</td>
</tr>
<tr>
<td>SpecialChars Minimum</td>
<td>1-2</td>
<td>Sets the minimum number of special characters needed for a valid password.</td>
<td>2</td>
</tr>
<tr>
<td>NumberOfRepeatCharsAllowed</td>
<td>1-4</td>
<td>Sets the number of repeated characters allowed in valid password.</td>
<td>2</td>
</tr>
<tr>
<td>MinNumberOfChangedChars</td>
<td>1-4</td>
<td>Sets the minimum number of characters needed to change when setting new password.</td>
<td>4</td>
</tr>
<tr>
<td>daysForPasswordExpireNotification</td>
<td>1-7</td>
<td>Sets the number of days before password expires that a ‘password expiration notice’ will be shown to user.</td>
<td>7</td>
</tr>
<tr>
<td>passwordReuse BuffSize</td>
<td>8-16</td>
<td>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.</td>
<td>10</td>
</tr>
</tbody>
</table>
### Advanced Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>userLockedOut Duration</td>
<td>0-480 minutes</td>
<td>Sets the number of minutes before user that was locked out will be automatically released. Value of 0 – means indefinite.</td>
<td>0</td>
</tr>
<tr>
<td>userSessionLimit</td>
<td>1-10 sessions</td>
<td>Sets the number of simultaneous sessions per user allowed.</td>
<td>5</td>
</tr>
<tr>
<td>auditLog Threshold</td>
<td>10 -100 percent of log capacity</td>
<td>Sets the audit log threshold, so that when this value is reached an audit log overflow trap is sent.</td>
<td>70</td>
</tr>
<tr>
<td>Password ExpirationTimeout</td>
<td>30-180 days</td>
<td>Sets the number of days till password will expire.</td>
<td>60</td>
</tr>
<tr>
<td>UserLockout FailuresInterval</td>
<td>60-1440 minutes. (1440 = 24 hours)</td>
<td>Period of time in which the failed login threshold must be exceeded the lock the users account.</td>
<td>60</td>
</tr>
<tr>
<td>UserLockoutMax Failure</td>
<td>2-10</td>
<td>Sets the number of login failures needed to lockout user. Failed login threshold.</td>
<td>3</td>
</tr>
</tbody>
</table>
Restoring the RMX Using the USB Port

Do not insert a USB device into the RMX’s USB port unless it is your intention to disable Secured Mode or perform a Comprehensive Restore to Factory Defaults.

Restoring the RMX Using the USB Port can be used to set the RMX back to its factory default settings, if for any combination of factors the system becomes unstable or unmanageable.

There are also administrative operations that cannot be performed on a secured or ultra secured system that require the RMX to be set back to its default (normal) security mode.

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

When performing operations using a USB device, 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.
Recovery Operations Performed Using a USB Device

The RMX has two recovery options:

- **Comprehensive Restore to Factory Defaults**
  Inserting a USB key with the following two text files will restore the RMX to factory defaults:
  - RestoreToFactoryDefault.txt
  - lan.cfg

  Do not insert a USB key containing a file named RestoreToFactoryDefault.txt if the USB key does not also contain a lan.cfg file.

- **Emergency CRL (Certificate Revocation List) Update**
  Inserting a USB key or USB mouse and restarting the RMX will:
  - Change the RMX from HTTPS mode to HTTP mode.
Disabling PKI Client Validation so that the RMX’s configuration or CRLs (or both) can be updated.

**Comprehensive Restore to Factory Defaults**

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

The Comprehensive Restore to Factory Defaults deletes the following files:

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

In addition all the conferencing entities are deleted:

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

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

**Procedure Summary for Performing a Comprehensive Restore to Factory Defaults:**

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

Restoring the RMX to Factory Defaults consists of the following steps:

- **Step 1:** Backup Configuration Files. These files will be used to restore the system in Step 10.
- **Step 2:** Configure a workstation for Direct Connection.
- **Step 3:** Connect to the RMX and the workstation using a LAN cable.
- **Step 4:** Into the RMX’s USB port, insert a USB key containing a file named `RestoreToFactoryDefault.txt` and also containing a `lan.cfg` file.
Do not insert a USB key containing a file named RestoreToFactoryDefault.txt if the USB key does not also contain a lan.cfg file.

Step 5: Restart the RMX.
Step 6: If you are not using an RMX4000 continue with Step 9.
Step 7: Into the RMX’s USB port, insert a USB key containing a file named lan.cfg file only.
Step 8: Restart the RMX.
Step 9: From the workstation, connect to the RMX’s Alternate Management Network.
Step 10: Apply the Product Activation Key.
Step 11: Unplug the USB key.
Step 12: Restart the RMX.
Step 13: Restore the System Configuration from the backup by applying the backup files created in procedure Step 1.
Step 14: Restart the RMX. (If the RMX is unresponsive after these procedures a further restart may be necessary.)
Step 15: Enable Secured Communication and re-apply the Certification procedures as set out in Procedure 6: Enable Secured Communication on page 56.

Detailed Procedure for Performing a Comprehensive Restore to Factory Defaults:

Step 1: 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:

a On the Collaboration Server menu, click Administration > Software Management > Backup Configuration.

The Backup Configuration dialog box opens.

b Browse to the Backup Directory Path and then click Backup.
Step 2: 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 Collaboration Server’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 Properties.

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 the Reserved IP Adresses table that follows should be used for the IP Address.

The addresses needed for connection to the Collaboration Server’s Alternate Management Network are listed in the following table.

**Reserved IP Adresses**

<table>
<thead>
<tr>
<th>Network Entity</th>
<th>Alternate Network IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Unit IP Address</td>
<td>169.254.192.10</td>
</tr>
</tbody>
</table>
g  Click OK.

**Step 3: 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.

<table>
<thead>
<tr>
<th>Network Entity</th>
<th>Alternate Network IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Unit Subnet Mask</td>
<td>255.255.240.0</td>
</tr>
<tr>
<td>Default Router IP Address</td>
<td>169.254.192.1</td>
</tr>
<tr>
<td>Shelf Management IP Address</td>
<td>169.254.192.16</td>
</tr>
<tr>
<td>Shelf Management Subnet Mask</td>
<td>255.255.240.0</td>
</tr>
<tr>
<td>Shelf Management Default Gateway</td>
<td>169.254.192.1</td>
</tr>
</tbody>
</table>

» Connect the cable between the RMX port and the LAN port configured on the workstation.
Step 4: Insert a USB key containing a file named RestoreToFactoryDefault.txt and a lan.cfg file into the USB port of the RMX.

Step 5: Power the RMX Off and then On.

Step 6: If you are not using an RMX 4000 continue with Step 9.

Step 7: Into the RMX’s USB port, insert a USB key containing a file named lan.cfg file only.

Step 8: Restart the RMX.

Step 9: Connect to the Alternate Management Network
   a Start the RMX Manager.
   b In the MCU's list, either modify the current MCU IP address to the Alternate Management Network’s IP address, 169.254.192.10 or add the Alternate Management Network’s IP address as a that of an additional MCU.
   c Login to the RMX.
      The Username / Password dialog box is displayed.

   d Enter the default Username (POLYCOM) and Password (POLYCOM) and click OK.

Step 10: Apply the Product Activation Key.
   The Product Activation dialog box is displayed 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.
   The system prompts with a restart dialog box:

Step 11: Unplug the USB device.
   »  Remove the USB device from the USB port of the RMX.

Step 12: Restart the RMX.
   »  In the restart dialog box, click Yes.

Step 13: Restore the System Configuration From the Backup.

To restore configuration files:
   a  On the RMX menu, click Administration > Software Management > Restore Configuration.
   b  Browse to the Restore Directory Path where the backed up configuration files are stored.
   c  Click Restore.
   d  When the Restore is complete, restart the RMX (Step 14).
      RMX system settings, with the exception of User data, are restored.
   e  Restore User data by repeating step a to step d of this procedure.

Step 14: Restart the RMX.

Step 15: Enable Secured Communication and re-apply the Certification procedure.
   This is described in Procedure 6: Enable Secured Communication.

Emergency CRL (Certificate Revocation List) Update

If CRLs are used, 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 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.

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.

To perform an Emergency CRL Update procedure:

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

![Warning]

The RMX supports the use of PEM and DER formats.

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

**Step 2: Disable Secure Communications mode**

- a  Connect a USB keyboard or mouse to the USB port of RMX.
  The USB port locations for RMX 1500/2000/4000 are shown in There are also administrative operations that cannot be performed on a secured or ultra secured system that require the RMX to be set back to its default (normal) security mode. on page 161.
  - 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 Browse 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 Reset.
   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 IP Network Services. (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.
Troubleshooting

Collaboration Server Web Client Installation - Troubleshooting Instructions

Use of the RMX Web Client is not recommended in Maximum Security Environments. Management using the RMX Manager is the recommended method.

If a Browser Environment Error occurs, close all the Internet Explorer sessions and reconnect to the MCU. If the problem persists, you can run the Automatic Troubleshooting Utility or perform the Troubleshooting Procedures manually.

The Manual Troubleshooting Procedures include several procedures that can be performed in order to solve the connection error. At the end of each procedure, check if you can connect to the MCU and if the problem persists, perform the next procedure.

In Secured Mode (https://), the DNS name specified in the RMX’s Certificate must correspond with that of the DNS Server used by the Client that is connecting to the RMX.
The following troubleshooting procedures can be performed manually:

- Procedure 1: Ending all Internet Explorer Sessions
- Procedure 2: Deleting the Temporary Internet Files, Collaboration Server Cookie and Collaboration Server Object
- Procedure 3: Managing Add-ons Collisions
- Procedure 4: Add the Collaboration Server to the Internet Explorer Trusted Sites List
- Procedure 5: Browser Hosting Controls (Optional)

**Procedure 1: Ending all Internet Explorer Sessions**

In some cases, although all the Internet Explorer sessions were closed, the system did not end one or several IE processes. These processes must be ended manually.

**To end all Internet Explorer sessions:**

Start the Task Manager and click the Processes tab.

1. Select an `iexplore` process and click the **End Process** button.

2. Repeat this process for all `iexplore` processes that are currently active.

3. Close the **Windows Task Manager** dialog box.

4. Open the Internet Explorer and connect to the MCU.
5 If the problem persists, continue with Procedure 2.

Procedure 2: Deleting the Temporary Internet Files, RMX Cookie and RMX Object

If at the end of Procedure 1 the error message is still displayed, and you cannot connect to the MCU, perform the following operations:

- Delete the Temporary Internet files
- Delete the RMX/Collaboration Server Cookie
- Delete the RMX/ActiveX Object

Deleting the Temporary Internet Files

To delete the Temporary files:

1. In the Internet Explorer, click Tools > Internet Options. The Internet Options dialog box opens.
2. In the Browsing history pane, click the Delete button.

![Internet Options dialog box](image)

The Delete Browsing History dialog box opens.
3 It is recommended to delete only the **Temporary Internet files**. By default, the **Cookies** option is also selected. Clear it if you do not want to clear the cookies from your computer.

![Internet Options dialog box]

4 Click the **Delete** button.

5 When the process is complete, the system return to the **Internet Options** dialog box.
Deleting the RMX/Collaboration Server Cookie

To delete the RMX Cookie:

1. In the Internet Options dialog box - Browsing History pane, click the Settings button.

The Temporary Internet Files and History Settings dialog box is displayed.
2 Click the **View files** button.

The Windows Explorer screen opens, listing **Windows Temporary Internet Files**.

3 Browse to the RMX/ RMX cookie. The cookie is listed in the format: **cookie:user name@RMX/RMX IP address**. For example: cookie:valerie@172.22.189.110.

4 Right-click the RMX cookie and click **Delete**.

The system prompts for confirmation.

5 Click **Yes**.

The cookie is deleted.

6 Close the Windows Explorer screen.
Deleting the RMX/Collaboration Server ActiveX Object

To delete the RMX/RMX ActiveX Object:

1. In the Temporary Internet Files and History Settings dialog box, click the View objects button.

   ![Temporary Internet Files and History Settings](image)

   The Windows Explorer screen opens, listing the Windows Downloaded Program Files.

2. Right-click the EMA.ClassLoader.dll and then click Delete.

   ![Windows Explorer](image)

   The system prompts for confirmation.

3. Click Yes.

   The RMX object is deleted.
4 Close the Windows Explorer screen.
5 In the **Temporary Internet Files and History Settings** dialog box, click **OK**.
6 In the **Internet Options** dialog box, click **OK** to close it.
7 Close the Internet Explorer session and reopen it.
8 Connect to the RMX.

If the problem persists, continue with Procedure 3.

**Procedure 3: Managing Add-ons Collisions**

In some cases, previously installed add-ons, such as anti virus programs can create collisions between applications and prevent the installation of a new add on. Disabling these add-ons may be required in order to install the RMX Web Client.

**To disable an add-on:**

1 In the Internet Explorer, click **Tools > Manage Add-ons**. The **Manage Add-ons - Toolbars and Extensions** dialog box opens.
2 Scroll to the add-on to disable (for example, the anti virus add-on), right-click it and then click **Disable**.
   Alternatively, select the add-on and click the **Disable** button.

3 Click the **Close** button to close this dialog box.
4 Connect to the RMX.

If the problem persists, continue with the Procedure 4.

**Procedure 4: Add the Collaboration Server to the Internet Explorer Trusted Sites List**

In some cases, local security settings may prevent Internet Explorer from accessing the RMX.

**To add the RMX to the Internet Explorer Trusted Sites list:**

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

2. Click the **Trusted Sites** tab.

3. Click the Sites button.

The **Trusted sites** dialog is displayed.

4. If the Collaboration Server is using Secure Mode:
   - a. In the **Add this website to the zone**: field, enter, **“https://”** followed by the IP address or the DNS name of the Collaboration Server.
   - b. Click the **Add** button.
   - c. Click the **Close** button.

5. If the Collaboration Server is using Standard Security Mode:
   - a. In the **Add this website to the zone**: field, enter, **“https://”** followed by the IP address or the DNS name of the Collaboration Server.
   - b. Click the **Add** button.
c Clear the Require server verification (https:) for all sites in this zone checkbox.
d Click the Close button.

Procedure 5: Browser Hosting Controls (Optional)

If the Collaboration Server Web Client does not load and run after Procedures 1-4 have been performed, the reason may be that .NET Framework 4 or higher is running on the workstation with Managed Browser Hosting Controls disabled.

Managed Browser Hosting Controls is an Internet Explorer operating mode required by the Collaboration Server Web Client. By default, .NET Framework 4 and higher are not enabled to support Managed Browser Hosting Controls.

Perform Procedure 5 to:

- Determine whether .NET Framework 4 or higher is running on the workstation.
- Determine whether a 32-bit or 64-bit version of Windows is running on the workstation.
- Enable Managed Browser Hosting Controls if .NET Framework 4 or higher is running on the workstation.

To enable Managed Browser Hosting Controls:

1 Determine whether .NET Framework 4 or higher is running on the workstation.
   a On the Windows Desktop, click Start.
   b In the Start Menu, click Control Panel.
   c In the Control Panel, click Programs and Features.
   d Inspect the Programs and Features list for the version of Microsoft .NET Framework Client Profile that is installed.
2 Determine whether a 32-bit or 64-bit version of Windows is running on the workstation:
   a On the Windows Desktop, click Start.
   b In the Start Menu, click Computer.
   c In the Computer Menu, System properties and inspect the value of the System type field in the System section
3 Enable Managed Browser Hosting Controls if .NET Framework 4 or higher is running on the workstation.
   a Open the Registry.
   b Navigate to the Subkey:
      ◆ 32-bit System: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\.NETFramework
      ◆ 64-bit System: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
   c Add the Dword Value: EnableIEHosting
   d Set value of EnableIEHosting to 1.
   e Close the Registry.
   f Close and re-open Internet Explorer.