



## **Configuration Guide for Cisco Unified Videoconferencing Manager Release 5.6**

October 2008

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-16910-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Configuration Guide for Cisco Unified Videoconferencing Manager Release 5.6*  
© 2008 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## PART 1

### Resource Manager

---

#### CHAPTER 1

#### **Managing Network Topologies in Resource Manager 1-1**

- How to Create a Network Topology with Device Islands 1-1
  - Adding a Device Island 1-2
  - Modifying Device Island Settings 1-3
  - Removing Connectivity Between Device Islands 1-3
  - Removing a Device Island 1-3
- Viewing IP and ISDN Network Topologies 1-3
- Modifying Your Network Topology View 1-4

---

#### CHAPTER 2

#### **Configuring a Gatekeeper Profile in Resource Manager 2-1**

- Selecting a Gatekeeper Type 2-1
  - Cisco IOS H.323 Gatekeepers 2-1
  - External Gatekeepers 2-1
- How to Create or Modify a Gatekeeper Profile 2-2
  - Defining Gatekeeper Address Details 2-2
  - Defining Dialing Plan Settings 2-2
  - Defining Resource Manager as the Gatekeeper Authorization Server 2-3
- Removing a Gatekeeper Profile 2-3
- Searching for a Gatekeeper Profile 2-4
- Accessing Meetings from an External Gatekeeper 2-4

---

#### CHAPTER 3

#### **Configuring a SIP Server Profile in Resource Manager 3-1**

- Creating or Modifying a SIP Server Profile 3-1
- Removing a SIP Server Profile 3-2
- Searching for a SIP Server Profile 3-2
- Configuring the MCU to Work in SIP Mode 3-3
- Disabling the SIP Back-to-Back User Agent 3-3

---

#### CHAPTER 4

#### **Managing an MCU Profile in Resource Manager 4-1**

- Configuring Cascading 4-1
- Creating or Modifying an MCU Profile 4-2

- Taking an MCU Offline 4-3
- Removing an MCU Profile 4-4
- Searching for an MCU Profile 4-4
- Synchronizing MCU Information with Cisco Unified Videoconferencing Manager 4-4
- How to Manage Meeting Types 4-5
  - Viewing Available Meeting Types on Network MCUs 4-5
  - Viewing Built-in Meeting Types 4-6
  - Removing a Meeting Type 4-7
  - Searching for a Meeting Type 4-7
  - Downloading a Meeting Type to Resource Manager 4-7
  - Resolving Meeting Type Conflicts Between MCUs 4-8
  - Resolving Meeting Type Conflicts Between Resource Manager and an MCU 4-8
  - Uploading a Meeting Type to Network MCUs 4-9
  - Viewing Meeting Type Details 4-9
  - Modifying Meeting Type Details 4-9
  - Accessing an MCU from the Meeting Type Details Screen 4-10
  - Viewing a List of MCUs Containing a Specified Meeting Type 4-10
- Limiting User Access to Meeting Types 4-10
- Customizing MCU Delimiters 4-11
- Designating a Service for IVR Use 4-11
- Defining Video IVR Services 4-12

**CHAPTER 5**

**Configuring a Gateway Profile in Resource Manager 5-1**

- Creating or Modifying a Gateway Profile 5-1
- Taking a Gateway Offline 5-3
- Removing a Gateway Profile 5-4
- Searching for a Gateway Profile 5-4

**CHAPTER 6**

**Configuring a Cisco Unified Videoconferencing Desktop Server Profile in Resource Manager 6-1**

- Creating or Modifying a Desktop Server Profile 6-1
- Removing a Desktop Server Profile 6-2
- Searching for a Desktop Server Profile 6-2
- How to Stream Meetings Using Desktop Server 6-2
  - Enabling Streaming on Cisco Unified Videoconferencing Desktop Server 6-3
  - Enabling Streaming for a Virtual Room 6-3
  - Allowing Recording by Specified Roles 6-3
  - Allowing Recording by Specified Users 6-3
  - Enabling Recording for Specified Virtual Rooms 6-4

**CHAPTER 7****Configuring a Meeting Room Profile in Resource Manager 7-1**

- Enabling Meeting Room Support 7-1
- Creating or Modifying a Meeting Room Profile 7-1
- Sending Meeting Details by E-mail 7-2
- Removing a Meeting Room Profile 7-2
- Searching for a Meeting Room Profile 7-3

**CHAPTER 8****Configuring a Terminal Profile in Resource Manager 8-1**

- How to Create or Modify a Terminal Profile 8-1
  - Defining H.323 IP Terminal Details 8-2
  - Defining SIP IP Terminal Details 8-2
  - Defining ISDN/PSTN H.320 Terminal Details 8-3
  - Defining Mobile Terminal Details 8-4
  - Defining Dual H.320 and H.323 Terminal Details 8-4
- Removing a Terminal Profile 8-5
- Searching for a Terminal Profile 8-5

**CHAPTER 9****Defining Resource Manager Call Routing Modes 9-1**

- Call Routing in H.323 Deployments 9-1
- Call Routing in SIP Deployments 9-2
- Masking Conference Topology with the Virtual MCU Feature 9-2
  - Creating a Centralized Conference 9-2
  - Creating a Distributed Conference 9-2

**CHAPTER 10****Managing Resource Manager Users and User Groups without an External Directory 10-1**

- Creating or Modifying a User Profile 10-1
- Removing a User Profile 10-2
- Searching for a User Profile 10-2
- Updating User Profiles 10-3
- Creating a User Group 10-3
- Modifying a User Group 10-4
- Removing a User Group 10-4

**CHAPTER 11****Provisioning Resource Manager Users via a Directory Server 11-1**

- Synchronization of User Information 11-1
- Synchronizing Resource Manager with Active Directory Server 11-2
- Configuring a Connection to an LDAP Server 11-3

Mapping Resource Manager User Roles to ADS Users 11-4  
 Defining Virtual Rooms for All LDAP Users 11-5  
 Forcing Resource Manager to Use a Virtual Room 11-5  
 Resource Manager LDAP Information Attributes 11-6

**CHAPTER 12**

**Viewing Meeting Schedules in Resource Manager 12-1**

Viewing Organization Meetings 12-1  
 Viewing the Creation Status of Meetings 12-2  
 Viewing the Termination Status of Meetings 12-2  
 Searching for a Meeting 12-3  
 Monitoring a Meeting 12-3  
 Generating Reports 12-4  
 Modifying Upcoming Meetings 12-5  
 Removing Meetings from the History Tab 12-5  
 Viewing Host MCUs 12-6  
 Terminating Meetings 12-6

**CHAPTER 13**

**Modifying Default Organization Settings for Resource Manager Users and Meetings 13-1**

About Settings Priorities 13-1  
 How to Define Default Settings for Organization Users 13-1  
     Defining Which Meeting Types are Available to New Users 13-1  
     Defining a Default Time Zone for a User 13-2  
     Defining Display Formats 13-2  
     Defining Date Display Formats 13-3  
     Defining Your Meeting Display Preferences 13-3  
 How to Define Default Settings for Meetings 13-3  
     Defining a Default Meeting Type 13-4  
     Defining the Default Cascading Mode 13-4  
     Defining How to End a Meeting 13-4  
     Defining the Meeting Default Length 13-5  
     Defining the Default Dialing Mode 13-5  
     Defining a Billing Destination 13-5  
     Defining Required Default Resources 13-6  
     Customizing Invitation E-mail 13-6  
 Modifying the Look and Feel of the Resource Manager Web User Interface 13-7

**CHAPTER 14**

<b>Using the Resource Manager Configuration Tool</b>	<b>14-1</b>
Setting Up the Java Runtime Environment	14-2
Launching the Configuration Tool	14-2
Retrieving an Administrator Password	14-3
Uninstalling the Resource Manager Configuration Tool	14-3
How to Modify General Settings	14-3
Defining E-Mail Server Settings	14-4
Defining the Unconnected Endpoint Timeout Period	14-4
Defining Table Row Display	14-5
Defining the Command Delay	14-5
Defining the Parent Zone Authorization Filter	14-5
Defining the Log Level	14-6
Defining the In-Meeting Control Refresh Rate	14-6
Defining the Resource Manager Server Name and Web Port	14-6
Defining the Online Help Host URL	14-7
How to Modify Scheduling Settings	14-7
Changing Call Authorization Settings	14-7
Dynamically Cascading Multiple EMPs for a Single Conference	14-8
Modifying Default Meeting Settings	14-9
Modifying Default Recurring Meeting Settings	14-10
Hiding Resource Manager User Interface Screens	14-10
How to Manage Custom Time Zones	14-11
Selecting a Time Zone Profile	14-11
Viewing a Time Zone Profile	14-11
Adding Daylight Saving to a Time Zone Profile	14-12
Creating a Customized Time Zone Profile	14-12
Removing a Customized Time Zone Profile	14-12
Reverting to Default Time Zone Settings	14-13
Customizing Product and Vendor Logos	14-13
Creating a Customized Billing Field	14-13
Defining Database Server Settings	14-14
How to Define Security Settings	14-14
Defining Password Settings	14-15
Defining a Login Message	14-15
Unlocking a User Account	14-15
How to Define Call Data Record (CDR) Settings	14-16
Creating CDR Information in XML Format	14-16
Defining Required Terminal Connection Duration	14-16

Defining a CDR File Prefix	14-17
Defining How Often CDRs Are Produced	14-17
Enabling Streaming to a Radius Server	14-17

**CHAPTER 15**

**CDR XML Tags and Attributes 15-1**

Accessing the CDR XML Files	15-1
Index of CDR XML Tags	15-1
Understanding the CDR XML Tags	15-7

**CHAPTER 16**

**Enabling Resource Manager to Use Secure Sockets Layer Connections on a JBoss Application Server 16-1**

Component Identity via SSL	16-1
How to Generate Certificates	16-1
Methods for Creating a New Certificate	16-2
Prerequisites	16-2
Using Keytool to Generate a Certificate	16-2
Configuring JBoss to Use SSL	16-4
Accessing Resource Manager via HTTPS	16-5

**PART 2**

**Network Manager**

**CHAPTER 17**

**Viewing Your Network in Network Manager 17-1**

How to View the Network as a Tree	17-1
Configuring Network Hierarchy	17-1
Creating a Custom Network Tree View	17-2
Viewing the Network as a Table	17-3
Viewing the Network as a Map	17-3

**CHAPTER 18**

**Managing Elements in Network Manager 18-1**

Displaying General Element Information	18-2
About the Management Status of Elements	18-2
Viewing all Network Elements	18-3
Creating or Modifying an Element Profile	18-3
Removing an Element Profile	18-4
Searching for an Element Profile	18-5
Defining Default Element Access Settings	18-5
Overriding Default Element Access Settings	18-6

How to Upgrade Element Software	18-6
Adding a Software Upgrade File	18-7
Modifying a Software Upgrade File	18-7
Removing a Software Upgrade File	18-7
Cancelling Pending Offline Configuration Settings	18-8
How to Manage the Element Software Upgrade Upload Log	18-8
Viewing Your Software Upgrade Upload History	18-8
Uploading a File After a Failed Attempt	18-9
Removing Entries from the Upload Log	18-9
How to Automatically Detect New Elements on the Network	18-10
Running the Auto-detect Mechanism Manually	18-10
Running the Auto-detect Mechanism Automatically	18-10
Adding or Modifying Auto-detect Element Access Information	18-11
Removing an Element Type from the Auto-detect Mechanism	18-11
Accessing an Element Web User Interface	18-12
Accessing the Monitor Tab for a Specified Element	18-12

**CHAPTER 19**

<b>Managing Endpoints in Network Manager</b>	<b>19-1</b>
Defining Default Endpoint Access Settings	19-1
How to Override Default Endpoint Settings	19-2
Overriding Default Endpoint Addressing	19-2
Overriding Default Access Settings for a Selected Endpoint	19-3
Configuring Endpoint Dialing	19-3
Retrieving Configuration Parameters	19-4
How to Upgrade Endpoint Software	19-5
Adding a Software Upgrade File	19-5
Modifying a Software Upgrade File	19-6
Removing a Software Upgrade File	19-6
How to Manage Endpoint Configuration Files	19-7
Viewing Saved Endpoint Configuration Files	19-7
Modifying an Endpoint Configuration File	19-8
Removing an Endpoint Configuration File	19-8
Updating Configuration for Selected Endpoints	19-9
Upgrading Software for Selected Endpoints	19-10
Upgrading Sony Endpoints	19-10
How to Manage the Endpoint Upload Log	19-11
Viewing Your Endpoint Configuration Upload History	19-11
Uploading a File After a Failed Attempt	19-12

Removing Entries from the Upload Log 19-12

**CHAPTER 20**

**Managing the Internal Gatekeeper in Network Manager 20-1**

- How to Manage Services 20-1
  - Viewing Internal Gatekeeper Supported Services 20-1
  - Creating or Modifying a Service 20-2
  - Viewing Global Services 20-3
  - Creating or Modifying a Global Service 20-3
  - Removing a Service 20-4
- How to Manage Prefixes 20-4
  - Creating or Modifying a Prefix 20-4
  - Removing a Prefix 20-5
- How to Configure a Parent Gatekeeper 20-5
  - Enabling the Parent Tab 20-5
  - Adding a Parent Manually 20-6
  - Adding a Parent Automatically 20-6
- How to Manage Parent Filters 20-6
  - Creating or Modifying a Parent Filter 20-6
  - Removing a Parent Filter 20-7
- How to Configure a Child Gatekeeper 20-7
  - Enabling the Children Tab 20-7
  - Viewing Child Gatekeepers 20-8
  - Adding a Child Manually 20-8
  - Adding a Child Automatically 20-9
- How to Manage Child Prefixes 20-9
  - Creating or Modifying a Child Prefix 20-9
  - Removing a Child Prefix 20-9
- How to Configure a Neighbor 20-10
  - Viewing Neighbor Gatekeepers 20-10
  - Adding or Modifying a Neighbor Gatekeeper 20-11
- How to Manage Zones 20-11
  - Creating or Modifying a Local Zone 20-11
  - Creating or Modifying a Remote Zone 20-12
  - Removing a Zone 20-12
- How to Manage Bandwidth Rules 20-12
  - Viewing Bandwidth Rules 20-13
  - Creating or Modifying a Bandwidth Rule 20-13
  - Removing a Bandwidth Rule 20-14

	How to Manage Debug Flags	20-14
	Creating or Modifying a Debug Flag	20-14
	Removing a Debug Flag	20-14
<b>CHAPTER 21</b>	<b>Managing an MCU in Network Manager</b>	<b>21-1</b>
	Setting Call Routing Devices	21-1
	Viewing Registered Multipoint Processors	21-1
	How to Manage Multipoint Processors	21-2
	Creating and Modifying an MP Profile	21-2
	Removing an MP Profile	21-3
	Viewing MCU Supported Services	21-3
	Configuring MCU Unit Type and Addressing	21-3
<b>CHAPTER 22</b>	<b>Managing a Gateway in Network Manager</b>	<b>22-1</b>
	How to Manage Services	22-1
	Viewing Gateway Supported Services	22-1
	Creating or Modifying a Service	22-1
	Removing a Service	22-2
	Configuring Gateway Addressing	22-2
<b>CHAPTER 23</b>	<b>Configuring a User Profile in Network Manager</b>	<b>23-1</b>
	Creating or Modifying a User Profile	23-1
	Removing a User Profile	23-2
	How to Define Network Subsets	23-2
	Creating or Modifying a Network Subset	23-2
	Removing a Network Subset	23-3
	Removing an Include or Exclude Criterion	23-4
<b>CHAPTER 24</b>	<b>Managing Traps and Alarms in Network Manager</b>	<b>24-1</b>
	Sending Traps to Network Manager	24-1
	Creating or Modifying a Trap Forwarding Rule	24-2
	Disabling a Trap Forwarding Rule	24-2
	Removing a Trap Forwarding Rule	24-3
	Creating or Modifying an Alert Recipient Profile	24-3
	Removing an Alert Recipient Profile	24-4
	Viewing Generated Events	24-4
	Filtering Generated Events	24-5

Viewing Events per Network Item 24-5

Viewing and Sorting Supported Alarms 24-6

Modifying Alarms 24-6

Viewing and Sorting Generated Alarms 24-6

Viewing Generated Alarms per Network Item 24-7

---

**CHAPTER 25**

**Managing Calls and Conferences in Network Manager 25-1**

Viewing Current Call Details 25-1

Viewing Current Call Details per Network Item 25-2

Disconnecting Calls 25-2

Searching for a Call 25-2

Viewing Current Conferences 25-3

Viewing Current Conferences per Network Item 25-3

Searching for a Conference 25-4

Accessing the Conference MCU 25-4

---

**CHAPTER 26**

**Configuring Logging for Network Manager 26-1**

Viewing Logs for a Selected Element 26-1

Defining Network Manager Logging Activity 26-2

Saving Element Logs 26-2

---

**PART 3**

**Desktop**

---

**CHAPTER 27**

**Cisco Unified Videoconferencing Desktop Features 27-1**

---

**CHAPTER 28**

**Configuring Cisco Unified Videoconferencing Desktop 28-1**

Accessing the Administration Interface 28-1

Viewing Server Status and Port Resource Usage 28-2

How to Configure Cisco Unified Videoconferencing Desktop Server Settings 28-3

    Configuring Settings for Single/Multiple-NIC Deployments 28-3

    Configuring Desktop Server Network Interface 28-3

Configuring Gatekeeper IP Address 28-4

Configuring Client-Related Settings 28-5

How to Configure Meeting Control Settings 28-6

    Configuring Server Type 28-6

    Configuring Cisco Unified Videoconferencing 3500 MCU Server Settings 28-7

    Configuring Cisco Unified Videoconferencing Manager Server Settings 28-7

Defining Security Settings	28-8
Configuring Meeting Features	28-9
How to Configure Streaming Server Settings	28-10
Configuring This Desktop Server to Manage Streaming	28-11
Configuring an Alternate Desktop Server for Watching Webcasts	28-12
How to Configure Recording Server Settings	28-13
Viewing Recording Server Status	28-13
About Configuring the Desktop Recording Server Connection	28-14
Configuring Recording Parameters	28-16
Modifying the Disk Space and Storage Location for Recordings	28-17
Disabling Automatic Recording Feature	28-18
How to Manage Recordings	28-19
Viewing Recording List	28-19
Editing Recording Attributes	28-20
Setting Categories for Multiple Recordings	28-21
Deleting Recordings	28-21
Stopping Recordings in Progress	28-22
Recording Meetings	28-22
Managing Categories	28-23
How to Restore Recordings	28-24
Backing up Recordings	28-24
Restoring Recordings	28-24
How to Brand Desktop User Interface	28-25
Replacing Images	28-25
Modifying Strings	28-26
Saving or Restoring Branding-related Changes	28-27
Restoring Default Images and Strings	28-28
Viewing the Cisco Unified Videoconferencing Desktop Online Help	28-28





## **PART 1**

### **Resource Manager**





# CHAPTER 1

## Managing Network Topologies in Resource Manager

---

This section is for Organization Administrators.

- [How to Create a Network Topology with Device Islands, page 1-1](#)
- [Viewing IP and ISDN Network Topologies, page 1-3](#)
- [Modifying Your Network Topology View, page 1-4](#)

### How to Create a Network Topology with Device Islands

IP network topology is the foundation of intelligent resource allocation. It allows Resource Manager to model the video network by recording distance and bandwidth between device islands (IP locations where central and essential devices such as gatekeepers, MCUs, and gateways are placed) and to perform least-cost or best-performance routing over the IP network. An IP endpoint is also associated with its nearest device island when the endpoint is configured. This information is used by Resource Manager to determine the best gatekeeper, MCU, and gateway resources to reserve and schedule for any call.

ISDN network topology intelligently manages ISDN/PSTN network connectivity and cost, gateway numbers, and PSTN/ISDN endpoint numbers that are assigned to ISDN device islands (similar to IP Network Topology). This allows Resource Manager to perform least-cost routing over the ISDN network according to the topology configuration.

Within the same ISDN device island, PSTN/ISDN least-cost routing is also performed based on country codes, area codes of gateway numbers, and PSTN/ISDN endpoint numbers. Costly telephone or PSTN/ISDN line-usage is reduced by selecting the least costly gateway resources via telephone number.

- [Adding a Device Island, page 1-2](#)
- [Modifying Device Island Settings, page 1-3](#)
- [Removing Connectivity Between Device Islands, page 1-3](#)
- [Removing a Device Island, page 1-3](#)

## Adding a Device Island

In a large distributed deployment, create a device island for each location containing network devices, such as MCUs, gateways, and endpoints. The Resource Manager monitors the bandwidth limitations and distance between each of the device islands.

In a multi-zone deployment where each Cisco IOS H.323 Gatekeeper has its own zone prefix, define a device island for each zone and assign the Cisco IOS H.323 Gatekeeper and the MCU/gateways registered to that Cisco IOS H.323 Gatekeeper to the same device island.

The IP Topology tab displays distance and bandwidth information for all device islands within your video meeting network.

- **Distance**—The distance between the specified device islands relative to all other configured islands on the organization LAN. This setting is used to find and allocate the best available resources. The Distance value is a weight factor (from 1 to 100) that describes relative network delay between two device islands. The larger the distance, the larger the round trip delay caused by the network between two device islands. The distance should be an attribute proportional to the network delay. One logical way to model delay is to “ping” the connection between the two LANs and use the average delay results.
- **Bandwidth**—The bandwidth connection (in Kbps) between specified device islands. This setting is used in bandwidth control during resource allocation. The Bandwidth field represents the connection bandwidth (in Kbps) between any two device islands that can be used for video meetings. This is defined by the narrowest section of bandwidth, usually one of the outgoing connections from the LAN.

The ISDN Topology tab displays distance and cost information for all device islands within your PSTN/ISDN network.

- **Cost**—The cost of a PSTN/ ISDN call between the specified device islands relative to all other configured islands on the organization PSTN/ISDN network. This setting is used to find and allocate best available resources.

### Procedure

---

**Step 1** Click **Network Management** in the sidebar menu.

**Step 2** Click **Add**.

An empty grid containing a single row appears. The row includes all of the existing device islands displayed in columns.

**Step 3** For device islands on an IP network, enter the required distance and bandwidth in each column.

**Step 4** For device islands on an ISDN network, enter the required distance and cost in each column.

**Step 5** Click **OK** to save your changes.

---

## Modifying Device Island Settings

### Procedure

---

- Step 1** Click **Network Management** in the sidebar menu.
  - Step 2** Modify the distance and bandwidth in the appropriate cell.
  - Step 3** Click **OK** to save your changes.
- 

## Removing Connectivity Between Device Islands

### Procedure

---

- Step 1** Click **Network Management** in the sidebar menu.
  - Step 2** Delete the distance and bandwidth values for the required device island pair.
  - Step 3** Click **OK** to save your changes.
- 

## Removing a Device Island

### Procedure

---

- Step 1** Click **Network Management** in the sidebar menu.
  - Step 2** Click the X above the device island that you want to delete.  
The Reassign Device Island window appears if there are network devices currently assigned to this device island.
  - Step 3** Select the device island you want to reassign the devices to, and then click **OK**.
  - Step 4** Click **OK** in the Network Management screen to save your changes.
- 

## Viewing IP and ISDN Network Topologies

The Network Management section is hidden by default.

### Procedure

---

- Step 1** Open the Resource Manager Configuration Tool.
- Step 2** Go to **System Configuration > UI Settings**.

- Step 3** Select the **IP Topology** and **ISDN Topology** fields.
  - Step 4** Click **Network Management** in the sidebar menu of the Resource Manager web user interface.
- 

## Modifying Your Network Topology View

### Procedure

---

- Step 1** Click **Network Management** in the sidebar menu.
  - Step 2** Click **Display Locations**.
  - Step 3** Use the arrows to move the device islands that you want to display from the Available Locations column to the Assigned Locations column.
  - Step 4** Click **Search**.
  - Step 5** The selected device islands appear in the grid display.
-



## CHAPTER 2

# Configuring a Gatekeeper Profile in Resource Manager

---

- [Selecting a Gatekeeper Type, page 2-1](#)
- [How to Create or Modify a Gatekeeper Profile, page 2-2](#)
- [Removing a Gatekeeper Profile, page 2-3](#)
- [Searching for a Gatekeeper Profile, page 2-4](#)
- [Accessing Meetings from an External Gatekeeper, page 2-4](#)

## Selecting a Gatekeeper Type

Cisco Unified Videoconferencing Manager supports the following types of gatekeeper:

- [Cisco IOS H.323 Gatekeepers, page 2-1](#)
- [External Gatekeepers, page 2-1](#)

## Cisco IOS H.323 Gatekeepers

Resource Manager supports the use of Cisco IOS Gatekeepers. In deployments with Cisco IOS Gatekeepers, we recommend that you register Cisco Unified Videoconferencing 3500 MCUs and 3545 Gateways with the Resource Manager internal gatekeeper to preserve the “virtual MCU” features, and that you register endpoints with the Cisco IOS Gatekeepers for scalability. The Resource Manager internal gatekeeper and the Cisco IOS Gatekeeper are then configured as neighbors.

## External Gatekeepers

Resource Manager supports external gatekeepers, such as the RADVISION ECS Gatekeeper. The Resource Manager can only support external gatekeepers if the external gatekeeper is configured as a neighbor to the Cisco Unified Videoconferencing Manager internal gatekeeper or Cisco IOS H.323 Gatekeeper. Only endpoints (terminals) can be registered to an external gatekeeper.

# How to Create or Modify a Gatekeeper Profile

Only an Organization Administrator has permission to configure an H.323 gatekeeper in the system for video conferences using the H.323 protocol.

- [Defining Gatekeeper Address Details, page 2-2](#)
- [Defining Dialing Plan Settings, page 2-2](#)
- [Defining Resource Manager as the Gatekeeper Authorization Server, page 2-3](#)

## Defining Gatekeeper Address Details

### Procedure

- 
- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gatekeeper/SIP server**.
- Step 3** Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
- Step 4** Locate the General section.
- Step 5** Enter the name and IP address of the gatekeeper in the relevant fields.
- Step 6** Select the gatekeeper model.
- If you select **Other** in the Model field, select **H.323** in the Protocol field.
- Step 7** Select the device island to which the gatekeeper belongs from the Location list.
- Each device island can have only one gatekeeper.
- The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 8** Click **OK** to save your changes.
- 

## Defining Dialing Plan Settings

### Procedure

- 
- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gatekeeper/SIP server**.
- Step 3** Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
- Step 4** Locate the Dialing Plan Information section.
- Step 5** (Optional) Select **Hierarchical** if the gatekeeper has a parent-child relationship with its neighbor in the dialing plan, rather than a flat peer relationship.

If you choose Hierarchical, the Parent Gatekeeper list becomes active. From the list choose a parent zone for the gatekeeper. **None** is automatically selected in the list if the gatekeeper is a parent at the top of the hierarchy.

Do not choose Hierarchical for a root gatekeeper. The root gatekeeper in a hierarchical tree structure has no parent but may have peer neighbors.

- Step 6** (Optional) Select **Stripping** for a gatekeeper that is configured to strip (remove) zone prefixes.
  - Step 7** Click **Add Zone Prefix** to add a zone prefix that matches the configuration of the gatekeeper.
  - Step 8** Click **OK** to save your changes.
- 

## Defining Resource Manager as the Gatekeeper Authorization Server

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Gatekeeper/SIP server**.
  - Step 3** Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
  - Step 4** Locate the Advanced section.  
The Advanced section appears if you are using the internal gatekeeper.
  - Step 5** Select **Enable Gatekeeper advanced features (authorization and point-to-point)** to set Resource Manager as the authorization server of the internal gatekeeper.
  - Step 6** You do not need to modify the internal gatekeeper default values for the Port, SNMP Get Community and SNMP Set Community fields.
  - Step 7** Click **OK** to save your changes.
- 

## Removing a Gatekeeper Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gatekeeper/SIP server**.
- Step 3** Click the gatekeeper entry you wish to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.

The gatekeeper profile is deleted from the scheduler and information about the gatekeeper is removed from the database.

---

## Searching for a Gatekeeper Profile

### Procedure

- 
- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gatekeeper/SIP server**.
- Step 3** Enter all or part of the name of the gatekeeper you want to find in the Name field.
- Step 4** Click **Search**.

Search results are listed. If you are using the internal gatekeeper, the following information about connection status is available in the list of search results:

- Authorization Connection indicates whether or not Resource Manager acts as the authorization server for the internal gatekeeper. This connection needs to appear as connected for advanced Resource Manager features such as Virtual MCU and point-to-point call control to function correctly.
- Call Control Connection indicates whether or not a Call Control API connection is established between the gatekeeper and Resource Manager.
- SNMP Connection indicates whether or not the SNMP connection between the Resource Manager and the gatekeeper is established.

- Step 5** To return to the complete list of gatekeepers, clear the Name field, and then click **Search**.
- 

## Accessing Meetings from an External Gatekeeper

If a standalone internal gatekeeper authorized by Resource Manager or an internal gatekeeper is neighbored to an external gatekeeper (for example, a Cisco IOS Gatekeeper), perform the following configuration steps in the internal gatekeeper web user interface to enable dial-in and dial-out to work properly between the internal gatekeeper and the external gatekeeper:

### Procedure

- 
- Step 1** In the external gatekeeper interface, add the Resource Manager internal gatekeeper as a neighbor to this external gatekeeper, and define the zone prefix for the internal gatekeeper according to the dial plan.
- Step 2** In the external gatekeeper interface, define the following forwarding rules:
- Forward any dial strings that begin with Resource Manager Meeting ID Prefix to the internal gatekeeper.
  - Forward any dial strings that begin with MCU service prefix or gateway service prefix to the internal gatekeeper.

Since terminals are registered to the external gatekeeper, these two forwarding rules allow these terminals to dial into the Resource Manager meetings from the external gatekeeper.

---



## CHAPTER 3

# Configuring a SIP Server Profile in Resource Manager

---

- [Creating or Modifying a SIP Server Profile, page 3-1](#)
- [Removing a SIP Server Profile, page 3-2](#)
- [Searching for a SIP Server Profile, page 3-2](#)
- [Configuring the MCU to Work in SIP Mode, page 3-3](#)
- [Disabling the SIP Back-to-Back User Agent, page 3-3](#)

## Creating or Modifying a SIP Server Profile

Resource Manager includes an embedded SIP Back-to-Back User Agent (B2BUA) component for managing SIP traffic to network devices (such as to MCUs) which are managed by Resource Manager.

To enable Resource Manager to operate with SIP endpoints, configure Resource Manager with an external SIP server to which SIP endpoints are registered.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gatekeeper/SIP server**.
- Step 3** Click the link in the Name column for the SIP server you require, or click **Add** to create a new SIP server profile.
- Step 4** Enter the name and IP address or Fully Qualified Domain Name (FQDN) of the SIP server in the relevant fields.
- Step 5** Select the SIP server model.  
You can select Microsoft LCS or other third-party SIP servers. Resource Manager is interoperable with the following external SIP servers:
  - Cisco Unified Communications Manager version 5.0 or later
  - Microsoft Live Communications Server 2005 with Service Pack 1
  - Broadsoft IPCentrix
- Step 6** (Optional) If you select **Other** in the Model field, select **SIP** in the Protocol field.
- Step 7** Select the device island to which the SIP server belongs from the Location list.

Each device island can have only one SIP server.

The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.

- Step 8** Enter the name of the SIP server in the **SIP Domain** field.
  - Step 9** (Optional) Enter the name of a preferred and an alternative DNS server in the relevant fields.
  - Step 10** Click **OK** to save your changes.
- 

## Removing a SIP Server Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Gatekeeper/SIP server**.
  - Step 3** Click the SIP server entry you wish to delete in the Name column.
  - Step 4** Click **Delete** and then **OK**.
- The SIP server profile is deleted from the scheduler and information about the SIP server is removed from the database.
- 

## Searching for a SIP Server Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Gatekeeper/SIP server**.
  - Step 3** Enter all or part of the name of the SIP server you want to find in the Name field.
  - Step 4** Click **Search**.
- Search results are listed.
- Step 5** To return to the complete list of SIP servers, clear the Name field, and then click **Search**.
-

## Configuring the MCU to Work in SIP Mode

Perform the following configuration steps in the MCU web user interface.

### Procedure

- 
- Step 1** Under **MCU > Protocols > SIP**, select **Enable SIP Protocol**.
  - Step 2** Set the SIP server IP address as the IP address of Resource Manager.  
Do not change the port number or the type (UDP/TCP). The default port is 5060 and type is UDP.
  - Step 3** If the external SIP server is LCS 2005 or OCS 2007, select **Using Microsoft LCS**.  
In this case, the type is always TCP.
  - Step 4** Select **Treat as outbound proxy** to set Resource Manager as the outbound proxy of the MCU that is working in SIP mode.
  - Step 5** Click **Advanced SIP Settings**.
  - Step 6** Select Use **“Empty Invite” when sending messages to endpoints**.



---

**Note** We recommend using an empty invite when dialing out to a SIP endpoint.

---

- Step 7** Click **OK** to save your changes.
- Step 8** On the external SIP server, define a routing rule that forwards all calls whose dialing strings begin with the Resource Manager meeting ID or service prefix to Resource Manager.  
The embedded SIP B2BUA can then forward the call to the appropriate MCU conference.



---

**Note** The default signalling port of the external SIP server is 5060.

---

## Disabling the SIP Back-to-Back User Agent

You can disable the B2BUA if Resource Manager is currently not operating with an external SIP server to which SIP endpoints are registered

### Procedure

- 
- Step 1** Go to **Control Panel > Administrative Tools > Services** on the Cisco Unified Videoconferencing Manager server.
  - Step 2** Locate the service named “SIP Server” and stop it.
  - Step 3** Use a text editor to open the vcs-core.properties file located at JBOSS\_HOME\bin on the Cisco Unified Videoconferencing Manager server where JBOSS\_HOME is the home directory of the JBOSS application server used in Cisco Unified Videoconferencing Manager.  
By default, JBOSS\_HOME is C:\Program Files\Cisco\Unified Videoconferencing Manager\CUVCMRM\jboss.

**Step 4** Set the following line as shown:

```
vnex.vcms.core.sip.serverAddress=
```

**Step 5** Save and close the vcs-core.properties file.

**Step 6** Restart the SIP Server service for the change to take affect.

---



## CHAPTER 4

# Managing an MCU Profile in Resource Manager

---

- [Configuring Cascading, page 4-1](#)
- [Creating or Modifying an MCU Profile, page 4-2](#)
- [Taking an MCU Offline, page 4-3](#)
- [Removing an MCU Profile, page 4-4](#)
- [Searching for an MCU Profile, page 4-4](#)
- [Synchronizing MCU Information with Cisco Unified Videoconferencing Manager, page 4-4](#)
- [How to Manage Meeting Types, page 4-5](#)
- [Limiting User Access to Meeting Types, page 4-10](#)
- [Customizing MCU Delimiters, page 4-11](#)
- [Designating a Service for IVR Use, page 4-11](#)
- [Defining Video IVR Services, page 4-12](#)

## Configuring Cascading

Resource Manager is able to manage multiple MCUs as a pool of resources. You can cascade MCUs to reduce potential drain on network resources, increase the efficiency of MCU usage, and allow large conferences to be held. The following points about cascading should be noted:

- The Meeting Type (MCU service) representing the required meeting must be available on all participating MCUs. For example, if the meeting uses MCU service 81, then 81 must exist on the master MCU and on the slave MCUs.
- A cascaded connection uses two ports—one on the master MCU conference, and one port on the slave MCU conference.
- Only one cascading stream exists between the master MCU and the slave MCU; therefore, only one participant from the slave MCU can send video for mixing and only one participant from the slave MCU can be seen by other participants in the meeting.
- Only one level of cascading is supported. All slave MCU conferences must cascade to the same master MCU conference.
- The administrator must define a default system level property that determines the cascading behavior.

To configure the MCU cascading behavior, use the following procedure:

**Procedure**

- 
- Step 1** From the sidebar menu, go to **Admin > Advanced Settings**.
- Step 2** On the Default Meeting Settings tab you can enable or disable automatic cascading of MCU conferences by configuring the Allow Cascaded Meeting field.
- Step 3** If Allow Cascaded Meeting is set to yes, choose one of the following options from the Prioritize field:
- **Bandwidth**—Resource Manager allocates resources to conserve bandwidth. For example, at a site with two users and one MCU, Resource Manager creates a local meeting. In some cases, this may cause a meeting to cascade to conserve bandwidth, even though a single MCU is available to host the meeting.  
Using this option, Resource Manager cascades a maximum of two MCUs.
  - **Delay (default)**—Resource Manager allocates resources to ensure the best video quality. Resource Manager invites all users directly to a main MCU, whatever their location. Since Delay can be costly in terms of bandwidth, it is recommended that you take topology into account before selecting the Delay option.
  - **Local MCU**—Select this option if Resource Manager has more than one MCU and there are at least two meeting participants. Resource Manager invites all of the participating terminals to meetings hosted on their respective local MCUs (according to IP Topology settings), and then cascades these meetings together to form a single conference.
- Step 4** Click **OK** to save the preferred behavior as the default.
- 

## Creating or Modifying an MCU Profile

The MCU is where a multipoint videoconference is hosted. Resource Manager reserves MCU resources, schedules MCU conferences, and controls in-session MCU meetings. In order for Resource Manager to correctly manage the MCU, it needs to retrieve configuration information from the MCU via the profiles defined under Admin > Resource Management.

**Procedure**

- 
- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **MCU**.
- Step 3** Click the link in the Name column for the MCU you require, or click **Add** to create a new MCU profile.
- Step 4** Enter the name and IP address of the MCU in the relevant fields.
- Step 5** Select the MCU model.
- Step 6** If you want the MCU to operate in H.323 mode, select a gatekeeper from the Registered To list.  
This is the gatekeeper to which the MCU registers.
- Step 7** If you want to register the MCU to operate in SIP mode only (without registering to an H.323 gatekeeper), select **MCU operates in SIP only mode**.  
The MCU is not required to register to a gatekeeper and the Registered To field is inactive.
- Step 8** From the Location list, choose the device island to which the MCU belongs.

The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.

**Step 9** Enter the login name and login password of the MCU in the relevant fields.

These must match the MCU web interface login name and password.

**Step 10** Define SNMP communities, user name and password, communication port and signaling port in the relevant fields.

SNMP community information must match the settings defined in the MCU to enable Resource Manager to retrieve information from the MCU.

**Step 11** Click **OK** to save your changes.

The MCU is added to the MCU tab and brought online by default.

If Resource Manager cannot connect to a newly configured MCU, the MCU is added but its status is shown as Offline in the MCU tab.

To try to reconnect to the MCU, select **Online**, and then click **OK**.

---

## Taking an MCU Offline

### Procedure

---

**Step 1** Click **Resource Management** in the sidebar menu.

**Step 2** Click **MCU**.

**Step 3** Click the link in the Name column for the MCU you require.

**Step 4** To take the MCU offline temporarily, select **Take this MCU offline and reschedule all meetings on this MCU up to this date** and set the date to bring the MCU online again.

**Step 5** To take the MCU offline permanently, select **Take this MCU offline and reschedule all meetings currently on this MCU**.

**Step 6** Click **OK** to save your changes.

When you take the MCU offline, the following changes occur:

- Resource Manager cannot schedule meetings for the offline MCU.
  - All meetings currently in progress are terminated. Resource Manager attempts to reschedule upcoming meetings for the offline MCU on other MCUs that use the same services and have sufficient, available resources. If no replacement MCUs are available when the MCU status is changed back to online, upcoming meetings are lost and not restored.
  - If the MCU goes offline temporarily, Resource Manager attempts to reschedule all meetings scheduled to this MCU from the time the MCU goes offline to the specified date for its return online.
  - If the MCU goes offline permanently, Resource Manager attempts to reschedule all future meetings scheduled to this MCU.
-

## Removing an MCU Profile

You must take an MCU offline before you can remove it from the Cisco Unified Videoconferencing Manager database.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **MCU**.
- Step 3** Click the MCU entry you wish to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.

The MCU profile is deleted from the scheduler and information about the MCU is removed from the database.

---

## Searching for an MCU Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **MCU**.
  - Step 3** Enter the partial or complete name of the MCU in the Name field.
  - Step 4** Click **Search**.  
Search results are listed.
  - Step 5** To return to the complete list of MCUs, clear the Name field, and then click **Search**.
- 

## Synchronizing MCU Information with Cisco Unified Videoconferencing Manager

When a new MCU is initially configured, its internal information is downloaded to Resource Manager. If you change the initial configuration, you must update the Resource Manager.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **MCU**.
- Step 3** Click the MCU entry you wish to update in the Name column.

**Step 4** Click **Synchronize**.

The information download includes the number of cards the MCU has and the resource capacity of each card.

---

## How to Manage Meeting Types

A meeting type in Resource Manager is the equivalent of the MCU service definition. Services should be defined in the MCU first and then synchronized to Resource Manager. In the Meeting Types section, retrieve services from MCUs configured in the system and then save them to Resource Manager. Resource Manager then distributes these services to other MCUs according to your specific deployment requirements. Meeting types in Resource Manager are used to schedule meetings on the MCU. There are also built-in meeting types that are not retrieved from the MCU in Resource Manager.

- [Viewing Available Meeting Types on Network MCUs, page 4-5](#)
- [Viewing Built-in Meeting Types, page 4-6](#)
- [Removing a Meeting Type, page 4-7](#)
- [Searching for a Meeting Type, page 4-7](#)
- [Downloading a Meeting Type to Resource Manager, page 4-7](#)
- [Resolving Meeting Type Conflicts Between MCUs, page 4-8](#)
- [Resolving Meeting Type Conflicts Between Resource Manager and an MCU, page 4-8](#)
- [Uploading a Meeting Type to Network MCUs, page 4-9](#)
- [Viewing Meeting Type Details, page 4-9](#)
- [Modifying Meeting Type Details, page 4-9](#)
- [Accessing an MCU from the Meeting Type Details Screen, page 4-10](#)
- [Viewing a List of MCUs Containing a Specified Meeting Type, page 4-10](#)
- [Limiting User Access to Meeting Types, page 4-10](#)

## Viewing Available Meeting Types on Network MCUs

### Procedure

---

**Step 1** Click **Meeting Types** in the sidebar menu.

**Step 2** Ensure that the Active Meeting Types tab is displayed.

All meeting types available for meeting scheduling are displayed with the parameters listed in [Table 4-1](#).

If the name of a meeting type appears in red, the meeting type does not belong to any MCU and cannot currently be used for meeting scheduling.

**Table 4-1 Meeting Type Parameters**

Parameter	Description
Name	The name of a meeting type defined in Resource Manager.
Prefix	The service prefix downloaded from the MCU.
Description	The service description downloaded from the MCU.
Media	The service media type downloaded from the MCU.
BW(Kbps)	The maximum service bandwidth (in kilobytes per second) for download from the MCU.
Lecture Mode	For MCU services that support exactly two views with the first view being single sub-frame and the second view being multiple sub-frames, you can set this service to support the lecture mode feature in which a meeting participant is set to one view and can be seen by all other participants, and the other participants are set to the other view and can be seen by the first participant.
In Use	Indicates whether or not there are currently or upcoming meetings in Resource Manager that use the specified meeting type. If so, the meeting type is considered in use and cannot be deleted from the system until the meeting type is no longer in use.
MCUs	Click Details to display a list of all MCUs defined in Cisco Unified Videoconferencing Manager containing the specified meeting type.

## Viewing Built-in Meeting Types

You cannot modify, upload or download built-in meeting types.

### Procedure

- 
- Step 1** Click **Meeting Types** in the sidebar menu.
- Step 2** Ensure that the Active Meeting Types tab is displayed.
- The built-in meeting types listed in [Table 4-2](#) are available.

**Table 4-2 Built-in Meeting Types**

Parameter	Description
Non Video Conference	This is a conference that involves only users and meeting rooms. There is no need for video conference devices. Use this meeting type to reserve users and room resources only.
Point to Point	This is a conference that involves only two endpoints (terminals) and no MCU resources. It can only be created if one endpoint dials another endpoint directly.

## Removing a Meeting Type

An active meeting type must be deactivated before it can be permanently removed from the system. Once a meeting type is inactive, it can no longer be used for meeting scheduling; however, you must wait until all current or future meetings that use this meeting type are in the past, or you must cancel them. When there are no longer any scheduled meetings that required this meeting type, the meeting type is marked not in use and is removed.

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
- Step 2** Select the meeting type you wish to delete.
- Step 3** Click **Deactivate** and then **OK**.

The meeting type is removed from the Active Meeting Types tab and placed on the Inactive Meeting Types tab.

---

## Searching for a Meeting Type

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Enter the partial or complete name of the meeting type in the Name field.
  - Step 3** Click **Search**.  
Search results are listed.
  - Step 4** To return to the complete list of meeting types, clear the Name field, and then click **Search**.
- 

## Downloading a Meeting Type to Resource Manager

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
- Step 2** Select the meeting types you want to download to Resource Manager on the Active Meeting Types tab.
- Step 3** Click **Download**.

MCU services are downloaded from all network MCUs.

Because MCU services are downloaded via SNMP, the process might take some time if there are many MCUs to connect to.

- Step 4** Enter a unique name for each meeting type.
  - Step 5** Click **OK**.
- 

## Resolving Meeting Type Conflicts Between MCUs

You might need to resolve a conflict when downloading MCU services if two services from two different MCUs in the network have the same service prefix. For example, both services might have prefix 80, which is the default prefix for an audio service.

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Select the meeting types you want to download to Resource Manager on the Active Meeting Types tab.
  - Step 3** Click **Download**.  
MCU services are downloaded from all network MCUs.  
Since MCU services are downloaded via SNMP, the process may take some time if there are many MCUs to connect to.
  - Step 4** Scroll down to the Meeting Type (Service) Conflicts section on the Download Meeting Types (Services) screen.
  - Step 5** Select the entry that you want to keep in the **Use Meeting Type (Service) Definition From** column for each service prefix listed.  
Resource Manager downloads the specified copy of the MCU service and overwrites all other MCU services that use the same prefix on other network MCUs.  
This process enables Resource Manager to ensure that all services with the same service prefix are identical on different MCUs in the network.  
This process does not assign a service to MCUs that do not already have the service prefix defined.
  - Step 6** Enter a unique name for each meeting type.
  - Step 7** Click **OK**.
- 

## Resolving Meeting Type Conflicts Between Resource Manager and an MCU

If a service downloaded from a network MCU conflicts with a service that already exists in Resource Manager, the service stored in Resource Manager is selected by default during conflict resolution.

If a service exists only on a single MCU that is removed from the network, that service can no longer be used for meeting scheduling. Such services are displayed in red.

## Uploading a Meeting Type to Network MCUs

We recommend that you configure all network MCUs with exactly the same service definitions so that you can treat all your MCUs as a pool of interchangeable resources.

Resource Manager supports mixed version 4 and 5 MCU deployments. However, version 4 and 5 MCU cannot share the same MCU service prefix. If you try to perform such operations, you receive a warning message.

MCU services defined as supporting High Definition Continuous Presence (HP CD) conferences cannot be synchronized to a MCU that is not HD CP enabled. If you try to perform such operations, you receive a warning message.

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
- Step 2** Select the meeting types you want to upload from Resource Manager on the Active Meeting Types tab.
- Step 3** Click **Upload**.
- Step 4** Use the arrows to select the target MCUs.
- Step 5** Click **OK**.

Because MCU services are uploaded via SNMP, the process might take some time if there are many MCUs to connect to.

---

## Viewing Meeting Type Details

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Click the link in the Name column for the meeting type you require on the Active Meeting Types tab.
- 

## Modifying Meeting Type Details

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
- Step 2** Click the link in the Name column for the meeting type you require on the Active Meeting Types tab.
- Step 3** (Optional) Enter a new name for the meeting type.
- Step 4** (Optional) Specify a default connection rate value.

The default connection rate value must be less than the maximum bandwidth value.

The default connection rate is used for any non-predefined terminals that you invited without specifying a bandwidth for those terminals during meeting scheduling process or in-meeting control operations.

- Step 5** (Optional) If the meeting type supports lecture mode, check **Select Lecture Mode** to enable this support.
  - Step 6** (Optional) Define an Auto Attendance session number for video IVR support.
  - Step 7** Click **OK** to save your changes.
- 

## Accessing an MCU from the Meeting Type Details Screen

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Click the link in the Name column for the meeting type you require on the Active Meeting Types tab. A link is available for each MCU containing the specified meeting type.
- 

## Viewing a List of MCUs Containing a Specified Meeting Type

### Procedure

---

- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Click **Detail** in the MCU column to see a list of MCUs containing the specified meeting type.
- 

## Limiting User Access to Meeting Types

Meeting types listed on the Active Meeting Types tab are automatically listed in the Meeting Type field at User > Meeting Scheduling > Meeting. You can limit which meeting types are accessible by users.

### Procedure

---

- Step 1** Customize the available meeting types in **Admin > Advanced Settings > Default User Settings**.
  - Step 2** (Optional) Configure which user can use which meeting type for scheduling in the profile of the user at **Admin > User Management > User Profile**.
-

## Customizing MCU Delimiters

By default, \*\* is the MCU delimiter for inviting an endpoint to a meeting, and \*\*\* is the MCU delimiter for the meeting password.

If MCU delimiters are customized via the MCU web user interface configuration, you need to configure MCU delimiters accordingly in Resource Manager as well.

### Procedure

- 
- Step 1** Open the vcs-core.properties file located at \JBOSS\_DIR\BIN.
  - Step 2** Locate the following string:  
vnex.vcms.core.mcuPasswordDelimiter=###
  - Step 3** Modify the delimiter to match the value configured in the MCU web user interface.
  - Step 4** Save and close the vcs-core.properties file.



**Note** JBOSS\_DIR is the default JBOSS home directory path. The default path is C:\Program Files\Cisco\Unified Videoconferencing Manager\CUVCMRM\jboss.

---

## Designating a Service for IVR Use

You can define the MCU service for entry into the IVR audio and video message utility.

When you download MCU services for the first time, Resource Manager automatically selects the first audio and video service that you download for IVR entry.

### Procedure

- 
- Step 1** Click **Meeting Types** in the sidebar menu.
  - Step 2** Click **Active Meeting Types**.
  - Step 3** Click the name of the service you want to use for entry to the IVR.
  - Step 4** Select **Used for auto attendance session**.
  - Step 5** Enter a number in the **Auto attendance session number** field.  
Verify that this number does not begin with any MCU or gateway service or Cisco IOS H.323 Gatekeeper zone prefix, or is the same as the number of an IP terminal.
  - Step 6** Click **OK** to save your changes.

The designated service is marked with an icon in the Name column of the Active Meeting Types screen.

---

# Defining Video IVR Services

Define the MCU service for video IVR entry as described here to obtain the best quality for the video IVR session.

We recommend that you do not use HD CP-enabled MCU services for video IVR sessions.

## Procedure

---

- Step 1** Access the MCU web user interface.
  - Step 2** Under **Services > Add > Advanced Audio Settings**, ensure that H.263 is the first entry in the Selected list.
  - Step 3** Under **Services > Add > Support image size up to**, select **4CIF** from the drop-down list.
  - Step 4** Click **OK** and **Upload** to save your changes.
-



## CHAPTER 5

# Configuring a Gateway Profile in Resource Manager

---

- [Creating or Modifying a Gateway Profile, page 5-1](#)
- [Taking a Gateway Offline, page 5-3](#)
- [Removing a Gateway Profile, page 5-4](#)
- [Searching for a Gateway Profile, page 5-4](#)

## Creating or Modifying a Gateway Profile

Configure gateways in your network to enable PSTN/ISDN/mobile terminals to join a meeting. Resource Manager uses the gateway information to provide proper dialing information for meeting participants, and to dial out to terminals to invite them to meetings. Resource Manager also manages gateway resources to allow successful call scheduling using network gateways.

When you add a gateway, settings in Resource Manager must be consistent with the actual gateway configuration. We recommend the following:

- If you make changes to the gateway, maintain the IVR and DID numbers in Resource Manager.
- To ensure that there are no gateway ports available for scheduled and ad hoc calls, maintain capacity information.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gateway**.
- Step 3** Click the link in the Name column for the gateway you require, or click **Add** to create a new gateway profile.
- Step 4** Enter the name of the gateway in the Name field.
- Step 5** Select a gateway model and enter an IP address in the relevant fields.



**Note** If multiple gateways are pooled together in a local network with the same access phone number, you can enter multiple IP addresses in the IP Address field to indicate the gateways in the gateway pool. IP addresses are separated by a colon (:).

---

- Step 6** From the Registered To list, choose the gatekeeper to which the gateway is registered.
- Step 7** From the Location list, choose the device island to which the MCU belongs.
- The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 8** Enter the bandwidth for the gateway or gateway pool. For example, for an E1 line, the bandwidth should be 30 B-channels (3940 Kbps).
- Step 9** Indicate in the Working Mode field whether the gateway operates in IVR or DID mode.
- Resource Manager works with the gateway in DID mode so that meeting participants can easily dial into a meeting. You can assign a range of DID numbers to the gateway. These numbers can be assigned to individual dial-in terminals (endpoints). If you dial one of the assigned DID numbers, you are automatically added to the meeting that the DID number is associated with. Only one terminal can dial a DID number at any given time.
- If you configure the gateway in DID mode and set a DID number in the Telephone Number field, when a terminal dials this DID number Resource Manager routes the call to the appropriate meeting based on the terminal number. If no associated meeting is found, then the dial-in call is routed back to the gateway for an IVR session. After entering the meeting ID using the IVR, the terminal is permitted to join the meeting.
- Step 10** Enter a gateway phone number.
- In the Description field, enter a description of the phone number for the gateway.
  - In the International Access Code field, enter the numeric prefix required to make an international long distance call.
  - In the Domestic Long Distance Prefix field, enter the numeric prefix required to make a long distance call within the same country.
  - In the Country Code field, enter the country code for the gateway phone number. Resource Manager adds this prefix when dial-out is performed from this gateway to a terminal located in a different country than the country in which the gateway is located.
  - If Allow Out of Area Calls is not checked, only endpoints with the same area code as the gateway are allowed to reach Resource Manager via the gateway.
  - If you check Allow Out of Area Calls, the gateway accepts incoming calls to Resource Manager from terminals with a different area code than that of the gateway.
  - Enter the domestic area code of the gateway number in the Area Code field.
  - Specify a local telephone number in the Telephone Number field that you want to assign to the specific port.
  - Enter a number in the To access an outside line for local calls, dial field for a gateway with no direct access to an outside line for local calls.
  - Enter a number in the To access an outside line for long distance calls, dial field, for a gateway with no direct access to an outside line for long distance calls.
  - Assign the ISDN device island that the gateway or gateway pool belongs to. If ISDN Topology is hidden, then this field is also hidden.
- Step 11** Define the DID range.
- If DID is selected in the Working Mode field, define the DID range for the gateway or gateway pool.

**Step 12** Click **Add Service** to add or modify the gateway service.



**Note** In the Bandwidth section, if you check **Restricted Mode**, 56 appears in the Kbps list. Multiples of 56 Kbps are used instead of multiples of 64. Resource Manager does not support gateway services whose bandwidth is set to “auto” since Resource Manager needs the specific bandwidth to perform resource reservation. If there is a gateway service with “auto” bandwidth, when you configure this service in Resource Manager, select a bandwidth value to best approximate the average bandwidth endpoints use when dialing that service.

**Step 13** Set the Advanced Settings.

- In the Signaling Port field, set the gateway port used for signaling. By default, it is left blank and signaling port will be negotiated dynamically on the fly.
- In the SNMP Get/Set Community fields, set the SNMP community name required by Resource Manager to communicate with the gateway.
- Choose **Dial-in Only** to mark the gateway for use only with terminals that users dial into. Resource Manager does not schedule dial-out calls on this gateway.

**Step 14** Click **OK** to save your changes.

## Taking a Gateway Offline

Once a gateway is configured, it is automatically brought online so that Resource Manager can schedule resources.

### Procedure

**Step 1** Click **Resource Management** in the sidebar menu.

**Step 2** Click **Gateway**.

**Step 3** Click the link in the Name column for the gateway you require.

**Step 4** To take the MCU offline temporarily, select **Take this gateway offline and reschedule all meetings on this gateway up to this date** and set the date to bring the gateway online again.

**Step 5** To take the MCU offline permanently, select **Take this gateway offline and reschedule all meetings currently on this gateway**.

**Step 6** Click **OK** to save your changes.

When you take the gateway offline, the following changes occur:

- Resource Manager cannot schedule meetings for the offline gateway.
- All meetings currently in progress are terminated. Resource Manager attempts to reschedule upcoming meetings for the offline gateway on other gateways that use the same services and have sufficient, available resources. If no replacement gateways are available when the gateway status is changed back to online, upcoming meetings are lost and not restored.

- If the gateway goes offline temporarily, Resource Manager attempts to reschedule all meetings scheduled to this gateway from the time the gateway goes offline to the specified date for its return online.
  - If the gateway goes offline permanently, Resource Manager attempts to reschedule all future meetings scheduled to this gateway.
- 

## Removing a Gateway Profile

You must take an MCU offline before you can remove it from the Cisco Unified Videoconferencing Manager database.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gateway**.
- Step 3** Click the gateway entry you wish to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.

The gateway profile is deleted from the scheduler and information about the gateway is removed from the database.

---

## Searching for a Gateway Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Gateway**.
- Step 3** Enter the partial or complete name of the gateway in the Name field.
- Step 4** Click **Search**.

Search results are listed.

The Status column indicates whether the gateway is online or not. Resource Manager only uses an online gateway for meeting scheduling and creation.

The SNMP Connection column indicates whether or not Resource Manager established an SNMP connection with the gateway.

- Step 5** To return to the complete list of gateways, clear the Name field, and then click **Search**.
-



## CHAPTER 6

# Configuring a Cisco Unified Videoconferencing Desktop Server Profile in Resource Manager

- [Creating or Modifying a Desktop Server Profile, page 6-1](#)
- [Removing a Desktop Server Profile, page 6-2](#)
- [Searching for a Desktop Server Profile, page 6-2](#)

## Creating or Modifying a Desktop Server Profile

Once a Desktop Server is configured, it is automatically brought online so that Resource Manager can schedule resources.

### Procedure

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Desktop**.
- Step 3** Click the link in the Name column for the Desktop Server you require, or click **Add** to create a new Desktop Server profile.
- Step 4** Enter the name of the Desktop Server in the Name field.
- Step 5** Enter the URL used by participants to join a meeting via Desktop Server in the Web Access URL field. The URL must be in the format [http://<IP address>:<port number>/desktop](#)
- Step 6** Enter an H.323 ID used to identify connections from Desktop Server in MCU conferences in the H.323 ID field.  
Ensure that the same H.323 ID is configured in the Desktop Server administrator web interface.  
Configuring this field allows Resource Manager to intelligently route calls from this Cisco Unified Videoconferencing Desktop Server based on the predefined IP topology.
- Step 7** Select a topology setting from the Location drop-down list. The default value is Home.  
The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 8** Enter any text you want to associate with the web access URL in the Description Text field.  
The description text is embedded in e-mail invitations sent to meeting participants.
- Step 9** Click **Access URL** to add a placeholder for the access URL for Desktop Server clients.

- Step 10** Click **Installer URL** to add a placeholder for the link via which users install the Desktop Server client before the meeting.
- Step 11** Click **OK** to save your changes.
- 

## Removing a Desktop Server Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Desktop**.
- Step 3** Click the Desktop Server entry you wish to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.

The Desktop Server profile is deleted from the scheduler and information about the Desktop Server is removed from the database.

---

## Searching for a Desktop Server Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Desktop**.
- Step 3** Enter the partial or complete name of the Desktop Server in the **Name** field.
- Step 4** Click **Search**.  
Search results are listed.
- Step 5** To return to the complete list of Desktop Servers, clear the Name field, and then click **Search**.
- 

## How to Stream Meetings Using Desktop Server

- [Enabling Streaming on Cisco Unified Videoconferencing Desktop Server, page 6-3](#)
- [Enabling Streaming for a Virtual Room, page 6-3](#)
- [Allowing Recording by Specified Roles, page 6-3](#)
- [Allowing Recording by Specified Users, page 6-3](#)
- [Enabling Recording for Specified Virtual Rooms, page 6-4](#)

## Enabling Streaming on Cisco Unified Videoconferencing Desktop Server

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Look and Feel**.
  - Step 3** Set Streaming to **Visible**.
  - Step 4** Click **OK** to save your changes.
- 

## Enabling Streaming for a Virtual Room

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
  - Step 2** Click the link in the Name column for the user you require, or click **Add** to create a new user profile.
  - Step 3** Click **Virtual Room Setting**.
  - Step 4** Set Streaming to **Enabled**.
  - Step 5** Click **OK** to save your changes.
- 

## Allowing Recording by Specified Roles

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Default User Settings**.
  - Step 3** Select an option from the Recording Policy field.  
Select **Allow everyone to record** to enable recording permission for endpoint-initiated ad hoc conferences that do not belong to a specific user.
  - Step 4** Click **OK** to save your changes.
- 

## Allowing Recording by Specified Users

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
- Step 2** Click **Users**.

- Step 3** Click the link in the Name column for the user you require.
- Step 4** Click **Advanced**.
- Step 5** (Optional) Select **Inherit recording policy from Default User Settings** to define custom recording policy for this user.
- Step 6** (Optional) Select **Allow user to record meeting** to enable this user to record meeting regardless of the global policy.
- Step 7** Click **OK** to save your changes.
- 

## Enabling Recording for Specified Virtual Rooms

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
- Step 2** Click **Users**.
- Step 3** Click the link in the Name column for the user you require.
- Step 4** Click **Virtual Room Setting**.
- Step 5** Select **Try to record meeting when meeting starts** to automatically record a meeting when the meeting starts.

This option is available if

- Recording is allowed for the current user according to the recording policy.
- The Record Meeting field is set to Enabled under Admin > Advanced Settings > Look and Feel.

The meeting will not be recorded if there are not enough available recording ports on the Desktop Server when the meeting is scheduled.

- Step 6** Click **OK** to save your changes.
-



## CHAPTER 7

# Configuring a Meeting Room Profile in Resource Manager

---

A meeting room is the physical location of one or more terminals. Meeting rooms are also used for non-videoconference meetings in which no terminals are involved.

- [Enabling Meeting Room Support, page 7-1](#)
- [Creating or Modifying a Meeting Room Profile, page 7-1](#)
- [Sending Meeting Details by E-mail, page 7-2](#)
- [Removing a Meeting Room Profile, page 7-2](#)
- [Searching for a Meeting Room Profile, page 7-3](#)

## Enabling Meeting Room Support

By default, the Meeting Rooms tab is hidden in Resource Manager. Enable support for meeting rooms as follows:

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Look and Feel**.
  - Step 3** Deselect **Hide Meeting Rooms**.
  - Step 4** Click **OK** to save your changes.
- 

## Creating or Modifying a Meeting Room Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Meeting Rooms**.

- Step 3** Click the link in the Name column for the meeting room you require, or click **Add** to create a new meeting room profile.
  - Step 4** Enter the name and location of the meeting room in the relevant fields.
  - Step 5** Click **OK** to save your changes.
- 

## Sending Meeting Details by E-mail

You can define an e-mail address to enable a terminal that participates in a meeting to receive notification e-mail messages.

By default, this option is hidden.

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Look and Feel**.
  - Step 3** Deselect **Hide Meeting Notification E-mail for meeting rooms and terminals**.
  - Step 4** Click **OK** to save your changes.
  - Step 5** Click **Resource Management** in the sidebar menu.
  - Step 6** Click **Meeting Rooms**.
  - Step 7** Click the link in the Name column for the meeting room you require.
  - Step 8** Select **Meeting e-mail notification address** and enter the e-mail address for the meeting room.
  - Step 9** Select a time zone for the meeting room.  
The default value is set at Advanced Settings > Default User Settings > Default Time Zone.
  - Step 10** Click **OK** to save your changes.
- 

## Removing a Meeting Room Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Meeting Rooms**.
  - Step 3** Click the meeting room entry you wish to delete in the Name column.
  - Step 4** Click **Delete** and then **OK**.  
The meeting room profile is deleted from the scheduler and information about the meeting room is removed from the database.
-

# Searching for a Meeting Room Profile

## Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Meeting Rooms**.
  - Step 3** Enter the partial or complete name of the meeting room in the Name field.
  - Step 4** Click **Search**.  
Search results are listed.
  - Step 5** To return to the complete list of meeting rooms, clear the Name field, and then click **Search**.
-

■ Searching for a Meeting Room Profile



## CHAPTER 8

# Configuring a Terminal Profile in Resource Manager

---

- [How to Create or Modify a Terminal Profile, page 8-1](#)
- [Removing a Terminal Profile, page 8-5](#)
- [Searching for a Terminal Profile, page 8-5](#)

## How to Create or Modify a Terminal Profile

The term “terminal” refers to any kind of endpoint (H.323, SIP, ISDN, or mobile) used for videoconferencing.

- [Defining H.323 IP Terminal Details, page 8-2](#)
- [Defining SIP IP Terminal Details, page 8-2](#)
- [Defining ISDN/PSTN H.320 Terminal Details, page 8-3](#)
- [Defining Mobile Terminal Details, page 8-4](#)
- [Defining Dual H.320 and H.323 Terminal Details, page 8-4](#)



### Note

---

To avoid conflicts between endpoint-initiated point-to-point meetings and endpoint-initiated multipoint meetings, the names of endpoints and terminals registered to gatekeepers in Resource Manager cannot start with the same prefix as the MCU service or as a meeting type ID in Resource Manager.

---

## Defining H.323 IP Terminal Details

Define all H.323 terminals registered to gatekeepers that are configured in Resource Manager.

### Procedure

- 
- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Terminals**.
  - Step 3** Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
  - Step 4** (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.
  - Step 5** Click **OK** to apply your selections and to close the Select Users window.
  - Step 6** (Optional) Enter any description text that you may have for this terminal in the Description field.
  - Step 7** Select **IP(H.323)** from the Terminal Type list.
  - Step 8** In the IP Phone Number field, enter the E.164 IP phone number of the terminal registered on the gatekeeper as specified in the Registered to field.  
If the terminal is not registered to a gatekeeper, enter the IP address of the terminal in the IP Phone Number field.
  - Step 9** Define the default bandwidth for the terminal in the Bandwidth field. Resource Manager uses the bandwidth number to reserve resources for this terminal.
  - Step 10** Select a topology setting from the Location drop-down list.  
The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
  - Step 11** Click **OK** to save your changes.
- 

## Defining SIP IP Terminal Details

Define all SIP terminals registered to gatekeepers that are configured in Resource Manager.

### Procedure

- 
- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Terminals**.
  - Step 3** Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
  - Step 4** (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.  
Click **OK** to apply your selections and to close the Select Users window.
  - Step 5** (Optional) Enter any description text that you may have for this terminal in the Description field.
  - Step 6** Select **IP(SIP)** from the Terminal Type list.

- Step 7** In the SIP URI field, define the terminal name or terminal number, followed by the SIP server domain name and a suffix derived from the domain name of the SIP server.
- For example, <terminal name>@<SIP server domain name> or “user@domain\_name.com”.
- Step 8** Define the default bandwidth for the terminal in the Bandwidth field. Resource Manager uses the bandwidth number to reserve resources for this terminal.
- Step 9** Select a topology setting from the Location drop-down list.
- The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 10** Click **OK** to save your changes.
- 

## Defining ISDN/PSTN H.320 Terminal Details

Define all H.320 terminals that you want Resource Manager to automatically invite to a meeting and manage their availability.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Terminals**.
- Step 3** Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
- Step 4** (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.
- Click **OK** to apply your selections and to close the Select Users window.
- Step 5** (Optional) Enter any description text that you may have for this terminal in the Description field.
- Step 6** Select **ISDN/PSDN(H.320)** from the Terminal Type list.
- Step 7** Define the default bandwidth for the terminal in the Bandwidth field. Resource Manager uses the bandwidth number to reserve resources for this terminal.
- Step 8** Select a topology setting from the Location drop-down list.
- The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 9** Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.
- Step 10** Enter the phone number of the terminal in the Country Code, Area Code and Number fields.
- If you do not specify this information, Resource Manager cannot find the optimal gateway for the terminal when scheduling a conference.
- Step 11** Click **OK** to save your changes.
-

## Defining Mobile Terminal Details

Define all mobile terminals that you want Resource Manager to automatically invite to a meeting and manage their availability.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Terminals**.
  - Step 3** Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
  - Step 4** (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.  
Click **OK** to apply your selections and to close the Select Users window.
  - Step 5** (Optional) Enter any description text that you may have for this terminal in the Description field.
  - Step 6** Select **Mobile** from the Terminal Type list.
  - Step 7** Define the default bandwidth for the terminal in the Bandwidth field. Resource Manager uses the bandwidth number to reserve resources for this terminal.
  - Step 8** Select a topology setting from the Location drop-down list.  
The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
  - Step 9** Enter the phone number of the terminal in the Country Code, Area Code and Number fields.  
If you do not specify this information, Resource Manager cannot find the optimal gateway for the terminal when scheduling a conference.
  - Step 10** Select **3G** for 3G terminals.
  - Step 11** Click **OK** to save your changes.
- 

## Defining Dual H.320 and H.323 Terminal Details

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Terminals**.
- Step 3** Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
- Step 4** (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.  
Click **OK** to apply your selections and to close the Select Users window.
- Step 5** (Optional) Enter any description text that you may have for this terminal in the Description field.
- Step 6** Select **Dual(H.320 and H.323)** from the Terminal Type list.

- Step 7** In the IP Phone Number field, enter the E.164 IP phone number of the terminal registered on the gatekeeper as specified in the Registered to field.
- If the terminal is not registered to a gatekeeper, enter the IP address of the terminal in the IP Phone Number field.
- Step 8** Define the default bandwidth for the terminal in the IP Bandwidth and ISDN Bandwidth fields. Resource Manager uses the bandwidth number to reserve resources for this terminal.
- Step 9** Select a topology setting from the Location drop-down list.
- The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.
- Step 10** Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.
- Step 11** Enter the phone number of the ISDN terminal in the Country Code, Area Code and Number fields.
- If you do not specify this information, Resource Manager cannot find the optimal gateway for the terminal when scheduling a conference.
- Step 12** Click **OK** to save your changes.
- 

## Removing a Terminal Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Terminals**.
- Step 3** Click the terminal entry you wish to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.
- The terminal profile is deleted from the scheduler and information about the terminal is removed from the database.
- 

## Searching for a Terminal Profile

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
- Step 2** Click **Terminals**.
- Step 3** Enter the partial or complete name of the terminal in the Name field, or enter the partial or complete IP or ISDN phone number of the meeting room in the Dialing Info field.
- The ISDN phone number of the terminal should not include dashes or spaces.
- The ISDN phone number can only be used when you select ISDN/PSTN(H.320) or Dual(H.320 and H.323) in the Terminal Type field.

Both IP and ISDN numbers are displayed if the terminal is configured as a dual terminal.

**Step 4** Click **Search**.

Search results are listed.

**Step 5** To return to the complete list of meeting rooms, clear the Name and Dialing Info fields, and then click **Search**.

---



## CHAPTER 9

# Defining Resource Manager Call Routing Modes

---

Resource Manager offers two call routing modes. This section describes these modes and explains their use in H.323 and SIP deployments.

- [Call Routing in H.323 Deployments, page 9-1](#)
- [Call Routing in SIP Deployments, page 9-2](#)

## Call Routing in H.323 Deployments

In Fully Routed H.323 Mode, Resource Manager acts as an authorization server to the internal gatekeeper. Resource Manager manages all traffic passing through the internal gatekeeper and can control where incoming calls will go.

Fully Routed Mode enables the “Virtual MCU” feature where Resource Manager can present multiple MCUs as a single pool of video and audio ports, or as a single virtual MCU.

For Fully Routed Mode, ensure you select the Enable Gatekeeper advanced features (authorization and point-to-point) option.

### Procedure

---

- Step 1** Click **Resource Management** in the sidebar menu.
  - Step 2** Click **Gatekeeper/SIP server**.
  - Step 3** Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
  - Step 4** Locate the Advanced section.  
The Advanced section appears if you are using the internal gatekeeper.
  - Step 5** Select **Enable Gatekeeper advanced features (authorization and point-to-point)**.
  - Step 6** Click **OK** to save your changes.
-

# Call Routing in SIP Deployments

In SIP deployments, Resource Manager works in Fully Routed Mode using the embedded SIP server to manage all traffic.

Because MCUs have Resource Manager configured as the outbound proxy, and the external SIP server is configured to route incoming calls to the Resource Manager embedded SIP server, Resource Manager can control all calls going through the MCU.

**Note**

Resource Manager cannot manage SIP endpoint point-to-point traffic because these endpoints are registered to the external SIP server.

## Masking Conference Topology with the Virtual MCU Feature

By controlling the call routing logic of the internal gatekeeper, Resource Manager can mask the complexity of the actual network deployment from end users. Resource Manager can create a conference spanning multiple MCUs and present the conference to the end user as a single conference with a single dialing ID, a single PIN, and a single In-meeting Control interface to manage it. This is the Resource Manager Virtual MCU feature.

## Creating a Centralized Conference

**Procedure**

- 
- Step 1** Under **Admin > Advanced Settings > Default Meeting Settings**, set the Prioritize field to **Delay** to host a conference on a single MCU when possible.
- Resource Manager cascades multiple MCUs to create a conference only if the conference size is larger than the capacity of a single MCU.
- Step 2** Click **OK** to save your changes.
- 

## Creating a Distributed Conference

**Procedure**

- 
- Step 1** Under **Admin > Advanced Settings > Default Meeting Settings**, set the Prioritize field to **Local MCU** to force endpoints to cascade to their local MCU first, according to the IP topology configured in the Network Management section.
- If there are endpoints from multiple locations, at least one MCU from each location is cascaded into the main MCU conference.
- Step 2** Click **OK** to save your changes.
-



# CHAPTER 10

## Managing Resource Manager Users and User Groups without an External Directory

---

- [Creating or Modifying a User Profile, page 10-1](#)
- [Removing a User Profile, page 10-2](#)
- [Searching for a User Profile, page 10-2](#)
- [Updating User Profiles, page 10-3](#)
- [Creating a User Group, page 10-3](#)
- [Modifying a User Group, page 10-4](#)
- [Removing a User Group, page 10-4](#)

### Creating or Modifying a User Profile

You can add or modify a user profile if Resource Manager uses its own database for storing user profiles.

If your organization is synchronized with an external directory server to provision users, you can only modify the settings stored in Resource Manager, such as virtual room, default terminals, allowed meeting types, groups, and time zone.

You can modify user passwords, e-mail, telephone and time zone settings at **Users > My Profile** if those settings are not stored in the external directory server.



#### Note

---

Before configuring user profiles, set default settings for each user type at **Advanced Settings > Default User Settings**.

---

#### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
- Step 2** Click **Users**.
- Step 3** Click the link in the Name column for the user you require, or click **Add** to create a new user profile.
- Step 4** Enter the user ID and last name in the relevant fields.
- Step 5** (Optional) Enter the first name, e-mail address and password for the user in the relevant fields, and confirm the password.

- Step 6** (Optional) Click **Virtual Room Setting** to add or modify virtual room settings for the user.
- Step 7** Click **Advanced**.
- Step 8** Select a user type and enter telephone numbers in the relevant fields.
- Step 9** Click **Select Terminal** to assign a default terminal to this user.
- Step 10** Click **Select** next to the Allowed Meeting Types field to restrict this user to a subset of all available meeting types.  
By default, all active meeting types are allowed.
- Step 11** From the Groups list, select the group to which this user belongs.
- Step 12** Select a default time zone.  
Local time zones are used by default at User > My Meetings and User > All Meetings.
- Step 13** Click **OK** to save your changes.  
The user profile is saved and Resource Manager sends the user a notification e-mail containing login access information.
- 

## Removing a User Profile

### Restriction

You cannot remove a user profile if

- You are provisioning users via an external directory server—The Delete button is disabled.
- The user is participating in an in-session meeting—You must wait for the user to leave the meeting.
- The user is the last user with Organization Administrator privileges.

### Procedure

- Step 1** Click **User Management** in the sidebar menu.
- Step 2** Click **Users**.
- Step 3** Click the user profile you want to delete in the Name column.
- Step 4** Click **Delete** and then **OK**.  
The user profile is deleted from the scheduler and information about the user is removed from the database.
- 

## Searching for a User Profile

### Procedure

- Step 1** Click **User Management** in the sidebar menu.
- Step 2** Click **Users**.

- Step 3** Enter the partial or complete name of the user in the Name field, or enter the partial or complete virtual room for the user in the Virtual Room field.
  - Step 4** Select the group in which you want to perform the search.  
The default is All Groups.
  - Step 5** Click **Search**.  
Search results are listed.
  - Step 6** To return to the complete list of users, clear the Name or Virtual Room field, and then click **Search**.
- 

## Updating User Profiles

If your organization uses an external directory server to provision users, you must update the list of Resource Manager user profiles if users are removed from that directory server.

Meeting creation and meeting scheduling issues may arise if you do not update as required.

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
  - Step 2** Click **Users**.
  - Step 3** Click **Update** to import an up-to-date list of users from the external directory server.  
The import process runs in the background enabling administrators to continue working with the system.  
Once the new updated user database is created, users log in to Resource Manager using a directory server login ID and password.
- 

## Creating a User Group

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
  - Step 2** Click **Groups**.
  - Step 3** Click **Add**.
  - Step 4** Enter a name for the group in the Name field.
  - Step 5** Select participants and terminals from the Available Contacts list and click the right-arrow button to move them to the Selected Contacts list.
  - Step 6** Click **OK** to save your changes.  
The group appears in the Groups tab list.
-

## Modifying a User Group

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
  - Step 2** Click **Groups**.
  - Step 3** Click **Add**.
  - Step 4** Click the link in the Name column for the user group you require.
  - Step 5** Modify the name of the user group.
  - Step 6** Click **OK** to save your changes.
- 

## Removing a User Group

### Procedure

---

- Step 1** Click **User Management** in the sidebar menu.
  - Step 2** Click **Groups**.
  - Step 3** Select the group you want to delete.
  - Step 4** Click **Delete** and then **OK**.  
The user group is deleted from the scheduler.
-



## CHAPTER 11

# Provisioning Resource Manager Users via a Directory Server

---

- [Synchronization of User Information, page 11-1](#)
- [Synchronizing Resource Manager with Active Directory Server, page 11-2](#)
- [Configuring a Connection to an LDAP Server, page 11-3](#)
- [Mapping Resource Manager User Roles to ADS Users, page 11-4](#)
- [Defining Virtual Rooms for All LDAP Users, page 11-5](#)
- [Forcing Resource Manager to Use a Virtual Room, page 11-5](#)
- [Resource Manager LDAP Information Attributes, page 11-6](#)

## Synchronization of User Information

If an organization uses an external directory server, Resource Manager can synchronize user information with the directory server, minimizing user setup and maintenance.

Resource Manager supports Microsoft Active Directory Server (ADS) 2000 and 2003.

When Resource Manager connects to an external directory server, each user defined in the directory server is included in Resource Manager, along with the associated user type for that user. If no user type is defined, a user is assigned the user type defined at **Advanced Settings > LDAP Configurations > Advanced**. The default user type setting is Meeting Organizer.

During the organization account creation process, Resource Manager registers the first user (the technical contact)—usually the administrator who performs the installation. This technical contact is automatically assigned the Organization Administrator user type, with permission to log in and provision the other users. The technical contact cannot be deleted from within Resource Manager and should not be deleted from the directory server.

If the directory server is customized not to use standard schema attributes and class labels, the Resource Manager installation application will not correctly configure the database to synchronize with the directory server.

# Synchronizing Resource Manager with Active Directory Server

We assume that Active Directory Server (ADS) includes an organizational unit (OU) called “China” with a sub-OU called “User”.

Resource Manager currently supports synchronization with a single directory server only.

## Procedure

**Step 1** Create the following groups for users under China:

- Organization Administrator
- Meeting Organizer
- Meeting Operator
- Regular User



**Note** These groups can be used by users belonging to any OU(s) in ADS.

**Step 2** Create users in the organizational unit China > Users.

If you do not configure the following properties for each new user, Resource Manager does not download the user from ADS:

- Logon name
- First name and/or last name
- E-mail address.



**Note** Resource Manager does not download users with no e-mail address configured if you select **Do not update users without an e-mail address from the LDAP server..** at Admin > Advanced Settings > LDAP Configurations > Advanced.

**Step 3** In Resource Manager, go to **Advanced Settings > LDAP Configurations** and enter “**ou=Users,ou=China**” in the LDAP Search Base field.

**Step 4** Download the users from China > Users.

The user account used for ADS synchronization requires the following attributes:

- Read-only access to all the users to be downloaded from ADS.
- The user account does not need to be part of the search base. This means that the user account used for accessing ADS does not have to be downloaded to Resource Manager.

**Step 5** To download users from more than one organizational unit, separate the organizational units with a semicolon.

For example, if there are two sub-OUs under “China” called “Users” and “Contractors”, enter the following string in the LDAP Search Base field:

“**ou=Users,ou=China;ou=Contractors,ou=China**”

- Step 6** For a user to be downloaded from a directory server, the following properties must be defined for that user on the directory server:
- User ID and password.
  - First name or last name.
  - E-mail address.
  - Belong to an OU.
  - Belong to a group (if you want to assign user role based on group).
- Step 7** In Resource Manager, go to **Advanced Settings > LDAP Configurations > Advanced** and use the **Do not update users without an e-mail address from the LDAP server to...** and **Update Frequency** options to define record synchronization.
- Step 8** To map specific Resource Manager user roles to ADS users, see the [“Configuring a Connection to an LDAP Server”](#) section on page 11-3.
- 

## Configuring a Connection to an LDAP Server

To work with an LDAP server for user provisioning, you must select user provisioning using a directory server during the installation process.

To work with Microsoft Active Directory and the Resource Manager Outlook Client, select user provisioning using a directory server with Single Sign-on enabled.

After installation, configure videoconferencing devices and terminals before defining LDAP server settings for user provisioning.

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **LDAP Configurations**.
- Step 3** Click **Add** to add a new LDAP server, or click the required LDAP server entry to modify an existing LDAP server.
- Step 4** Select the type of LDAP server to connect Resource Manager to in the Directory Server Type field. Options are Active Directory Server or Lotus Domino Server.
- Step 5** Enter the directory server domain or directory server URL in the Domain/URL field.
- Step 6** Enter the directory server login ID and password in the relevant fields.  
For Active Directory Server, the login ID should be in the format “user@mycompany.com”.



**Note** The user account needs to have read access to all user accounts that you want to synchronize to Resource Manager. This user account does not have to be part of the search base.

---

- Step 7** Click **Configure** to configure the LDAP Search Base field.  
A tree structure appears showing all OUs defined on the Directory Server.
- Step 8** Select the OUs that you want to download users from.

- Step 9** Click **Close**.  
The selected OUs are displayed in the LDAP Search Base field.
- Step 10** Click **OK** to save your changes.
- 

## Mapping Resource Manager User Roles to ADS Users

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **LDAP Configurations**.
- Step 3** In the Advanced section, assign LDAP users to different user roles in Resource Manager by assigning an LDAP group to a specific Resource Manager user role.
- The following user types are available:
- Organization Administrator
  - Meeting Operator
  - Meeting Organizer
  - Regular User
  - Default User Type
- By default, all users are assigned the Organization Administrator user role.
- Step 4** Enter the name of an ADS user group in the Selected Groups field, or click the **Select** button in each row to map an ADS user group to each Resource Manager default user type.
- For example, to assign all users in the ADS Organization Administrator user group to the Resource Manager Organization Administrator user role, type “Organization Administrator” in the Selected Groups field next to the Organization Administrator user type.
- You can assign multiple ADS user groups to each Resource Manager user role.
- Resource Manager maps all users that are not assigned to any listed Resource Manager user role to the user role specified in the Default User Type field.
- To instruct Resource Manager not to download users that are not assigned to any listed Resource Manager user role, set the Default User Type field to **Don't Download**.
- Step 5** Click **OK** to save your changes.
-

## Defining Virtual Rooms for All LDAP Users

This section describes how to define a unique virtual meeting room for a specified LDAP user.

Each user can schedule a meeting in his/her own virtual room, or schedule a random meeting. A user cannot schedule a meeting in the virtual room of another user.

A virtual room is created for each user during LDAP synchronization.

To automatically create a virtual room, the following conditions must be met:

- The value of the LDAP field mapped to the virtual room must be numeric.
- The virtual room number for an LDAP server is not editable on the virtual room profile screen.
- If the same virtual room number is defined for two users in the LDAP server, the virtual room is created for only one of the users.

Each virtual room obeys the default settings defined at **Advanced Settings > Default Meeting Settings**.

### Procedure

---

**Step 1** Click **Advanced Settings** in the sidebar menu.

**Step 2** Click **LDAP Configurations**.

**Step 3** Click **Advanced**.

**Step 4** Check **Virtual Room Number** to create a virtual room for all LDAP users.

**Step 5** Select a parameter that you want to use as the virtual room number.

By default, the `telephoneNumber` parameter is used since everyone within an organization should have a unique telephone number.

The resulting virtual room is the concatenation of the Resource Manager Meeting ID prefix and the LDAP field that is used for generating the virtual room number.

**Step 6** Click **OK** save your changes.

---

## Forcing Resource Manager to Use a Virtual Room

This section describes how to force endpoint-initiated ad hoc conferences to be hosted in a predefined virtual room.

### Procedure

---

**Step 1** In the Resource Manager Configuration Tool, go to **System Configuration > Scheduling Settings**.

**Step 2** Check **Allow Only Endpoint Initiated Virtual Room Meetings** to ensure that endpoint-initiated ad hoc conferences can only be hosted within a predefined virtual room.

You cannot create random conferences when **Allow Only Endpoint Initiated Virtual Room Meetings** is checked.

This configuration prevents users from dialing into the system and randomly creating MCU conferences and using up MCU ports. If all virtual rooms are PIN protected, only users who know the virtual room PIN can create endpoint-initiated conferences.



**Note** The **Allow Only Endpoint Initiated Virtual Room Meetings** option is enabled only when the **Allow Endpoint Initiated Multipoint Calls** field is checked.

## Resource Manager LDAP Information Attributes

Table 11-1 lists the LDAP information attributes used by Resource Manager.

**Table 11-1** Resource Manager LDAP Information Attributes

Identifier	Attribute	Description
1	uid	User identifier
2	email	User e-mail address
3	telephone	User telephone number
4	mobile	User mobile telephone number
5	fax	User fax number
6	cn	Full name of user
7	givenName	Given name of user
8	sn	Surname of user
9	company	User company name
10	branch	Branch
11	department	Department
12	country	Country
13	state	State
14	city	City
15	description	Description
16	zipCode	Zip code
17	address	Address



## CHAPTER 12

# Viewing Meeting Schedules in Resource Manager

---

This section is for Meeting Operators and Organization Administrators.

- [Viewing Organization Meetings, page 12-1](#)
- [Viewing the Creation Status of Meetings, page 12-2](#)
- [Viewing the Termination Status of Meetings, page 12-2](#)
- [Searching for a Meeting, page 12-3](#)
- [Monitoring a Meeting, page 12-3](#)
- [Generating Reports, page 12-4](#)
- [Modifying Upcoming Meetings, page 12-5](#)
- [Removing Meetings from the History Tab, page 12-5](#)
- [Viewing Host MCUs, page 12-6](#)
- [Terminating Meetings, page 12-6](#)

## Viewing Organization Meetings

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
  - Step 2** Click **Current** to see all meetings that are currently in progress.
  - Step 3** Click **Upcoming** to see all meetings that have not yet started.
  - Step 4** Click **History** to see all meetings that have already finished.
-

## Viewing the Creation Status of Meetings

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **Current** to see all meetings that are currently in progress.
- Step 3** Click **Upcoming** to see all meetings that have not yet started.
- Step 4** Click **History** to see all meetings that have already finished.

The creation status of each of the displayed meetings is shown in the Status column.

- Green—Successful status
- Orange—Alert status
- Red—Failure status

There are three status indicators in each row

- First (left) status icon—Indicates meeting creation status.  
If meeting creation fails due to device failure, Resource Manager attempts to recreate the meeting whenever it receives a dial-in call from a meeting participant. This allows the system multiple attempts at creating the meeting after initial failure.
- Second (middle) status icon—Indicates participant/terminal status.  
If the second status indicator is red, a participant/terminal is not connected.  
If the second status indicator is orange, a participant/terminal is disconnecting from the meeting.
- Third (right) status icon—Indicates meeting termination status.

- Step 5** To view the Reason Failed error message, click the **red status indicator**, and then click **Retry** to resend the meeting information to the MCU.

If a terminal is disconnected correctly via the In-meeting Control interface, there is no red status indicator.

---

## Viewing the Termination Status of Meetings

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **History** to see all meetings that have already finished.

The termination status of each of the displayed meetings is shown in the Status column.

- Green—Indicates successful termination and all participants successfully exited the meeting.
- Red—Indicates unsuccessful meeting termination or the abnormal exit of a terminal from a meeting.

- Step 3** To view the Reason Failed error message, click the **red status indicator**.
-

# Searching for a Meeting

## Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **Current**, **Upcoming** or **History**, as required.
- Step 3** Perform any of the following:
- Enter the partial or complete subject of the meeting in the Subject field.  
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
  - Enter the E.164 number of an attending terminal in the E164 field.  
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
  - Click the calendar icon in the From field, and select a date and time in the window that opens.  
Meetings scheduled after the selected time are listed.
  - Click the calendar icon in the To field, and select a date and time in the window that opens.  
Meetings scheduled before the selected time are listed.
  - Enter the partial or complete meeting ID in the Meeting ID field.  
If any part of the meeting ID matches the search string, the meeting record is displayed in the search results.
- Step 4** Click **Search**.  
Search results are listed.
- Step 5** To return to the complete list of meetings, clear each of the fields.
- Step 6** Click **Search**.
- 

# Monitoring a Meeting

## Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **Current**.
- Step 3** Click the link in the Subject field for the meeting you want to monitor.
- Step 4** Enter the moderator PIN if one is used for this meeting.
- Step 5** Click the **Take Control** icon.
- The In-meeting Control interface is not available for meetings in which you are not a participant or the organizer.
-

# Generating Reports

On the Upcoming and History tabs, you can generate a report in .csv format which shows all meetings scheduled between selected dates (as specified in the To and From fields). Once you have saved a report, you can view it with Microsoft Excel.

## Procedure

- 
- Step 1** Click **All Meetings** in the sidebar menu.
  - Step 2** Click **Upcoming** or **History**, as required.
  - Step 3** Click the calendar icon in the From and To fields to choose a start and end date for information in the generated report.
  - Step 4** Click **Generate Report**.

[Table 12-1](#) describes the information categories that are included in a generated report.

**Table 12-1** *Generated Report Information Categories*

Category	Description
Virtual Meeting ID	Dialable meeting ID used by users to access a specific meeting.
Master Meeting ID	Corresponds to a physical meeting ID on the master MCU.
Slave Meeting ID	Corresponds to a physical meeting ID on the slave MCU.
Cisco Unified Videoconferencing Manager Meeting ID	Internal database ID for the meeting.
Subject	Corresponds to Subject field in Meeting Scheduling.
Meeting Type	Corresponds to the Meeting Type field in Meeting Scheduling. The name of the meeting type is displayed.
Reference Code	Corresponds to the Reference Code field in Meeting Scheduling.
Start Time	Corresponds to the Start Time field in Meeting Scheduling.
Duration	Corresponds to the Duration field in the Meeting Scheduling.
Meeting Room	Meeting room used for scheduling a meeting.
Organizer Name	Corresponds to the Organizer field in Meeting Scheduling.
Service Prefix	MCU service prefix used for the meeting.
Services	MCU service used for the meeting.
MCU Name(s)	MCUs used for the meeting. For cascaded meetings, “(master)” appears after the MCU name.
Terminals	Number of terminals used for the meeting.
Number of Extra IP Ports Reserved	Corresponds to the Reserve additional ports field in Meeting Scheduling.
Dial-in IP Terminals	Number of dial-in IP terminals.
Dial-out IP Terminals	Number of dial-out IP terminals.
Dial-in ISDN Terminals	Number of dial-in PSTN/ISDN terminals.
Dial-out ISDN Terminals	Number of dial-out PSTN/ISDN terminals.

**Table 12-1** Generated Report Information Categories (continued)

Category	Description
Gateway List	Gateways used for the meeting.
Device Failure Cause (Device Name, IP Failure, Cause)	Any failure on a network device such as an MCU or gateway.
Attendee Failure Cause (Name, Number, ISDN, Dial-in, Total Time, Failing Attempts, Last Failure Cause)	Any failures on attending terminals.

**Step 5** Click **Save** to save the report to a location of your choice.

---

## Modifying Upcoming Meetings

You can reschedule the meeting to another time, change the meeting parameters, or delete the meeting request.

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
  - Step 2** Click **Upcoming**.
  - Step 3** Click the subject of the meeting you want to modify in the In-meeting Control interface.  
The In-meeting Control interface is not available for meetings in which you are not a participant or the organizer.
  - Step 4** Enter the required information.
- 

## Removing Meetings from the History Tab

You can define a rule to instruct Resource Manager to automatically delete past meetings.

### Procedure

---

- Step 1** Open the Resource Manager Configuration Tool.
  - Step 2** Go to **System Configuration > Scheduling Settings**.
  - Step 3** Select **Delete meetings older than** and enter a value in days up to a maximum of 9999 days.  
Meetings older than this date are automatically deleted from the database.
  - Step 4** Click **Save**.
-

## Viewing Host MCUs

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **Current**, **Upcoming** or **History**, as required.
- All host MCUs are listed in the MCU column with an indication of whether the meeting is cascaded.
- 

## Terminating Meetings

You can terminate meetings via the All Meetings section without entering the In-meeting Control interface.

### Procedure

---

- Step 1** Click **All Meetings** in the sidebar menu.
- Step 2** Click **Current**.
- Step 3** Click the icon to the right of the Meeting ID column for a meeting.
-



## CHAPTER 13

# Modifying Default Organization Settings for Resource Manager Users and Meetings

---

- [About Settings Priorities, page 13-1](#)
- [How to Define Default Settings for Organization Users, page 13-1](#)
- [How to Define Default Settings for Meetings, page 13-3](#)
- [Modifying the Look and Feel of the Resource Manager Web User Interface, page 13-7](#)
- [Provisioning Resource Manager Users via a Directory Server, page 11-1](#)

## About Settings Priorities

When configuring advanced settings, note the following priority rules:

- Changes to an individual user profile override default settings
- Settings you make for a meeting during scheduling override settings in a virtual room
- Settings in a virtual room override default meeting settings

## How to Define Default Settings for Organization Users

- [Defining Which Meeting Types are Available to New Users, page 13-1](#)
- [Defining a Default Time Zone for a User, page 13-2](#)
- [Defining Display Formats, page 13-2](#)
- [Defining Date Display Formats, page 13-3](#)
- [Defining Your Meeting Display Preferences, page 13-3](#)

## Defining Which Meeting Types are Available to New Users

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default User Settings**.

- Step 3** Select a meeting type in the Available Meeting Types list that you want to make available to new users.
- Step 4** Use the right-pointing arrow to move the meeting type to the Selected Meeting Types list.  
We recommended that you select all available meeting types.  
Non-Video Conference and Point-to-Point meeting types are default meeting types in Resource Manager. They do not exist on the MCU.
- Step 5** If you want all users to have access to the selected meeting types, select **Update Meeting Types for All Users Now**.  
All user profiles are updated to reflect the new default values.
- Step 6** Deselect **Update Meeting Types for All Users Now** if you want only new users to have access to the selected meeting types.  
When you save the settings, only default settings in the profiles of new users change.
- Step 7** Click **OK** to save your changes.
- 

## Defining a Default Time Zone for a User

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default User Settings**.
- Step 3** Select a default time zone for the selected meeting types.
- Step 4** Select **Update All Users Now** if you want the default time zone to appear for all users.
- Step 5** Deselect **Update All Users Now** if you want the default time zone to appear for new users only.
- Step 6** Click **OK** to save your changes.
- 

## Defining Display Formats

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default User Settings**.
- Step 3** Select an option from the Name Display Format list to change the way user names are displayed in meeting-related information and in the meeting video display.
- Step 4** Select **Last name** or **First name** from the Sort by list to change the sort order for participant name columns.
- Step 5** Click **OK** to save your changes.
-

## Defining Date Display Formats

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Default User Settings**.
  - Step 3** Select an option from the Date Display Format list to change the way dates are displayed in meeting-related information and in the meeting video display.
  - Step 4** Click **OK** to save your changes.
- 

## Defining Your Meeting Display Preferences

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Default User Settings**.
  - Step 3** Click **Display all meeting records on My Meetings screens** to display all meetings within the organization in My Meetings.
  - Step 4** Click **OK** to save your changes.
- 

## How to Define Default Settings for Meetings

On the Default Meeting Settings tab, the Organization Administrator sets which default values are available to users when scheduling meetings or defining virtual rooms.

When a new meeting is scheduled, default settings configured in the Default Meeting Settings tab also appear in the Meeting Scheduling tab.

- [Defining a Default Meeting Type, page 13-4](#)
- [Defining the Default Cascading Mode, page 13-4](#)
- [Defining How to End a Meeting, page 13-4](#)
- [Defining the Meeting Default Length, page 13-5](#)
- [Defining the Default Dialing Mode, page 13-5](#)
- [Defining a Billing Destination, page 13-5](#)
- [Defining Required Default Resources, page 13-6](#)

## Defining a Default Meeting Type

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Default Meeting Settings**.
  - Step 3** Select a default meeting type from the Meeting Type list or all new meeting templates and new meetings.
  - Step 4** Click **OK** to save your changes.
- 

## Defining the Default Cascading Mode

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
  - Step 2** Click **Default Meeting Settings**.
  - Step 3** Set Allow Cascaded Meeting to **Yes** to enable Resource Manager to automatically create cascaded meetings on the MCUs.  
  
Set to No to instruct Resource Manager to create only meetings no larger than the capacity of a single MCU/EMP card. Resource Manager will not cascade two MCU conferences together to increase conference size or save network bandwidth.  
  
When set to No, the Prioritize field is disabled.
  - Step 4** From the Prioritize list, select the priority by which meetings are scheduled and which is used in meeting templates by default. This is an important factor in creating efficient conferences. The options are
    - Local MCU
    - Bandwidth
    - Delay (for more information, see the [“Configuring Cascading” section on page 4-1](#))
  - Step 5** Click **OK** to save your changes.
- 

## Defining How to End a Meeting

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.
- Step 3** Select **At scheduled time** to terminate the meeting according to the termination time define for the meeting.
- Step 4** Enter a value in the **Alert n minutes before termination** field to indicate the length of time before the scheduled termination of the meeting that terminals receive the end-of-meeting warning.

At the defined length of time before the end of the meeting, an audio alert message is played to the meeting participants. The only way to extend the meeting is to do it manually in the In-meeting Control screen.

- Step 5** Select **n minutes after all terminals have left** to terminate the meeting only a defined period of time after the last terminal leaves.
- Resource Manager automatically extends the meeting as long as meeting participants are still connected to the meeting, and there is no resource conflict with upcoming scheduled meetings.
- Step 6** Enter the required value in the **n minutes after all terminals have left** field.
- By default, you cannot automatically extended Resource Manager meetings to last more than 4 hours. Administrators can change this default via Resource Manager Configuration Tool > System Configuration > Scheduling Settings > Maximum Length of Meeting Extension.
- Step 7** Click **OK** to save your changes.
- 

## Defining the Meeting Default Length

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.
- Step 3** Enter the default length of a meeting in minutes in the Duration field.
- Step 4** Click **OK** to save your changes.
- 

## Defining the Default Dialing Mode

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.
- Step 3** Select **Dial-out** or **Dialing-in** from the Default Dialing Mode list.
- Step 4** Click **OK** to save your changes.
- 

## Defining a Billing Destination

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.

- Step 3** Select **Host**, **All Participants** or **Organizer** in the Bill To field.  
If the host and the organizer are the same person, the Organizer option does not appear.  
The cost of the meeting is billed accordingly.  
The selection in the Bill To field determines the default setting in the Virtual Room and Meeting Scheduling screens.
- Step 4** Click **OK** to save your changes.
- 

## Defining Required Default Resources

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.
- Step 3** From the Required list, select the default resources required for the meeting to be confirmed. A meeting is not allowed if these resources are not available at the time of the meeting.  
You can choose to require that participating users, rooms, or terminals cannot be double booked for a meeting before you can successfully schedule a meeting.
- Step 4** Click **OK** to save your changes.
- 

## Customizing Invitation E-mail

You can customize the content of the invitation e-mail that participants receive when a meeting is scheduled, modified or cancelled.

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Default Meeting Settings**.
- Step 3** (Optional) Select **Customize the 'meeting invitation' introduction message** and then enter your text to override the introduction message in the initial meeting invitation e-mail.
- Step 4** (Optional) Select **Customize the 'meeting update' introduction message** and enter your text to override the introduction message in the meeting update e-mail.
- Step 5** (Optional) Select **Customize the 'meeting cancellation' introduction message** and enter your text to override the introduction message in the meeting cancellation e-mail.
- Step 6** (Optional) Select **Override IP Terminal Access Information** and enter your text to override default access information for IP terminals.
- Step 7** (Optional) Click **Meeting ID** to insert meeting ID placeholders into the text.
- Step 8** (Optional) Select **Override ISDN/PSTN/Mobile Terminal Access Information** and enter your text to override default access information for ISDN/PSTN/Mobile terminals.

Default access information for ISDN/PSTN/Mobile terminals consists of access information for all gateways configured in Resource Manager.

- Step 9** (Optional) Click **Meeting ID** to insert meeting ID placeholders into the text.
  - Step 10** (Optional) Select **Hide the Attendees list** to hide the attendees section in the invitation e-mail.
  - Step 11** (Optional) Select **Hide dial-in information for attendees** to hide only the dial-in access information for each attendee when Hide the Attendees list is deselected.
  - Step 12** Click **OK** to save your changes.
- 

## Modifying the Look and Feel of the Resource Manager Web User Interface

### Procedure

---

- Step 1** Click **Advanced Settings** in the sidebar menu.
- Step 2** Click **Look and Feel**.
- Step 3** Use the **Meeting Scheduling button** list to select either of two different ways to schedule the three types of meetings supported by Resource Manager.
  - **One Button**—When the user clicks Meeting Scheduling in the sidebar menu, the Basic tab appears.
  - **Sub Menu**—When the mouse is over Meeting Scheduling in the sidebar menu, a sub-menu appears that contains three scheduling options: Normal, Recurrence, and Ad-Hoc.
- Step 4** Select **Visible** or **Hidden** to determine whether the following fields are displayed or hidden at Meeting Scheduling > Basic:
  - PIN
  - Waiting Room
  - Record Meeting
  - Streaming
  - Description
  - Bill To
  - Reference Code
- Step 5** Select **Visible to Meeting Organizer** or **Hidden from Meeting Organizer** to determine whether the Attendees Settings tab, the Attendees Availability tab and the Advanced tab are displayed or hidden on the Meeting Scheduling tab.
- Step 6** Use the Invite Attendees By field to indicate whether to invite users or terminals by default at Meeting Scheduling > Invite.
- Step 7** Select **Visible** or **Hidden** to determine whether the Reserved Ports field is displayed or hidden at **Meeting Scheduling > Invite**.
- Step 8** Select **Visible** or **Hidden** to determine whether the Reserve Additional Ports field is displayed or hidden at Meeting Scheduling > Invite.

- Step 9** Select **Visible** or **Hidden** to determine whether the Attendees Settings tab, the Attendees Availability tab and the Advanced tab are displayed or hidden on the Meeting Scheduling tab.
- Step 10** Select **Visible** or **Hidden** to determine whether the PSTN/ISDN and Dial-in columns are displayed or hidden at Meeting Scheduling > Attendees Settings.
- Step 11** Determine whether attendee terminal settings are editable or read-only at Meeting Scheduling > Attendees Settings. The Attendee Terminal Settings option determines whether or not a meeting organizer can change the default association between an attending user and his/her default terminal when scheduling a meeting.
- Step 12** Select **Visible** or **Hidden** to determine whether the following are displayed or hidden at Meeting Scheduling > Advanced:
- Bill To
  - Reference Code
  - Customize Reference Code Field Label—Determines the label used for the Reference Code field.
  - Enforce Reference Code Entry—Determines whether or not the reference code is mandatory.
  - Field Type—Determines the type of content that can be entered in the Reference Code Entry field.
  - Field Length—Determines the length of the value entered in the Reference Code field.
  - Enforce Full Length—Determines whether or not the full Reference Code field length is used.
- Step 13** Select **Visible** or **Hidden** to determine whether the following are displayed or hidden in the In-meeting Control interface:
- Statistics tab
  - Extend Meeting option
  - Terminal Invitation option
  - Advanced Invitation tab
  - Terminate Meeting option
  - Layout Control—Determines whether the layout control panel is displayed or hidden.
  - Hide Meeting Room—Determines whether or not the Meeting Room tab is hidden in the Resource Management section.
  - Hide Meeting Notification E-mail for meeting rooms and terminals—Determines whether or not e-mail and time zone fields for meeting rooms and terminals are enabled. If meeting rooms and terminals are enabled, they can directly receive notification e-mails.
  - Show My Profile—Determines whether or not the My Profile section is displayed.
  - Enable Personal Address Book—Determines whether or not the Address Book section is displayed.
  - Play a sound upon scheduling failure—Plays a warning sound in the event of a meeting scheduling failure.
  - Use Full Screen Display—Determines whether or not the Resource Manager user-interface is displayed full-screen after login.
- Step 14** Click **OK** to save your changes.
-



## CHAPTER 14

# Using the Resource Manager Configuration Tool

---

During initial installation of Cisco Unified Videoconferencing Manager, defined network environment settings and other configurable elements, such as page length and meeting identifiers, are set to default values. This enables Resource Manager to run upon installation without the need for additional configuration.

The Resource Manager Configuration Tool, a client-server application based on Java™ Web Start, enables the system administrator to configure Resource Manager system settings, set CDR preferences, and modify default value settings.

- [Setting Up the Java Runtime Environment, page 14-2](#)
- [Launching the Configuration Tool, page 14-2](#)
- [Retrieving an Administrator Password, page 14-3](#)
- [Uninstalling the Resource Manager Configuration Tool, page 14-3](#)
- [How to Modify General Settings, page 14-3](#)
- [How to Modify Scheduling Settings, page 14-7](#)
- [Hiding Resource Manager User Interface Screens, page 14-10](#)
- [How to Manage Custom Time Zones, page 14-11](#)
- [Customizing Product and Vendor Logos, page 14-13](#)
- [Creating a Customized Billing Field, page 14-13](#)
- [Defining Database Server Settings, page 14-14](#)
- [How to Define Security Settings, page 14-14](#)
- [How to Define Call Data Record \(CDR\) Settings, page 14-16](#)

# Setting Up the Java Runtime Environment

Install Java Runtime Environment on the client machine before using the Resource Manager Configuration Tool.

## Procedure

---

- Step 1** Go to **http://cuvcmrm\_serverhost:port/cuvcmrm-config**.
- The first time you access the Resource Manager Configuration Tool, it detects whether or not Java Runtime Environment is installed on the client machine (such as the user's computer).
- If Java Runtime Environment is not installed on the client machine, a download message appears.
- Step 2** Click **Install Java Runtime Environment**.
- Step 3** Click **download** on the Java download web page.
- The Java Runtime Environment is installed on the client machine (your computer).
- To return to the Resource Manager Configuration Tool, in the Java download web page, click **previous page**.
- 

# Launching the Configuration Tool

The Resource Manager Configuration Tool is accessible from any client machine on which the Java Web Start application is installed.

## Procedure

---

- Step 1** Go to **http://cuvcmrm\_serverhost:port/cuvcmrm-config**.
- The Resource Manager Configuration Tool launch page appears.
- Step 2** Click **Launch Resource Manager Configuration Tool**.
- The Resource Manager Configuration Tool checks for the latest version of the Java Web Start application on the client machine, and then starts the Resource Manager Configuration Tool.
- Step 3** If a warning message appears stating that the digital signature is invalid and asking if you want to run the application, click **Run**.
- To avoid the appearance of this message upon launch of the Resource Manager Configuration Tool from the same site address, in the message window, click **Always trust content from this publisher**, and then click **Run**.
- Step 4** Click **Launch Resource Manager Configuration Tool** on the Resource Manager launch page.
- Step 5** Enter the login and password of the Service Provider Administrator or Organization Administrator.
- Step 6** Click **Login**.
- The Resource Manager Configuration Tool window opens.
-

## Retrieving an Administrator Password

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool login window, click the down arrow to open the lower part of the login window.
- Step 2** Enter the administrator login ID in the Send Admin Password for Login ID field.
- Step 3** Click **Send** to send the administrator password to the e-mail address associated with the login ID.
- 

## Uninstalling the Resource Manager Configuration Tool

### Procedure

---

- Step 1** Go to **Start > Settings > Control Panel > Add or Remove Programs** on the client machine.
- Step 2** Select **Resource Manager Configuration Tool**, and click **Remove**.
- 

## How to Modify General Settings

- [Defining E-Mail Server Settings, page 14-4](#)
- [Defining the Unconnected Endpoint Timeout Period, page 14-4](#)
- [Defining Table Row Display, page 14-5](#)
- [Defining the Command Delay, page 14-5](#)
- [Defining the Parent Zone Authorization Filter, page 14-5](#)
- [Defining the Log Level, page 14-6](#)
- [Defining the In-Meeting Control Refresh Rate, page 14-6](#)
- [Defining the Resource Manager Server Name and Web Port, page 14-6](#)
- [Defining the Online Help Host URL, page 14-7](#)

## Defining E-Mail Server Settings

You can define settings that are used by Resource Manager to send e-mail notifications, such as meeting reservations and meeting updates, to users and administrators.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
- Step 2** Enter the e-mail server IP address or domain name in the Host field.
- Step 3** Enter the e-mail server communications port in the Port field.
- Step 4** Enter the e-mail server Login ID and password in the relevant fields to enable access to the e-mail server.
- Step 5** Select **E-mail meeting organizer upon** to send an e-mail notification to the meeting organizer in the event of a meeting failure.
- Step 6** Select one or more of the following meeting-failure check boxes:
- Meeting creation
  - EP abnormal connection
  - EP connection
  - Dial-in considered—This check box is only active if you check **EP connection**.
- If you check **Dial-in considered**, dial-in connections are considered as endpoints and e-mail notifications are sent in the case of a dial-in connection failure.
- Step 7** Click **Save**.
- 

## Defining the Unconnected Endpoint Timeout Period

If an endpoint does not respond within the designated timeout period to a connection request, the system classifies the endpoint as unconnected.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
- Step 2** Enter a value in seconds in the EP Unconnected Time Out field.
- Step 3** Click **Save**.
-

## Defining Table Row Display

You can define the number of rows that are displayed in Resource Manager tables.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
  - Step 2** Enter a value in the Number of table rows per page field.
  - Step 3** Click **Save**.
- 

## Defining the Command Delay

You can define the amount of time that Resource Manager waits between the sending of internal messages to the MCU.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
  - Step 2** Enter a value in milliseconds in the Delay between two commands from Resource Manager to MCU field.  
  
Enter 0 for deployments consisting of version 5.x MCUs only.  
Enter 100 for deployments containing version 4.x MCUs.
  - Step 3** Click **Save**.
- 

## Defining the Parent Zone Authorization Filter

The setting is only applicable when working with the Cisco IOS H.323 Gatekeeper. In a hierarchical mode, this setting determines whether or not the parent zone prefix should be added when going from a child gatekeeper to a parent gatekeeper during multi-zone navigation. This is useful for Resource Manager to determine the dial-out string when a terminal is invited.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
  - Step 2** Select the Enable Parent Zone Authorization Filter field.
  - Step 3** Click **Save**.
-

## Defining the Log Level

You can select from three levels of detail for a log file. The more detailed a log file, the larger the log file.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
- Step 2** Select one of the following options in the Log Level field:
- **WARN**—This is the standard, recommended setting in most cases.
  - **INFO**—This setting includes more detailed information in the log file.
  - **DEBUG**—This setting includes issue details in the log file and produces the most detailed log.
- Step 3** Click **Save**.
- 

## Defining the In-Meeting Control Refresh Rate

You can define the time interval between refreshes of the In-meeting Control interface.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
- Step 2** Enter the number of seconds that the In-meeting Control interface is displayed before the next refresh in the Refresh In-Meeting Control window every n seconds field.
- Step 3** Click **Save**.
- 

## Defining the Resource Manager Server Name and Web Port

You can define the server name and Web port after installation.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
- Step 2** Enter the server name and Web port in the Server URL address for the In-Meeting Control URL link field in the format `http://<server_URL>:port_number<`.
- Step 3** Click **Save**.
-

## Defining the Online Help Host URL

You can point the online help files to a remote URL. We recommend that you do not customize the online help host URL without making a copy of the target online help files.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > General Settings**.
  - Step 2** Enter the remote URL in the Online Help Host URL field.
  - Step 3** Click **Save**.
- 

## How to Modify Scheduling Settings

- [Changing Call Authorization Settings, page 14-7](#)
- [Dynamically Cascading Multiple EMPs for a Single Conference, page 14-8](#)
- [Modifying Default Meeting Settings, page 14-9](#)
- [Modifying Default Recurring Meeting Settings, page 14-10](#)

## Changing Call Authorization Settings

When Resource Manager and Cisco IOS H.323 Gatekeeper are working in authorization mode, Resource Manager can restrict endpoint-initiated conferences with settings in this section to prevent uncontrolled and unmanaged access in a video conference network.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Scheduling Settings**.
  - Step 2** Unselect **Allow Endpoint Initiated Point to Point Calls** to prevent endpoint-initiated point-to-point calls.
  - Step 3** Unselect **Allow Endpoint Initiated Multipoint Calls** to prevent endpoint-initiated MCU calls.
  - Step 4** Select **Allow Only Endpoint Initiated Virtual Room Meetings** to ensure that the endpoint-initiated MCU calls must use a defined virtual room.

The Allow Only Endpoint Initiated Virtual Room Meetings option is enabled only when the Allow Endpoint Initiated Multipoint Calls field is checked.



---

**Note** You cannot create random endpoint-initiated conferences when Allow Only Endpoint Initiated Virtual Room Meetings is checked.

---

**Step 5** Select **Allow Advanced Virtual Room Management for Meeting Organizer** to enable Meeting Organizers to have multiple virtual rooms. When checked, a meeting organizer can have multiple virtual rooms under his or her user profile. The Basic and Invite tabs are also displayed under the Virtual Room Profile screens.

Only Administrators can add a new virtual room for a Meeting Organizer. A Meeting Organizer can only delete or modify his or her existing virtual rooms.

By default, **Allow Advanced Virtual Room Management for Meeting Organizer** is unchecked. Each Meeting Organizer can have a single virtual room only, and only the virtual room Basic tab is displayed.

Administrators and Meeting Operators can always have multiple virtual rooms and the virtual room Basic and Invite tabs are both displayed by default.



**Note** If a Meeting Organizer already has more than one virtual room, even if the Allow Advanced Virtual Room Management for Meeting Organizer is unchecked, a full list of the user's virtual rooms is displayed as well as all of the virtual room's configuration tabs.

**Step 6** Click **Save**.

---

## Dynamically Cascading Multiple EMPs for a Single Conference

To allow an existing endpoint-initiated ad hoc meeting to grow beyond the size of a single EMP, you can instruct Resource Manager to dynamically cascade additional EMPs to this meeting when the number of available ports on the EMP reaches the value you define.

On reaching this value, Resource Manager creates a new meeting on another EMP when a new call joins the meeting. Resource Manager then cascades this new meeting to the original meeting.

Dynamic cascading is only available for video meetings using EMPs. An endpoint-initiated ad hoc audio meeting will only grow to the size of a single MCU blade.

### Procedure

---

**Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Scheduling Settings**.

**Step 2** Enter a positive number in the Reserve Port on MVP for dynamic cascading field.

We recommend 1 or 2 ports.

**Step 3** Click **Save**.

---

## Modifying Default Meeting Settings

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Scheduling Settings**.
- Step 2** Select **Use MCU Meeting ID** to work with the MCU conference ID instead of the Resource Manager conference ID.
- This option is meant to work when Resource Manager and Cisco IOS H.323 Gatekeeper are not working in authorization mode, and all meetings dial out to their meeting participants.
- Step 3** Enter a value for the number of characters allowed in meeting ID strings in the Meeting ID Length field.
- Step 4** Enter a numeric value for the meeting prefix in the Meeting ID Prefix field.
- The prefix must be shorter than the number specified in the Meeting ID Length field.
- Step 5** Enter a value in minutes in the Duration of Endpoint Initiated Calls field to set the maximum duration of endpoint-initiated calls.
- The default value is 30 minutes. Resource Manager uses this value in resource allocation and meeting creation.
- Step 6** Select **Dial-in** or **Dial-out** from the Default Dialing Mode list.
- If you select Dial-in, meeting participants enter a meeting by dialing into the meeting.
- If you select Dial-out, the Resource Manager system dials out to meeting participants.
- Step 7** Select **Remove ad hoc participants when disconnected from conference** to enable ad participants not on the original invited list to be kept in the In-Meeting Control screen after they disconnect.
- This is useful for endpoint initiated ad-hoc conference where Resource Manager will remove a participant from the conference list when the participant disconnects.
- If you unselect this field, and disconnected participants are still kept in the In-Meeting Control participant list, such participants still use MCU ports even though they are no longer connected. This option is useful for managed conferences where a meeting operator can determine which disconnected participants should be removed from the meeting and do so manually.
- Step 8** Enter a value in minutes in the Launch Meetings <n> Minutes before scheduled start field to specify the amount of time prior to the scheduled start of a meeting that the meeting actually begins.
- If the early start attempt fails, Resource Manager attempts to create this meeting again at the regular scheduled start time.
- Step 9** Select **Delete meetings older than** and enter a value in days up to a maximum of 9999 days to define the length of time a meeting appears in the Cisco Unified Videoconferencing Manager web interface.
- Step 10** Enter a value in minutes in the Meeting Auto Extend Length field to define the length of time that a meeting can be extended after the scheduled end of the meeting.
- Step 11** Select **Waiting Room Timeout** and enter a value in the <n> Minutes After The Waiting Room Start field to define the length of time a meeting can remain in Waiting Room mode until the meeting host joins.
- If the host does not join within the specified period of time, the meeting ends.

- Step 12** Enter a value in the Maximum Length of Meeting Extension field to specify the maximum length of time that you want to allow for extending a meeting.
- The maximum values that Resource Manager allows are 10 days, 240 hours and 14400 minutes.
- Step 13** Click **Save**.
- 

## Modifying Default Recurring Meeting Settings

You can modify the default number of days in advance that a recurring meeting can be scheduled.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Scheduling Settings**.
- Step 2** Enter a value in days in the Schedule Recurring Meetings field.
- The maximum value is 730 days (2 years).
- Step 3** Click **Save**.
- 

## Hiding Resource Manager User Interface Screens

You can simplify the Resource Manager web interface by defining which screens in the following sections of the Resource Manager user interface are hidden from administrators and users.

- IP Topology in Admin > Network Management
- Gatekeeper Definition > Gatekeeper/SIP server tab in Admin > Resource Management > Gatekeeper/SIP server
- Gateway Definition tab in Admin > Resource Management
- ISDN Topology tab in Admin > Network Management. The ISDN Topology tab is only displayed when the gateway is enabled
- Terminal Definition tab in Admin > Resource Management
- All Meetings section accessible via the Admin sidebar menu
- User Management section accessible via the Admin sidebar menu
- Advanced Settings section accessible via the Admin sidebar menu.
- Other Settings tab in the Scheduling a New Meeting and in Meeting Details windows.
- Customization Tool button on upper-right of the application window that provides access to the Customization Tool window in which you can customize terminology in the Resource Manager web interface.
- Meeting Scheduling and Meeting Templates sections accessible via the User sidebar menu.
- My Meetings section accessible via the User sidebar menu.

**Procedure**

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > UI Settings**.
- Step 2** Select the screens you wish to show.
- Step 3** Unselect the screens you wish to hide.
- Step 4** Click **Save**.
- 

## How to Manage Custom Time Zones

- [Selecting a Time Zone Profile, page 14-11](#)
- [Viewing a Time Zone Profile, page 14-11](#)
- [Adding Daylight Saving to a Time Zone Profile, page 14-12](#)
- [Creating a Customized Time Zone Profile, page 14-12](#)
- [Removing a Customized Time Zone Profile, page 14-12](#)
- [Reverting to Default Time Zone Settings, page 14-13](#)

## Selecting a Time Zone Profile

Only selected time zones are displayed in the web interface in the user, terminal, and meeting time zone fields. You can define a subset of all available time zones in the Selected Time Zones list. This enables you to expose only the relevant time zones to the end users in the web interface.

**Procedure**

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
- Step 2** Select a time zone in the Available Time Zones list.
- Step 3** Click the right-pointing arrow to move the time zone to the Selected Time Zones list.
- Step 4** Click **Save**.
- 

## Viewing a Time Zone Profile

**Procedure**

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
- Step 2** Double-click a time zone in either the Available Time Zones list or the Selected Time Zones list.
-

## Adding Daylight Saving to a Time Zone Profile

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
  - Step 2** Double-click a time zone in either the Available Time Zones list or the Selected Time Zones list.
  - Step 3** Select **Observer Daylight Saving**.
  - Step 4** Add a daylight saving duration in minutes.
  - Step 5** Configure daylight saving start and end dates and times.
  - Step 6** Click **Save**.
- 

## Creating a Customized Time Zone Profile

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
  - Step 2** Click **New** below either the Available Time Zones list or the Selected Time Zones list.
  - Step 3** Enter a name and time difference from GMT for the new time zone.  
You cannot change a time zone name you have saved the time zone profile.  
If you create a custom time zone profile that has the same name as a default time zone profile, the new custom profile overrides the settings of the default time zone.
  - Step 4** (Optional) Select **Observer Daylight Saving**.
  - Step 5** (Optional) Add a daylight saving duration in minutes.
  - Step 6** (Optional) Configure daylight saving start and end dates and times.
  - Step 7** Click **Save**.
- 

## Removing a Customized Time Zone Profile

You can remove a time zone profile that you have added to either the Available Time Zones list or the Selected Time Zones list.

### Procedure

- 
- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
  - Step 2** Select a custom defined time zone from either the Available Time Zones list or the Selected Time Zones list.

- Step 3** Click **Remove** below the Available Time Zones list or the Selected Time Zones list.
  - Step 4** Click **Yes**.
  - Step 5** Click **Save**.
- 

## Reverting to Default Time Zone Settings

You can undo your changes if you have not yet clicked **Save**.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
  - Step 2** Move, modify or create time zone profiles.
  - Step 3** Click **Reset** to undo your changes.
- 

## Customizing Product and Vendor Logos

You can change the Resource Manager product logo via Admin > Advanced Settings > Look and Feel.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
  - Step 2** Enter the name of a file that contains the logo in the Product logo file name field, or click **Browse** to select the file.  
  
The logo must be a .gif file with a maximum height of 45 pixels and a maximum width of 250 pixels.
  - Step 3** Enter a URL for the company that provides the branded logo and can authorize its use in the URL field.
  - Step 4** Select **Reset to Default** to restore the default vendor logo.
  - Step 5** Click **Save**.
- 

## Creating a Customized Billing Field

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Customized Settings**.
- Step 2** Select a display rule for your billing field from the Billing Code Field Property list.

- Step 3** Select **Customized Field Label** and enter a name for your billing field in the text box that becomes active.
  - Step 4** Enter the maximum number of characters allowed in your billing field in the Field Length field.
  - Step 5** Select **Enforce Full Length** to restrict the length of your billing field to the value set in the Field Length field.
  - Step 6** Select an input type for your billing field from the Field Type list.
  - Step 7** Enter an identifier for your billing field in the Field Value field.
  - Step 8** Click **Save**.
- 

## Defining Database Server Settings

### Procedure

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Database Settings**.
  - Step 2** Enter the default database server name in the Server name field.  
The port number in use by the database server automatically appears in the Server Port field.
  - Step 3** Enter the account name used by Resource Manager to connect to the database in the Connection Account field.  
“Root” appears by default.
  - Step 4** Enter a password in the Connection Password field for use by Resource Manager when a connection to the database server is established.
  - Step 5** Click **Test**, to verify that the database configuration is correct.  
A message window shows the test results.
  - Step 6** Click **Reset** to revise your configured database server settings.
  - Step 7** Click **Save**.
  - Step 8** Restart Resource Manager to apply your changes.
- 

## How to Define Security Settings

- [Defining Password Settings, page 14-15](#)
- [Defining a Login Message, page 14-15](#)
- [Unlocking a User Account, page 14-15](#)

## Defining Password Settings

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Security Settings**.
  - Step 2** (Optional) Select **Display password in user profile** and **Modify password in user profile** as required.
  - Step 3** (Optional) Select **Allow only secure passwords** if required.
  - Step 4** (Optional) Define the minimum allowed password length, password validity period, and number of allowed login attempts in the relevant fields.
  - Step 5** (Optional) Enter the number of previous passwords that are considered when processing a new password in the **Cannot be the same as the last <n> password(s)** field.
  - Step 6** Click **Save**.
- 

## Defining a Login Message

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Security Settings**.
  - Step 2** Select **Display login message** and enter a login message in the text box that becomes active.
  - Step 3** Click **Save**.
- 

## Unlocking a User Account

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **System Configuration > Security Settings**.
  - Step 2** Enter the login ID of the locked user account in the Please enter the User ID that you want to unlock field.
  - Step 3** Click **Unlock**.
  - Step 4** Click **Save**.
-

# How to Define Call Data Record (CDR) Settings

Resource Manager creates and stores Call Data Records (CDRs) in XML format. CDRs contain comprehensive records of each call. These records are useful for analyzing and tracking system use, as well as for supporting diagnostics and billing.

- [Creating CDR Information in XML Format, page 14-16](#)
- [Defining Required Terminal Connection Duration, page 14-16](#)
- [Defining a CDR File Prefix, page 14-17](#)
- [Defining How Often CDRs Are Produced, page 14-17](#)
- [Enabling Streaming to a Radius Server, page 14-17](#)

## Creating CDR Information in XML Format

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **CDR Configuration**.
- Step 2** Select **Enable XML CDR**.
- Step 3** Enable CDRs for meeting scheduling, rescheduling and/or cancellation.
- Step 4** Click **Save**.
- 

## Defining Required Terminal Connection Duration

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **CDR Configuration**.
- Step 2** Enter a value in seconds in the Minimum connection required to produce CDR field for the minimum length of time a terminal must be connected before an entry for that terminal is created in the Actual Information section of the CDR.
- If the terminal is connected to a meeting for the specified minimum time or longer, the CDR records the actual connection time as the total connection time for that terminal.
- If a terminal is connected to a meeting for less than the specified minimum time, the CDR records the total connection time for that terminal as zero.
- Step 3** Click **Save**.
-

## Defining a CDR File Prefix

A standard Resource Manager installation creates a directory called Resource Manager in the Program Files directory. For example, C:\Program Files\Cisco Cisco Unified Videoconferencing Manager\Resource Manager.

CDR files are stored in a default sub-directory called cdrdata. For example, C:\Program Files\Cisco Cisco Unified Videoconferencing Manager\Resource Manager\cdrdata\cdrfilename.xml.

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **CDR Configuration**.
  - Step 2** Enter a prefix in the File prefix name field.  
The prefix appears at the beginning of the CDR file name.  
The default prefix is “cdr”.
  - Step 3** Click **Save**.
- 

## Defining How Often CDRs Are Produced

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **CDR Configuration**.
  - Step 2** Select **One file per meeting** to create one CDR file for each meeting occurrence.
  - Step 3** Select **One file every day** to create a CDR file containing information for every scheduled meeting within a 24-hour period.  
This is the default selection.
  - Step 4** Click **Save**.  
CDR file names are labeled by date, followed by a sequential identifier. Filename suffixes are sequential regardless of how often a CDR is produced, and even if a different CDR production-time option is selected.
- 

## Enabling Streaming to a Radius Server

### Procedure

---

- Step 1** In the Resource Manager Configuration Tool interface, click **CDR Configuration**.
- Step 2** Select **Use RADIUS server**.
- Step 3** Define the Radius server IP address and port in the relevant fields.
- Step 4** Enter a password for the Radius server in the Shared Secret field.

Resource Manager and the Radius server exclusively use the shared secret password as part of the security system.

**Step 5** Click **Save**.

If you do not select **Use RADIUS server**, the IP Address, Port and Shared Secret fields include read-only information by default.

---



# CHAPTER 15

## CDR XML Tags and Attributes

---

The production and storage of CDR (Call Data Records) in Resource Manager is enabled via the Resource Manager Configuration Tool. A CDR file is generated each day by default.

CDR records are saved in XML format and provide comprehensive records of each call which can then be used for analysis of the system for diagnostic and billing purposes.

This section details the XML tags used to label data in the stored CDR .xml file, the attributes of each configurable tag, and the order in which the tags are arranged.

- [Accessing the CDR XML Files, page 15-1](#)
- [Index of CDR XML Tags, page 15-1](#)
- [Understanding the CDR XML Tags, page 15-7](#)



### Note

---

All references to “VCS” in this section are equivalent to “Resource Manager”.

---

## Accessing the CDR XML Files

### Procedure

---

**Step 1** From the Windows Start menu, select **Programs > Cisco Unified Videoconferencing Manager > CDR files**.

**Step 2** Open the relevant CDR file.

The information configured to appear is listed within the tags. For a list of the XML tags that can appear in the CDR, see [Figure 15-1](#).

---

## Index of CDR XML Tags

This section contains a list of all XML tags in the CDR, listed in their hierarchical relationship to each other.



### Note

---

In the tags, “conference” is equivalent to “meeting”, and “service” is equivalent to “meeting type”.

---

**Figure 15-1** Index of CDR XML Tags

```

<conferences>
  <ConferenceData>
    <Event>
      <Scheduling-Data>
        <Conference>
          <Basic-Information>
            <Conference-ID />
            <Virtual-Conference-ID />
            <Master-Conference-ID />
            <Slave-Conference-ID-List>
              <Slave-Conference-ID />
              <Slave-Conference-ID-List />
            <Subject />
            <Reference-Code />
            <Description />
            <MultiPoint-PointToPoint />
            <Scheduled-Adhoc />
            <Start-Time />
            <Duration />
            <Server-TimeZone />
            <Auto-Extend />
            <Bill-To/>
            <Billing-Code/>
          <Basic-Information/>
          <Advanced-Information>
            <Extra-Ports-Reserved>>
            <Priority />
            <DateTime-Scheduled />
            <DateTime-Cancelled />
            <Streaming-Recording-Activated/>
            <Export-Upon-Completion/>
            <Streaming-Target-File-Name/>
            <Streaming-Recording-View/>
          <Advanced-Information/>
          <Conference-Lifecycle-Summary>
            <Resources-Scheduled>
              <DateTime-Modified />
              <Total-IP-Bandwidth />
              <Total-ISDN-Bandwidth />
              <Total-MCU-Connections-Number />
              <Total-GW-Connections-Number />
            </Resources-Scheduled>
          </Conference-Lifecycle-Summary>
        </Conference>
      </Scheduling-Data>
    </Event>
  </ConferenceData>
</conferences>

```

```
<Max-Frame-Rate-Out />
<Max-Picture-Format-In />
<Max-Picture-Format-Out />
<Max-T120-Ports-Reserved />
<Max-Subconferences />
</Conference-Service>
<Resources-Scheduled-At-Time-Of-Conference>
  <Total-IP-Bandwidth />
  <Total-ISDN-Bandwidth />
  <Total-MCU-Connections-Number />
  <Total-GW-Connections-Number />
</Resources-Scheduled-At-Time-Of-Conference>
<Resources>
  <Attendees-Terminals>
    <Host>
      <User-Id />
      <Login-Id />
      <First-Name />
      <Last-Name />
      <Email />
      <Customer-Id />
      <Company-Name />
      <Customer-Profile-Type />
      <Customer-Billing-Phone />
      <Is-Controller />
    </Host>
    <Organizer>
      <User-Id />
      <Login-Id />
      <First-Name />
      <Last-Name />
      <Email />
      <Customer-Id />
      <Company-Name />
      <Customer-Profile-Type />
      <Customer-Billing-Phone />
      <Is-Controller />
    </Organizer>
    <Predefined-Attendees>
      <Predefined-Attendee>
        <User-Id />
        <Login-Id />
        <First-Name />
        <Last-Name />
        <Email />
        <Customer-Id />
        <Company-Name />
        <Customer-Billing-Phone />
        <Is-Controller />
      </Predefined-Attendee>
    </Predefined-Attendees>
    <External-Attendees>
      <External-Attendee>
        <Email />
        <First-Name />
```

```

    <Last-Name />
  </External-Attendee>
</External-Attendees>
<Predefined-Terminals>
  <Predefined-Terminal>
    <Terminal-Id />
    <Alias />
    <Dial-String />
    <IP-ISDN-SIP />
    <Dial-in-Dial-out />
    <MCU />
    <Gateway />
    <Room />
    <Gatekeeper />
    <Zone-Prefix />
  </Predefined-Terminal>
</Predefined-Terminals>
<External-Terminals>
  <External-Terminal>
    <Party-ID/>
    <Name />
    <Dial-String />
    <IP-ISDN-SIP />
    <Dial-in-Dial-out />
    <MCU />
    <Gateway />
    <Room />
    <Gatekeeper />
    <Zone-Prefix />
    <Desktop-Client/>
    <Desktop-Server/>
  <External-Terminal>
<External-Terminals>
<Attendees-Terminals-Association>
  <Association />
</Attendees-Terminals-Association>
</Attendees-Terminals>
<Network-Devices>
  <GKs>
    <GK-Proxy-Information>
      <ID />
      <Name />
      <Model />
      <IP-Address />
      <Zone-Prefix />
      <SIP-Domain />
      <GK-Device-Association>
        <Association />
      </GK-Device-Association>
    </GK-Proxy-Information>
  </GKs>
  <MCUs>
    <MCU-Information>
      <ID />
      <Alias />

```

```

    <Model />
    <Master-Slave />
    <Zone-Prefix />
    <Gatekeeper />
    <Service-Prefix />
    <List-of-Assigned-Terminals>
      <Terminal />
    </List-of-Assigned-Terminals>
  </MCU-Information>
</MCUs>
<GateWays>
  <Gateway-Information>
    <ID />
    <Phone-Number />
    <Service-Prefix />
    <Service-Bandwidth />
    <Country-Code />
    <Area-Code />
    <Zone-Prefix />
    <Terminal-Gateway-Association>
      <Association />
    </Terminal-Gateway-Association>
  </Gateway-Information>
</GateWays>
<Rooms>
  <Room-Information>
    <ID />
    <Name />
    <Terminal-Room-Association>
      <Terminal />
    </Terminal-Room-Association>
  <Room-Information>
</Rooms>
</Network-Devices>
</Scheduling-Data>
<Completed-Conference-Data>
  <Conference-Status />
  <Reason-Failed />
  <Actual-Start-Time />
  <Actual-End-Time />
<Actual-Predefined-Terminals>
  <Actual-Predefined-Terminal>
    <Terminal-Id />
    <Alias />
    <Dial-String />
    <IP-ISDN-SIP />
    <Source-IP-Address />
    <Total-Connection-Time />
    <Failing-Attempts />
    <Last-Failure-Cause />
    <List-of-Connection-Records />
      <Connection />
    </List-of-Connection-Records />
  </Actual-Predefined-Terminal>
</Actual-Predefined-Terminals>

```

```

<Actual-External-Terminals>
  <Actual-External-Terminal>
    <Party-ID />
    <Name />
    <Dial-String />
    <IP-ISDN-SIP />
    <Desktop-Client />
    <Desktop-Server />
    <Total-Connection-Time />
    <Failing-Attempts />
    <Last-Failure-Cause />
    <List-of-Connection-Records />
      <Connection />
    </List-of-Connection-Records >
  </Actual-External-Terminal>
</Actual-External-Terminals>
<Connected-MCUs>
  <MCU-information>
    <ID />
    <Alias />
    <Model />
    <Master-Slave />
      <Zone-Prefix />
      <Gatekeeper />
      <Service-Prefix />
    </List-of-Assigned-Terminals>
  </MCU-information>
</Connected-MCUs>
<Connected-GWs>
  <Gateway-information>
    <ID />
    <Phone-Number />
    <Service-Prefix />
    <Service-Bandwidth />
    <Country-Code />
    <Area-Code />
    <Zone-Prefix />
    <Terminal-Gateway-Association>
      <Association />
    </Terminal-Gateway-Association>
  </Gateway-information>
</Connected-GWs>
</Completed-Conference-Data>
</Conference-Data>
</conferences>

```

# Understanding the CDR XML Tags

Table 15-1 provides details about each CDR tag and includes a reference to information about configuring the tag in the CDR.



**Note**

In the tags, “conference” is equivalent to “meeting”, and “service” is equivalent to “meeting type”.

**Table 15-1** CDR XML Tag Details

Tag	Description	Attribute	Type	Example
<conferences> </conferences>	Defines the beginning of all conference data. Contains data for the conferences of an entire day or for a single conference depending on the configuration			
<ConferenceData></ConferenceData>	Defines the beginning of data recording for a meeting instance			
<Event></Event>	Defines the record type.	value	Schedule/ Reschedule/ Cancel/ Complete	
<Scheduling-Data></Scheduling-Data>	Contains data directly related to meeting scheduling, such as which resources are reserved and which attendees and/or terminals are invited as part of meeting scheduling.			
<Conference> </Conference>	Contains basic information about the scheduling of a meeting.			
<Basic-Information></Basic-Information>	Contains basic information about the scheduling of a meeting.			
<Conference-ID />	Contains the Resource Manager internal ID of a specific conference.	value	String	<Conference-ID value="1307" />
<Virtual-Conference-ID />	Contains the Virtual Conference ID number of a specific conference.	value	String	<Virtual-Conference-ID value="1307" />
<Master-Conference-ID />	Contains the ID used to identify the meeting on the master MCU	value	String	<Master-Conference-ID value="N/A" />
<Slave-Conference-ID-List></Slave-Conference-ID-List>	Contains the meeting ID for a single slave MCU.			

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Slave-Conference-ID />	Contains the meeting ID for a single slave MCU.	value	Zone Number + Service Prefix ID + Physical Conference ID	<Slave-Conference-ID value="175-80-4417" />
<Subject />	Contains the meeting subject as entered during meeting scheduling.	value	String	<Subject value="Monthly Update" />
<Reference-Code />	Contains any internal department, billing, client or account numbers used to track resource use within a company, that are entered during meeting scheduling.	value	String	<Reference-Code value="A112" />
<Description />	Contains the description of the meeting, which is entered during meeting scheduling.	value	String	<Description value="N/A" />
<MultiPoint-PointToPoint />	Displays whether a multipoint meeting or a point-to-point meeting is scheduled. Possible values: Multipoint, PointToPoint	value	String	<MultiPoint-PointToPoint value="MultiPoint" />
<Scheduled-Adhoc />	Displays whether the meeting is scheduled to start at a future time or if it is created immediately (ad hoc) via Resource Manager or an endpoint. Possible values: Scheduled, Ad Hoc, Endpoint Initiated Ad Hoc.	value	String	<Scheduled-Adhoc value="AdHoc" />
<Start-Time />	Contains the scheduled start time of the meeting.	value	yyyy-mm-ddThh-mm-ssZ	<Start-Time value="2003-03-29 T11:35:47Z" />
<Duration />	Contains the scheduled meeting duration.	value	String	<Duration value="30 Minutes"/>
<Server-TimeZone />	Contains time zone information of the Resource Manager server	value	GMT+/-XX:XX (Integer + 'Minutes')	<Server-TimeZone value="GMT+08:00"/>
<Auto-Extend />	Determines whether or not Auto Extend is selected during meeting scheduling	value	Boolean	<AutoExtend value="true"/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Bill-To />	Contains information about who will be billed for the conference. Possible values: BILL_ALL_PARTICIPANTS, BILL_ORGANIZER, BILL_HOST, BILL_CONTROLLERS.	value	String	<Bill-To value="BILL_HOST"/>
<Billing-Code />	Contains the billing code relevant to the billing of the conference.	value	String	<Billing-Code value="1234" />
<Advanced-Information/></Advanced-Information>	Contains advanced meeting scheduling information.			
<Extra-Ports-reserved/>	Contains the number of additional ports that are reserved for the meeting during meeting scheduling	value	Integer	
<Priority />	Displays the Priority option selected during meeting scheduling. Possible values: Unspecified, Bandwidth, Delay	value	String	<Priority value="Delay" />
<DateTime-Scheduled/>	Contains the date and time that the meeting is scheduled via the Resource Manager.	value	yyyy-mm-ddThh-mm-ssZ	<DateTime-Scheduled value="2003-03-29T11:35:47Z" />
<DateTime-Cancelled/>	If a meeting is cancelled prior to its scheduled start time, the tag contains the date and time of cancellation.	value	yyyy-mm-ddThh-mm-ssZ	<DateTime-Cancelled value="N/A" />
<Streaming-Recording-Activated/>	Indicates whether streaming recording is enabled or not.	value	Boolean	<Streaming-Recording-Activated value="false"/>
<Export-Upon-Completion-Activated/>	Indicates whether or not the recorded file should be exported upon conference completion.	value	Boolean	<Export-Upon-Completion-Activated value="false"/>
<Streaming-Target-File-Name/>	Contains the recorded file's name, if specified by the user	value	String	<Streaming-Target-File-Name value="N/A"/>
<Streaming-Recording-View/>	Contains the view chosen for recording	value	String	<Streaming-Recording-View value="N/A"/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Conference-Lifecycle-Summary/>	Contains lifecycle information for a single instance of a scheduled meeting, including basic statistics captured during meeting scheduling, as well as records of any modifications prior to the actual meeting.			
<Resources-Scheduled/>	Contains a list of resources scheduled when a meeting is created or modified.			
<DateTime-Modified/>	Contains the date and time of modification of a scheduled meeting.	value	yyyy-mm-ddThh-mm-ssZ	<DateTime-Modified value="2003-03-30 T10:20:25Z" />
<Total-IP-Bandwidth/>	Contains the total amount of IP bandwidth, in Kbps, scheduled for the meeting	value	Integer	<Total-IP-Bandwidth value="768" />
<Total-ISDN-Bandwidth/>	Contains the total amount of ISDN bandwidth scheduled for a meeting, in Kbps.	value	Integer	<Total-ISDN-Bandwidth value="192"/>
<Total-MCU-Connections-Number/>	Contains the total number of MCU connections scheduled for a meeting (number of terminals, extra ports and cascading MCUs).	value	Integer	<Total-MCU-Connections-Number value="1" />
<Total-GW-Connections-Number/>	Contains the total number of gateway connections scheduled for the conference (number of terminals and reserved ISDN ports).	value	Integer	<Total-GW-Connections-Number value="1" />
<Resources>	Contains a list of resources committed or required for a meeting.			
<Conference-Service>	Contains a list of meeting types scheduled for use.			
<Service-Id/>	Lists the Resource Manager ID (name) of the service selected for use during the meeting.	value	String	<Service-Id value="10045" />
<MCU-Service-Prefix />	Contains the MCU service prefix on the master MCU selected for use during the meeting.	value	String	<MCU-Service-Prefix value="80"/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Min-Video-Layout/>	Displays the minimal (smallest) video layout of all schemes associated with the scheduled meeting type	value	Integer	<Min-Video-Layout value="1" />
<Max-Video-Layout/>	Displays the maximum (largest) video layout of all schemes associated with the scheduled meeting type.	value	Integer	<Max-Video-Layout value="1" />
<Max-Bit-Rate-In/>	Displays the maximum incoming video bit-rate available for the meeting type, In Kbps.	value	Integer	<Max-Bit-Rate-In value="384" />
<Max-Bit-Rate-Out/>	Displays the maximum outgoing video bit-rate available for the meeting type, in Kbps.	value	Integer	<Max-Bit-Rate-Out value="0" />
<Max-Frame-Rate-In/>	Displays the maximum incoming frame-rate available for the meeting type.	value	Integer	<Max-Frame-Rate-In value="30" />
<Max-Frame-Rate-Out/>	Displays the maximum outgoing frame-rate among all schemes available for the meeting type. Possible values: NONE, 5, 7.5, 10, 15, 25, 30, 50, 60	value	String	<Max-Frame-Rate-Out value="30" />
<Max-Picture-Format-In/>	Displays the maximum incoming picture format available for the meeting type. Possible values: NONE, SQCIF, QCIF, SIF, CIF, VGA, 4SIF, 4CIF, SVGA, XGA, SXGA, 16CIF, UXGA, 4XGA	value	String	<Max-Picture-Format-In value="4SIF" />
<Max-Picture-Format-Out/>	Displays the maximum outgoing picture format available for the meeting type. Possible values: NONE, SQCIF, QCIF, SIF, CIF, VGA, 4SIF, 4CIF, SVGA, XGA, SXGA, 16CIF, UXGA, 4XGA	value	String	<Max-Picture-Format-Out value="4SIF" />
<Max-T120-Ports-Reserved />	Contains the total number of T120 ports reserved for the meeting.	value	Integer	<Max-T120-Ports-Reserved value="0"/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Max-Subconferences/>	Contains the number of breakout meetings (or sub-conferences) that are a part of the selected meeting type.	value	Integer	<Max-Subconferences value="0" />
<Resources-Scheduled-At-Time-Of-Conference>	Contains a list of resources at the time the meeting starts (including modifications made to the meeting reservation prior to the meeting start).			
<Total-IP-Bandwidth/>	Contains the total amount of IP bandwidth scheduled at the time of the meeting.	value	Integer	<Total-IP-Bandwidth value="768" />
<Total-ISDN-Bandwidth/>	Contains the total amount of ISDN bandwidth scheduled at the time of the meeting.	value	Integer	<Total-ISDN-Bandwidth value="192"/>
<Total-MCU-Connection-Number/>	Contains the total number of MCU connections scheduled at the time of the meeting.	value	Integer	<Total-MCU-Connections-Number value="5"/>
<Total-GW-Connections-Number/>	Contains the total number of gateway connections scheduled at the time of the meeting.	value	Integer	<Total-GW-Connections-Number value="5"/>
<Attendees-Terminals>	Contains lists of attendees and terminals scheduled for a conference.			
<Host>	Contains information about the meeting host assigned during meeting scheduled.			
<User-Id/>	Contains the Resource Manager ID number of the meeting host.	value	String	<User-Id value="75" />
<Login-Id />	Contains the Resource Manager login ID of the meeting host.	value	String	<Login-Id value="Jsmith" />
<First-Name />	Contains the first name of the meeting host.	value	String	<First-Name value="Jennifer" />
<Last-Name />	Contains the last name of the meeting host.	value	String	<Last-Name value="Smith" />
<Email />	Contains the email address of the meeting host	value	String	<Email value=jsmith@testco.com/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Customer-ID />	Contains the Resource Manager customer ID of the meeting host.	value	String	<Customer-Id value="67" />
<Company-Name />	Contains the name of the company of the meeting host, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />
<Customer-Profile-Type />	Contains the customer profile-type for the company to which the meeting host belongs. For future use.	value	String	
<Customer-Billing-Phone/>	Contains the telephone number for the billing contact of the meeting host.	value	String	<Customer-Billing-Phone value="8499551" />
<Is-Controller/>	Notes whether the organizer, during meeting scheduling, granted the meeting host permission to control the meeting.	value	Boolean	
<Organizer>	Contains information about the meeting organizer.			
<User-Id/>	Contains the Resource Manager ID number of the meeting organizer.	value	String	<User-Id value="75" />
<Login-Id />	Contains the Resource Manager login ID of the meeting organizer.	value	String	<Login-Id value="Jsmith" />
<First-Name />	Contains the first name of the meeting organizer.	value	String	<First-Name value="Jennifer" />
<Last-Name />	Contains the last name of the meeting organizer.	value	String	<Last-Name value="Smith" />
<Email />	Contains the email address of the meeting organizer	value	String	<Email value="jsmith@testco.com"/>
<Customer-ID />	Contains the Resource Manager customer ID of the meeting organizer.	value	String	<Customer-Id value="67" />
<Company-Name />	Contains the name of the company of the meeting organizer, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Customer-Profile-Type />	Contains the customer profile-type for the company to which the meeting organizer belongs. For future use.	value	String	
<Customer-Billing-Phone/>	Contains the telephone number for the billing contact of the meeting organizer.	value	String	<Customer-Billing-Phone value="8499551" />
<Is-Controller/>	Notes whether or not the organizer has permission to control the meeting.	value	Boolean	
<Predefined-Attendees>	Contains information about meeting attendees that are registered in the Resource Manager.			
<Predefined-Attendee />	Contains information about a meeting attendee registered in Resource Manager			
<User-Id/>	Contains the Resource Manager ID number of the attendee.	value	String	<User-Id value="75" />
<Login-Id />	Contains the Resource Manager login ID of the attendee.	value	String	<Login-Id value="SPerkins" />
<First-Name />	Contains the first name of the attendee.	value	String	<First-Name value="Sam" />
<Last-Name />	Contains the last name of the attendee.	value	String	<Last-Name value="Perkins" />
<Email />	Contains the email address of the attendee.	value	String	<Email value="sperkins@testco.com"/>
<Customer-ID />	Contains the Resource Manager customer ID of the attendee.	value	String	<Customer-Id value="73" />
<Company-Name />	Contains the name of the company of the attendee, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />
<Is-Controller/>	Notes whether the organizer, during meeting scheduling, granted the attendee permission to control the meeting.	value	Boolean	

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<External-Attendees>	Contains a list of external meeting attendees (attendees not registered to Resource Manager).			
<External-Attendee>	Contains information about an individual external meeting attendee who is not registered in Resource Manager.			
<Email />	Contains the email address of an external meeting attendee.	value	String	<Email value="BJones@externalco.co/" >
<First-Name />	Contains the first name of an external meeting attendee.	value	String	<First-Name value="Bill"/>
<Last-Name />	Contains the last name of an external meeting attendee.	value	String	<Last-Name value="Jones"/>
<Predefined-Terminals>	Contains a list of all Resource Manager-registered terminals scheduled for the meeting.			
<Predefined-Terminal/>	Contains information about a single Resource Manager registered terminal scheduled for the meeting.			
<Terminal-ID />	Contains the internal Resource Manager ID string of a terminal.	value	String	<Terminal-Id value="0001-PARTY-10007" />
<Alias />	Contains the internal Resource Manager name or the alias of a terminal.	value	String	<Alias value="T1"/>
<Dial-String />	Contains the dial-string information of a terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="812518" />
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP	value	String	<IP-ISDN-SIP value="IP" />
<Dial-in-Dial-out />	Contains the dialing mode of the terminal. Possible values: Dial-in, Dial-out	value	String	<Dial-in-Dial-out value="Dial-out" />
<MCU />	Contains MCU information for an individual terminal registered to the Resource Manager.	value	String	<MCU value="0001-MCU-10001" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Gateway />	Contains gateway information for an individual terminal registered to the Resource Manager.	value	String	<Gateway value="N/A" />
<Room />	Contains room information for a terminal registered to Resource Manager, if that terminal is associated with a room in Resource Manager.	value	String	<Room value="0001-ROOM-10001" />
<Gatekeeper />	Contains Gatekeeper information for an individual terminal registered to Resource Manager.	value	String	<Gatekeeper value="001-GK-10001"/>
<Zone-Prefix />	Contains the zone prefix for an individual terminal registered to Resource Manager.	value	String	<Zone-Prefix value="81" />
<External-Terminals>	Contains a list of external terminals (terminals not registered to Resource Manager) scheduled for the meeting.			
<External-Terminal>	Contains information for an individual terminal scheduled for a meeting.			
<Party-ID />	Contains the internal Resource Manager ID string given to the external terminal.	value	String	<Party-Id value="EXTRA:2222" />
<Name />	Contains the name of an external terminal as entered during meeting scheduling.	value	String	<Name value="Bob Baxton Mobile"/>
<Dial-String />	Contains the dial-string information of an external terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="8125199" />
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP	value	String	<IP-ISDN-SIP value="IP" />
<Dial-in-Dial-out />	Contains the dialing mode of the terminal. Possible values: Dial-in, Dial-out	value	String	<Dial-in-Dial-out value="Dial-out" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<MCU />	Contains MCU information of the external terminal.	value	String	<MCU value="0001-MCU-10001" />
<Gateway />	Contains gateway information of the external terminal.	value	String	<Gateway value="N/A" />
<Room />	Contains room information of the external terminal (if relevant).	value	String	<Room value="N/A" />
<Gatekeeper />	Contains Gatekeeper information of the external terminal.	value	String	<Gatekeeper value="0001-GK-10001"/>
<Zone-Prefix />	Contains the zone prefix of the external terminal.	value	String	<Zone-Prefix value="81" />
<Desktop-Client />	Indicates whether or not this external terminal is a Desktop client. Only appears if value is True.	value	Boolean	<Desktop-Client value="true" />
<Desktop-Server />	Contains the internal Resource Manager ID of the Cisco Unified Videoconferencing Desktop Server that is associated with this terminal.	value	String	<Desktop-Server value="0001-SDG-10002" />
<Attendees-Terminals-Association>	Contains a list of attendee and terminal associations, allowing administrators to determine which users used which terminals for an individual meeting.			
<Association />	Associates an attendee with a terminal, login ID, email address, and terminal/dial string.	Dial-String, Email, LoginId	String	<Association Dial-String = "812518" Email = "Mjones@tco.com" LoginId = "Mjones"/>
<Network-Devices>	Contains information about network devices scheduled for use in a meeting during resource allocation.			
<GKs>	Contains a list of all gatekeepers reserved for use during a meeting.			

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<GK-Proxy-Information>	Contains information about an individual gatekeeper that is reserved for use during the meeting.			
<ID />	Contains the internal gatekeeper ID in the Resource Manager.	value	String	<ID value = "0001-GK-10001" />
<Name />	Contains the name of the gatekeeper in the Resource Manager.	value	String	<Name value = "GK 58" />
<Model />	Contains gatekeeper model information.	value	String	<Model value = "Cisco IOS H.323 Gatekeeper" />
<IP-Address />	Contains the IP address of the gatekeeper.	value	String	<IP-Address value = "192.168.1.58" />
<Zone-Prefix />	Contains the zone prefix of the gatekeeper.	value	String	<Zone-Prefix value = "58" />
<SIP-Domain />	Contains the SIP domain of a gatekeeper.	value	String	<SIP-Domain = "N/A" />
<GK-Device-Association>	Contains a list of gatekeeper and device associations, including all devices (terminals, MCUs, and gateways) registered to the gatekeeper.			
<Association />	Associates an individual gatekeeper with devices registered to that gatekeeper.	Alias, E.164, device-Address, device-Type	String	<Association Alias="2509" E.164="2509" device-Address="N/A" device-Type="Terminal" />
<MCUs>	Contains a list of all MCUs reserved for use during the meeting.			
<MCU-Information>	Contains information about an individual MCU reserved for use during the meeting.			
<ID />	Contains the internal Resource Manager ID of the MCU.	value	String	<ID value = "0001-MCU-10002" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Alias />	Contains the name of the MCU name in the Resource Manager.	value	String	<Alias value="MCU 82" />
<Model />	Contains model information for an individual MCU scheduled for use for the meeting.	value	String	<Model value="Cisco MCU 3.0+" />
<Master-Slave />	Specifies whether or not this MCU is master or slave if the meeting is scheduled with cascading (set to True if the MCU served as Master in a cascaded conference).	value	String	<Master-Slave value="false" />
<Zone-Prefix />	Specifies the zone prefix of an MCU.	value	String	<Zone-Prefix value="58" />
<Gatekeeper />	Specifies the gatekeeper to which the MCU is registered.	value	String	<Gatekeeper value="0001-GK-10001" />
<Service-Prefix />	Specifies the service prefix of an MCU.	value	String	<Service-Prefix value="80" />
<List-of-Assigned-Terminals>	Contains a list of terminals assigned to the MCU for the meeting.			
<Terminal />	Contains information about a single terminal assigned to the MCU for the meeting. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="2518" Dial-String="812 518" IP-ISDN-SIP="IP"/>
<Gateways>	Contains a list of all gateways reserved for use during the meeting.			
<Gateway-Information>	Contains information about an individual gateway reserved for use during the meeting.			
<ID />	Contains the internal Resource Manager ID of the gateway.	value	String	<ID value = "0001-GW-10006" />
<Phone-Number />	Contains the gateway phone number.	value	String	<Phone-Number value="88372361" />
<Service-Prefix />	Contains the prefix of the requested service.	value	String	<Service-Prefix value="9384" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Service-Bandwidth />	Specifies the bandwidth associated with the requested service configured on the gateway.	value.	String	<Service-Bandwidth value="384" />
<Country-Code />	Specifies the country code of a gateway.	value	String	<Country-Code value="86" />
<Area-Code />	Specifies the area code of a gateway.	value	String	<Area-Code value="10" />
<Zone-Prefix />	Specifies the zone prefix of a gateway.	value	String	<Zone-Prefix value="58" />
<Terminal-Gateway-Association>	Contains a list of endpoints (terminals) assigned to the gateway for the meeting.			
<Association />	Associates an ISDN terminal with the gateway it will use for the meeting.	Alias, ISDN-Phone-Number, Scheduled-Service-Bandwidth, Scheduled-Service-Prefix	String, String, Integer, String	<Association Alias="ISDN002" ISDN-Phone-Number="22-55-88" Scheduled-Service-Bandwidth="64" Scheduled-Service-Prefix="9064" />
<Rooms>	Contains a list of all rooms reserved for use during the meeting.			
<Room-Information>	Contains information about an individual room reserved for use during the meeting.			
<ID />	Contains the Resource Manager ID number of the room.	value	String	<ID value = "0001-ROOM-10003" />
<Name />	Contains the room name in Resource Manager.	value	String	<Name value="Conference Room" />
<Terminal-Room-Association>	Contains a list of terminals and rooms to which they are assigned for the meeting.			

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Terminal />	Associates a room with any terminals that are located there for the meeting.	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="ISDN001" Dial-String="44-55-66" IP-ISDN-SIP="ISDN"/>
<Completed-Conference-Data>	Contains actual conference data collected during the course of the meeting and at the conclusion of the meeting.			
<Conference-Status />	Contains information about the results of the meeting, such as whether or the meeting was canceled before its scheduled start time or started successfully. Possible values: STARTED, CANCELLED-BY-SERVER, CANCELLED-BY-USER, FAILED-TO-START.	value	String	<Conference-Status value="STARTED"/>
<Reason-Failed />	Describes the reason a meeting fails to start.	value	String	<Reason-Failed value="N/A" />
<Actual-Start-Time />	Contains the actual (versus scheduled) start time of the meeting.	value	yyyy-mm-ddThh-mm-ssZ	<Actual-Start-Time value = "2003-03-29T11:35:49Z" />
<Actual-End-Time />	Contains the actual (versus scheduled) end time of the meeting.	value	yyyy-mm-ddThh-mm-ssZ	<Actual-End-Time value="2003-03-29T11:47:43Z" />
<Actual-Predefined-Terminals>	Contains a list of terminals registered to Resource Manager that actually participated in the meeting.			
<Actual-Predefined-Terminal>	Contains information on an individual terminal registered to Resource Manager that actually participated in the meeting.			
<Terminal-ID />	Contains the internal Resource Manager ID of a participating terminal.	value	String	<Terminal-Id value="0001-PARTY-10005" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Alias />	Contains the Resource Manager alias of a participating terminal.	value	String	<Alias value="2518" />
<Dial-String />	Contains the dial string of the participating terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="812518" />
<IP-ISDN-SIP />	Defines the type of the participating terminal.	value	String	<IP-ISDN-SIP value="IP" />
<Source-IP-Address />	Contains the IP address of the participating terminal.	value	String	<Source-IP-Address value="192.168.223.23" />
<Total-Connection-Time />	Contains the total connection time of the participating terminal to the meeting, in seconds.	value	String (Integer + 's')	<Total-Connection-Time value="600s"/>
<Failing-Attempts />	Contains the number of times that this terminal attempted to join the conference and failed.	value	Integer	<Failing-Attempts value="2" />
<Last-Failure-Cause />	Contains the cause of failure of the last failed attempt	value	String	<Last-Failure-Cause value="" />
<List-of-Connection-Records>	Contains a list of records for each time the participating terminal connected to and disconnected from the meeting.			
<Connection />	Contains connection records for a specific terminal.	Connection Time; Dialin-Dialout; Disconnection-Time; Over-GW-port-limit; Over-MCU-port-limit; Reason-Disconnection	yyyy-mm-ddThh-mm-ssZ; Dial-in/Dial-out; yyyy-mm-ddThh-mm-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dialin-Dialout" Disconnection-Time="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Disconnect"/>

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Actual-External-Terminals>	Contains a list of external terminals that actually participate in the meeting.			
<Actual-External-Terminal>	Contains information on an individual external terminal that actually participates in the meeting.			
<Party-ID />	Contains the internal Resource Manager ID string given to the external terminal.	value	String	<Party-Id value="EXTRA:2222" />
<Name />	Contains the name of the external terminal.	value	String	<Name value="Bob Baxton Mobile"/>
<Dial-String />	Contains the dial-string information of the external terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="8125199" />
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP	value	String	<IP-ISDN-SIP value="IP" />
<Desktop-Client />	Indicates whether or not this external terminal is a Desktop client. Only appears if value is True.	value	Boolean	<Desktop-Client value="true" />
<Desktop-Server />	Contains the internal Resource Manager ID of the Cisco Unified Videoconferencing Desktop Server that is associated with this terminal.	value	String	<Desktop-Server value="0001-SDG-10002" />
<Total-Connection-Time />	The overall time that the external terminal was connected in the conference, in seconds.	value	String (Integer+'s')	<Total-Connection-Time value="600s"/>
<Failing-Attempts />	Contains the number of times that this terminal attempted to join the conference and failed.	value	Integer	<Failing-Attempts value="0" />
<Last-Failure-Cause />	Contains the cause of failure of the last failed attempt.	value	String	<Last-Failure-Cause value="N/A" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<List-of-Connection-Records>	Contains a list of records for each time the participating terminal connected to and disconnected from the meeting.			
<Connection />	Contains connection records for a specific terminal.	Connection Time; Dialin-Dialout; Disconnection-Time; Over-GW-port-limit; Over-MCU-port-limit; Reason-Disconnection	yyyy-mm-ddThh-mm-ssZ; Dial-in/Dial-out; yyyy-mm-ddThh-mm-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dialin-Dialout" Disconnection-Time="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Disconnect" />
<Connected-MCUs>	Contains a list of all MCUs actually used during the meeting.			
<MCU-Information>	Contains information about an individual MCU used during the meeting.			
<ID />	Contains the internal Resource Manager ID of the MCU.	value	String	<ID value="0001-MCU-10002" />
<Alias />	Contains the name of the MCU name in the Resource Manager.	value	String	<Alias value="MCU 82" />
<Model />	Contains model information for an individual MCU scheduled for use for the meeting.	value	String	<Model value="Cisco MCU 3.0+" />
<Master-Slave />	Specifies whether or not this MCU is master or slave, in case the meeting is scheduled with cascading (set to True if the MCU served as Master in a cascaded conference).	value	String	<Master-Slave value="false" />
<Zone-Prefix />	Specifies the zone prefix of an MCU.	value	String	<Zone-Prefix value="58" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Gatekeeper />	Specifies the gatekeeper to which the MCU is registered.	value	String	<Gatekeeper value="0001-GK-10001" />
<Service-Prefix />	Specifies the service prefix of an MCU.	value	String	<Service-Prefix value="80" />
<List-of-Assigned-Terminals>	Contains a list of terminals assigned to the MCU for the meeting.			
<Terminal />	Contains information about a single terminal assigned to the MCU for the meeting. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="2518" Dial-String="812518" IP-ISDN-SIP="IP"/>
<ConnectedGWs>	Contains a list of all gateways that actually participated in the meeting.			
<Gateway-Information>	Contains information about an individual gateway used during the meeting.			
<ID />	Contains the internal Resource Manager ID of the gateway.	value	String	<ID value="0001-GW-10006" />
<Phone-Number />	Contains the gateway phone number.	value	String	<Phone-Number value="88372361" />
<Service-Prefix />	Contains the prefix of the requested service.	value	String	<Service-Prefix value="9384" />
<Service-Bandwidth />	Specifies the bandwidth associated with the requested service configured on the gateway.	value	String	<Service-Bandwidth value="384" />
<Country-Code />	Specifies the country code of a gateway.	value	String	<Country-Code value="86" />
<Area-Code />	Specifies the area code of a gateway.	value	String	<Area-Code value="10" />
<Zone-Prefix />	Specifies the zone prefix of a gateway.	value	String	<Zone-Prefix value="58" />

Table 15-1 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Terminal-Gateway-Association>	Contains a list of terminals assigned to the gateway for the meeting.			
<Association />	Associates an ISDN terminal with the gateway it will use for the meeting.	Alias, ISDN-Phone-Number, Scheduled-Service-Bandwidth, Scheduled-Service-Prefix	String, String, Integer, String	<Association Alias="ISDN002" " ISDN-Phone-Number="22-55-88" Scheduled-Service-Bandwidth="64" " Scheduled-Service-Prefix="9064" />



## CHAPTER 16

# Enabling Resource Manager to Use Secure Sockets Layer Connections on a JBoss Application Server

---

- [Component Identity via SSL, page 16-1](#)
- [How to Generate Certificates, page 16-1](#)

## Component Identity via SSL

Secure Sockets Layer (SSL) connections rely on the existence of digital certificates. A digital certificate reveals information about its owner, including the owner's identity.

During the initialization of an SSL connection, the server must present its certificate to the client for the client to determine the server identity. The client can also present the server with its own certificate for the server to determine the client identity. SSL is therefore, a means of propagating identity between components.

## How to Generate Certificates

- [Methods for Creating a New Certificate, page 16-2](#)
- [Prerequisites, page 16-2](#)
- [Using Keytool to Generate a Certificate, page 16-2](#)
- [Configuring JBoss to Use SSL, page 16-4](#)
- [Accessing Resource Manager via HTTPS, page 16-5](#)

## Methods for Creating a New Certificate

A client can trust the contents of a certificate if that certificate is digitally signed by a trusted third party. A Certificate Authority (CA) acts as a trusted third party and signs certificates on the basis of its knowledge of the certificate requestor.

There are two methods for creating a new certificate.

- Request that a CA generates the certificate on your behalf.

The CA creates a new certificate, digitally signs it, and delivers it to the requester. Popular web browsers are preconfigured to trust certificates that are signed by certain CAs. No further client configuration is necessary for a client to connect to the server through an SSL connection.

Therefore, CA signed certificates are useful where configuration for each and every client that accesses the server is impractical.

- Generate a self-signed certificate.

This option is quicker and requires fewer details to create the certificate, but the certificate is not signed by a CA. Any client that connects to this server over an SSL connection needs configuration to trust the signer of this certificate. Therefore, self-signed certificates are only useful when you can configure each of the clients to trust the certificate. It is possible in some cases to present a self-signed certificate to an untrusting client. In some web browsers, when the certificate is received and does not match any of those listed in the client trust file, a prompt appears asking if the certificate should be trusted for the connection and added to the trust file.

## Prerequisites

Cisco Unified Videoconferencing Manager uses the JBoss application server platform. The JBoss application server installs with Cisco Unified Videoconferencing Manager automatically.

To use SSL with JBoss, the following conditions must be met:

- You have a certificate.
- You configure JBoss to use this certificate.
- You store the certificate in a JKS keystore.

## Using Keytool to Generate a Certificate

Keytool is the command line Java utility. This section describes how to use keytool to create a private and public self-signed certificate key pair.

### Procedure

**Step 1** Open a DOS window and set the path to point to the JDK or JRE *bin* directory. For example

```
D:\>set path= D:\jdk1.5.0\bin
```

**Step 2** Create a self-signed certificate key pair. For example

```
D:\>keytool -genkey -keyalg RSA
-dname "cn=scheduler,ou=users,ou=yourcountry,
DC=yourcompany,DC=com"
```

```
-alias scheduler -keypass yourcompany -keystore
scheduler.keystore
-storepass yourcompany
```

- Step 3** Specify RSA as the private key to ensure that the MD5 with RSA signature algorithm is used. Not all web browsers support the DSA cryptograph algorithm, which is the default when RSA is not specified.
- Step 4** Set a password of at least six characters to protect the private key.
- Step 5** Specify the keystore file and keystore password (the option is storepass). Type each string on a single line.
- Step 6** If you do not wish to send a certificate signing request, skip to [“Configuring JBoss to Use SSL” section on page 16-4](#).

- Step 7** Generate the certificate signing request. For example
- `D:\>keytool -certreq -v -alias scheduler -file scheduler.csr -keypass yourcompany`
  - `-keystore scheduler.keystore -storepass yourcompany`

This request generates the following output:

Certification request stored in file <scheduler.csr>

Submit this to your CA

- Step 8** Send the scheduler.csr file to your selected CA for signing.
- Step 9** Save the content of the signed certificate to a file. For example, scheduler.cer.
- Step 10** Import the CA trusted root certificate into the keystore. For example

```
D:\>keytool -import -alias "Provider Test CA Root" -file "Provider Test Root.cer"
-keystore sceduler.keystore -storepass yourcompany
```

where

- `Provider Test CA Root` is the directory containing the test CA root binary and text files.
- `Provider Test Root.cer` is the test CA root binary file.

When the command is successfully executed, the following output displays:

```
Certificate was added to keystore
```

- Step 11** Import the certificate responses from the CA into the keystore file using the same alias name that was first given to the self-signed certificates.

In this example, the alias name is `scheduler`. Using an alternative alias name generates a new signed certificate and not a personal certificate chain.

```
D:\>keytool -import -trustcacerts -alias scheduler -file scheduler.cer
-keystore scheduler.keystore -storepass yourcompany
```

When the command is successfully executed, the following output displays:

```
Certificate reply was installed in keystore
```

You have now created a keystore file that stores a valid certificate for use.

## Configuring JBoss to Use SSL

Configure the JBoss application server for use with SSL.

### Procedure

- 
- Step 1** Copy the scheduler.keystore file to  
<Resource Manager installation directory>\jboss\server\default\conf
- Step 2** Open the server.xml file located in jboss\server\default\deploy\jbossweb-tomcat50.sar
- Step 3** Locate the section beginning with the line  
 <!-- SSL/TLS Connector configuration using the admin devl guide keystore
- Step 4** Remove the comment indicators and make the following changes:
- Uncomment out the SSL/TLS connector.
  - Change the keystore file from **chap8.keystore** to **scheduler.keystore**.
  - Change the keystorePass from **rmi+ssi** to **yourcompany**.
  - We recommend that you change the port from 8443 to 443 so that the user does not need to type the port when accessing Resource Manager. Like port 80, port 443 is a known HTTPS port.

The amended text appears as follows:

```
<!-- A HTTP/1.1 Connector on port 8080 or 80 -->
<Connector port="8080" address="{jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>

<!-- A AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="{jboss.bind.address}"
enableLookups="false" redirectPort="443" debug="0"
protocol="AJP/1.3"/>

<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/
scheduler.keystore"
keystorePass="yourcompany" sslProtocol = "TLS" />
<!-- -->
```

- Step 5** Restart JBoss.
-

## Accessing Resource Manager via HTTPS

### Procedure

---

- Step 1** Type a URL of the format `https://localhost`, or `https://localhost:8443` (if port 8443 is used instead of 443). If the certificate in use is a test root certificate or a self-signed certificate that is not trusted by Internet Explorer, a security alert appears.
- Step 2** Click **Yes** to access Resource Manager.
- Step 3** To avoid this message in future logins, click **View Certificate**:
- Step 4** Click **Install Certificate**.
- Step 5** After the certificate is installed, the user will not see the security alert on subsequent logins.
-





## **PART 2**

### **Network Manager**





# CHAPTER 17

## Viewing Your Network in Network Manager

---

- [How to View the Network as a Tree, page 17-1](#)
- [Viewing the Network as a Table, page 17-3](#)
- [Viewing the Network as a Map, page 17-3](#)

### How to View the Network as a Tree

The Network Tree view organizes the information about the IP conferencing network into one or more tabbed views, each of which lists the elements in the network in a tree structure. By default, the tree divides the elements by zones.

- [Configuring Network Hierarchy, page 17-1](#)
- [Creating a Custom Network Tree View, page 17-2](#)

### Configuring Network Hierarchy

The drag and drop feature enables quick configuration of the network hierarchy and automatically reconfigures element relationships by automatically assigning and updating the appropriate details of the elements with which the managed element registers.

You can configure these element relationships:

- Gatekeeper Parent - Child
- Gatekeeper - MCU/Gateway
- MCU - EMP

Network Manager automatically updates element tables for Gatekeeper parent and child elements in the relationship. Network Manager updates MCU and gateway elements with the appropriate gatekeeper IP address. Network Manager updates EMP elements with the relevant IP address and configuration details for registering with the MCU.

**Procedure**

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select an element in the network tree.
  - Step 3** Drag and drop the element to the required location in the hierarchy.
  - Step 4** Deselect the element.
- 

## Creating a Custom Network Tree View

You can create your own tree structures according to criteria you define, such as the physical location or other customer-specific criteria. You can add folders and elements to the custom views and organize them as needed.

**Procedure**

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Do one of the following:
    - Right-click a tab in the Network Tree view (above the tree) and select **Add tree view**.
    - Select **Edit > New > New tree view**.
  - Step 3** Enter a name for the new tree view and click **OK**.  
The new tree view is added to the Network Tree view.  
By default, the new tree view includes a Network root directory and an Unassigned folder. The Unassigned folder contains all the elements in the network organized by type.
  - Step 4** Create folders for organizing the elements in the tree view by right-clicking the location in the tree where each folder should be located, and selecting **Add folder**.
  - Step 5** Drag and drop elements from the Unassigned folder to the folders that you created.

**Note**

To rename or remove tree views, either use the Edit menu or right-click the tree view. To rename or remove folders, right-click the folder and select the relevant option.

---

## Viewing the Network as a Table

The Network Table view displays information about all the elements in the IP conferencing network in a single table and provides element editing, search and auto-detect capabilities.

### Procedure

---

**Step 1** Click **Network Table** in the sidebar menu.

The Network Table view includes the following information about each element:

- Element status
- Element type
- Element name
- IP address
- Version number
- Location
- Gatekeeper calls
- Resource usage versus capacity

**Step 2** Click the column headers to sort the information displayed.

**Step 3** Double-click any element in the table to display the relevant element manager for that element.

---

## Viewing the Network as a Map

The Network Map view displays information about the IP conferencing network in the form of graphic maps created for each node in the network hierarchy.

### Procedure

---

**Step 1** Click **Network Map** in the sidebar menu.

The top level of the Network Map view displays the network root and the zones into which the network is divided.

Each square represents either the network root, a zone (or user-defined folder) or a single element. Each square includes the following information:

- Current status
- Number of calls
- Number of conferences
- Number of registered participants versus capacity
- Number of B-channels handled by gateways versus capacity
- Total bandwidth handled by gatekeepers versus capacity

Inter-zone bandwidth information appears above the zones when relevant.

**Step 2** Use the Up and Down buttons to navigate between map levels.

The Network Map view enables you to navigate from the zone level (or folder) to the element level by double-clicking a square.

**Step 3** Use the list to select which view to display.

---



## CHAPTER 18

# Managing Elements in Network Manager

---

- [Displaying General Element Information, page 18-2](#)
- [About the Management Status of Elements, page 18-2](#)
- [Viewing all Network Elements, page 18-3](#)
- [Creating or Modifying an Element Profile, page 18-3](#)
- [Removing an Element Profile, page 18-4](#)
- [Searching for an Element Profile, page 18-5](#)
- [Defining Default Element Access Settings, page 18-5](#)
- [Overriding Default Element Access Settings, page 18-6](#)
- [How to Upgrade Element Software, page 18-6](#)
- [Cancelling Pending Offline Configuration Settings, page 18-8](#)
- [How to Manage the Element Software Upgrade Upload Log, page 18-8](#)
- [How to Automatically Detect New Elements on the Network, page 18-10](#)
- [Accessing an Element Web User Interface, page 18-12](#)
- [Accessing the Monitor Tab for a Specified Element, page 18-12](#)

## Displaying General Element Information

The Monitor tab, which is the default tab displayed when an item is selected in the Network Tree view, displays general information about the item.

When the gatekeeper in a zone is unmanaged or inferred, the calls, bandwidth and registration information appears as zero.

The information displayed on the Monitor tab is dependent on the item selected in the tree.

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the element you require in the tree.
  - Step 3** Click **Monitor**.
  - Step 4** (Optional) Click the link to display the element manager for the selected element.
- 

## About the Management Status of Elements

Table 18-1 describes the different types of element management status.

**Table 18-1** Element Management Status

| Element Status | Description  |
|----------------|--|
| Managed        | The element exists in the Network Manager database and provides monitoring information and access to configuration settings.   |
| Inferred       | The element does not exist in the Network Manager database, but it might appear as an inferred element because a managed element refers to that element.<br><br>For example, a gatekeeper is inferred when a managed element is registered to that gatekeeper zone, but the gatekeeper is not managed by the Network Manager.                                |
| Unmanaged      | The element exists in the Network Manager database but has no open communication channels with the Network Manager and provides no monitoring information or access to configuration settings.<br><br>An element might be unmanaged when the Network Manager license limitations have been exceeded or when the user manually sets the element as unmanaged. |

## Viewing all Network Elements

The Elements tab displays a table of all elements related to the network, zone or folder selected in the tree.





Any element listed in the tree with a question mark (?) is considered to be an inferred element by the system. This means that the element is not listed in the database, but it is presumed to exist because another known element refers to the element. Inferred elements cannot be managed; therefore, we recommend that you either initiate auto-detect to discover an element, add an element manually or manually connect an inferred element.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select Network root element.
- Step 3** Click **Elements**.


The table in the Elements tab includes the following information about each element:


- Element status, indicated by an icon, as follows:
    -  Online
    -  Unmanaged
    -  Offline
    -  Faulty
  - Element type (MCU, gatekeeper and so on)
  - Element name (acts as a link to its element manager)
  - IP address
  - Version number
  - Location (as defined on the Configure tab of each element)
  - Number of calls
  - Traffic usage versus capacity
- 

## Creating or Modifying an Element Profile


### Procedure

---


- Step 1** Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- Step 2** Do one of the following to modify an existing element profile:
- Right-click the element you require and select **Edit element**.
  - Select the element you require and select **Edit > Modify > Modify element**.
  - Select the element you require and click **Edit element** .

- Step 3** Select the location in the Network Tree or Network Map view where the new element should be added, and do one of the following to create a new user profile:
- Select **Edit > New > New element**.
  - Click **Add element** .
- Step 4** Enter the element name and IP address in the relevant fields.
- Step 5** Select the required element type.  
The element type cannot be modified.
- Step 6** Select **Managed element** to enable Network Manager to manage the element.
- Step 7** Select **Allow offline configuration** to allow offline configuration of the element.  
The Network Manager can hold configuration details for offline elements and apply settings as each element goes online. Both added elements and existing elements can be configured to allow offline configuration.
- Step 8** Click **OK** to save your changes.
- 

## Removing an Element Profile

Deleted elements are not added to the Network Manager database in any subsequent auto-detect operations. You can only add a deleted element manually either by using the New element option in the Edit menu, selecting the Add element button  in the network views (Network Tree, Network Table or Network Map), or by connecting to a deleted element that is inferred.


### Procedure

- Step 1** Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- Step 2** Do one of the following to remove an existing element profile:
- Right-click the element you require and select **Delete element**.
  - Select the element you require and select **Edit > Delete > Delete element**.
  - Select the element you require and click **Delete element** .
- Step 3** Click **Yes**.  
The element profile is deleted from the scheduler and information about the element is removed from the database.
-

# Searching for an Element Profile

## Procedure

---

- Step 1** Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- Step 2** Do one of the following to search for an element profile:
- Right-click the element you require and select **Delete element**.
  - Select **Edit > Find > Find element**.
  - Click **Find element** .
- Step 3** Enter the IP address of the element or select the element type.
- Step 4** Click **Find**.

The required element is highlighted in the Network Tree, Network Table or Network Map view.

---

# Defining Default Element Access Settings

Default access settings allow access to a network element for monitoring and configuration without having to first go through the login window for that element.



## Note

You can override default access settings for a specified element at Network Tree > Access.

---

## Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Access**.
- Step 4** Select an element type.
- Step 5** Define SNMP read and write communities, user name and password, HTTP communication port and Telnet password in the relevant fields.
- SNMP community and Telnet information must match the settings defined in the selected element to enable Network Manager to retrieve information from the element.
- Step 6** Click **Upload** to save the information to the Network Manager database.
-

# Overriding Default Element Access Settings

## Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the required network element.
- Step 3** Click **Access**.
- Step 4** Check **Use default** to use the default access settings for the element type.  
When unchecked, all other tab options are disabled.  
Availability of the following access configuration parameters depends on the element type selected.
- Step 5** The Element type list appears when the selected element is an inferred gatekeeper. Select to display the appropriate access configuration parameters for the inferred gatekeeper.
- Step 6** Click **Connect** to connect to an inferred element and add it to the Network Manager database.  
SNMP community and Telnet information must match the settings defined in the selected element to enable Network Manager to retrieve information from the element.
- Step 7** Configure the following parameters:
- SNMP read community
  - SNMP write community
  - User name
  - Password
  - HTTP port
  - Telnet password (MCU, Cisco IOS H.323 Gatekeeper)
  - Telnet user name (Cisco IOS H.323 Gatekeeper only)
  - Enable Telnet (Cisco IOS H.323 Gatekeeper only)
- 

## How to Upgrade Element Software

Network Manager enables you to manage software upgrade files for Cisco Unified Videoconferencing 3500 MCUs and gateways, and Sony endpoints on your network.

- [Adding a Software Upgrade File, page 18-7](#)
- [Modifying a Software Upgrade File, page 18-7](#)
- [Removing a Software Upgrade File, page 18-7](#)

## Adding a Software Upgrade File

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Software Upgrade Files**.
- Step 4** Select the type of element you require in the Show field.
- Step 5** Click **Add**.
- Step 6** Enter the full path of the software upgrade file to be added to the Network Manager database, or browse to the file.
- Step 7** Enter a name and description for the upgrade file in the relevant fields.
- Step 8** Click **OK** to save your changes.
- 

## Modifying a Software Upgrade File

You can change the name and description of a software upgrade file that you have already added to Network Manager.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Software Upgrade Files**.
- Step 4** Select the type of element you require in the Show field.
- Step 5** Do one of the following:
- Double-click the software upgrade file you require.
  - Select the software upgrade file you require and click **Edit**.
  - Right-click the software upgrade file you require and select **Edit**.
- Step 6** Enter a new name and description for the upgrade file in the relevant fields.
- Step 7** Click **OK** to save your changes.
- 

## Removing a Software Upgrade File

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.

- Step 3** Click **Software Upgrade Files**.
- Step 4** Select the type of element you require in the Show field.
- Step 5** Do one of the following:
- Select the software upgrade file you require and click **Delete**.
  - Right-click the software upgrade file you require and select **Delete**.
- Step 6** Click **OK** to save your changes.
- The software upgrade file is removed from the database.
- 

## Cancelling Pending Offline Configuration Settings

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Right-click an offline element.
- Step 3** Select **Clear offline updates**.
- The element configuration settings which existed before the offline modifications are restored.
- 

## How to Manage the Element Software Upgrade Upload Log

- [Viewing Your Software Upgrade Upload History, page 18-8](#)
- [Uploading a File After a Failed Attempt, page 18-9](#)
- [Removing Entries from the Upload Log, page 18-9](#)

## Viewing Your Software Upgrade Upload History

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Upload Log**.
- Step 4** Select the type of element you require in the Show field.
- The Upload Log tab displays the history of all your attempts to upload a software upgrade file, and shows all scheduled future upload attempts.
-

## Uploading a File After a Failed Attempt

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Upload Log**.
- Step 4** Select the type of element you require in the Show field.
- Step 5** Do one of the following to attempt to upload a software upgrade file after a previous upload attempt has failed:
- Select the log entry you require and click **Retry**.
  - Right-click the log entry you require and select **Retry**.
- Step 6** Click **OK** to save your changes.
- 

## Removing Entries from the Upload Log

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Element Management**.
- Step 3** Click **Upload Log**.
- Step 4** Select the type of element you require in the Show field.
- Step 5** Do one of the following to remove a single log entry:
- Select the log entry you require and click **Delete**.
  - Right-click the log entry you require and select **Delete**.
- Step 6** Click **OK** to save your changes.
- Step 7** Click **Delete All** to remove all entries from the log.
- Step 8** Click **OK** to save your changes.
-

# How to Automatically Detect New Elements on the Network

Auto-detect enables you to search the network for elements and add them to the Network Manager database.

Auto-detect is performed by broadcasting requests to all SNMP communities defined in the Network Manager to Cisco elements. The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element.

Once these elements respond to the requests, the Network Manager can query the elements directly for full configuration and status details.

The auto-detect method of discovery might not find all the elements located behind equipment such as routers. Therefore, the Network Manager interface enables you to complete the database by adding elements manually.




## Note

Elements manually deleted from the Network Manager database are not detected in subsequent auto-detect procedures. These elements must be manually added to the Network Manager database. For more information, see the [“Creating or Modifying an Element Profile”](#) section on page 18-3.

- [Running the Auto-detect Mechanism Manually](#), page 18-10
- [Running the Auto-detect Mechanism Automatically](#), page 18-10
- [Adding or Modifying Auto-detect Element Access Information](#), page 18-11
- [Removing an Element Type from the Auto-detect Mechanism](#), page 18-11

## Running the Auto-detect Mechanism Manually

### Procedure

- 
- Step 1** Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- Step 2** Do one of the following:
- Select **Tools > Auto-detect elements**.
  - Click **Auto-detect elements** .
- Step 3** Click **Yes**.
- The Network Manager interface is updated accordingly.
- The auto-detect procedure might take some time, depending on the size of the network.
- 

## Running the Auto-detect Mechanism Automatically

### Procedure

- 
- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Auto-detect**.

- Step 3** (Optional) Click **Run auto-detect on server startup** to instruct Network Manager to look for new elements on the network whenever the Cisco Unified Videoconferencing Manager server is restarted.
- Step 4** (Optional) Click **Run auto-detect every (hrs)** and set an hourly interval to instruct Network Manager to look for new elements periodically.
- Step 5** (Optional) Click **Use default access information in auto-detect routine** to instruct Network Manager to use the default element access settings defined at Settings > Element Management > Access.
- Step 6** Click **Upload** to save your changes.
- 

## Adding or Modifying Auto-detect Element Access Information

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Auto-detect**.
- Step 3** Do one of the following to modify existing access settings for a network element:
- Double-click the element you require in the Type column.
  - Select the element you require and click **Edit**.
  - Right-click the element you require in the Type column and select **Edit**.
- Step 4** Do one of the following to create new access settings for a network element:
- Click **Add**.
  - Right-click any link in the Recipient Name column and select **Add**.
- Step 5** Select the unit type you require.
- Step 6** Define an SNMP read community in the relevant field.
- SNMP community information must match the settings defined in the selected element to enable Network Manager to retrieve information from the element.
- Step 7** (Optional) Define a description, SNMP write community, and user name and password in the relevant fields.
- Step 8** Click **Enabled** to activate the new access settings.
- Step 9** Click **OK** to save the information to the Network Manager database.
- 

## Removing an Element Type from the Auto-detect Mechanism

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Auto-detect**.

- Step 3** Do one of the following:
- Select the element type you require and click **Delete**.
  - Right-click the element type you require and select **Delete**.
- Step 4** Click **OK** to save your changes.
- 

## Accessing an Element Web User Interface

### Procedure

---

- Step 1** Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- Step 2** Right-click the element you require and select **Open element manager**
- or–
- Click the link to the name or IP address of the element.
- 

## Accessing the Monitor Tab for a Specified Element

### Procedure

---

- Step 1** Click **Network Table** in the sidebar menu.
- Step 2** Double-click the element you require the table.
-



# CHAPTER 19

## Managing Endpoints in Network Manager

---

- [Defining Default Endpoint Access Settings, page 19-1](#)
- [How to Override Default Endpoint Settings, page 19-2](#)
- [Retrieving Configuration Parameters, page 19-4](#)
- [How to Upgrade Endpoint Software, page 19-5](#)
- [How to Manage Endpoint Configuration Files, page 19-7](#)
- [Updating Configuration for Selected Endpoints, page 19-9](#)
- [Upgrading Software for Selected Endpoints, page 19-10](#)
- [How to Manage the Endpoint Upload Log, page 19-11](#)

### Defining Default Endpoint Access Settings

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

Default access settings for common endpoint types recognized by the Network Manager allow elements such as MCUs and gateways to access these endpoints.



**Note**

---

You can override default access settings for a specified endpoint at Network Tree > Endpoints.

---

**Procedure**

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.
- Step 3** Click **Access**.

- Step 4** Select an element type.
  - Step 5** Define a user name and password in the relevant fields.
  - Step 6** Click **Upload** to save the information to the Network Manager database.
- 

## How to Override Default Endpoint Settings

- [Overriding Default Endpoint Addressing, page 19-2](#)
- [Overriding Default Access Settings for a Selected Endpoint, page 19-3](#)
- [Configuring Endpoint Dialing, page 19-3](#)

## Overriding Default Endpoint Addressing

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the endpoint you require in the tree.
  - Step 3** Click **Endpoints**.
  - Step 4** Do one of the following:
    - Select the endpoint you require and click **Configure**.
    - Double-click the endpoint you require.
  - Step 5** Click the **Configure** tab.
  - Step 6** Select a gatekeeper IP address from the list of gatekeepers available on the network.
  - Step 7** Enter an E.164 number for the endpoint.
  - Step 8** Enter an H.323 alias for the endpoint.
  - Step 9** Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
-

## Overriding Default Access Settings for a Selected Endpoint

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the endpoint you require in the tree.
- Step 3** Click **Endpoints**.
- Step 4** Do one of the following:
- Select the endpoint you require and click **Configure**.
  - Double-click the endpoint you require.
- Step 5** Click the **Access** tab.
- Step 6** Select an endpoint from the list of supported endpoints.
- Step 7** Check **Use default access** to use default access settings defined by the endpoint.
- Step 8** Enter the user name required for communicating with the endpoint.
- Step 9** Enter the password required for communicating with the endpoint.
- Step 10** Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
- 

## Configuring Endpoint Dialing

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

**Procedure**

- 
- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the endpoint you require in the tree.
- Step 3** Click **Endpoints**.
- Step 4** Do one of the following:
- Select the endpoint you require and click **Configure**.
  - Double-click the endpoint you require.
- Step 5** Click the **Dial** tab.
- Step 6** In the Dial to address field, specify the address that you want this endpoint to call.
- Step 7** In the Dial to network endpoint field, specify the network endpoint that you want this endpoint to call.
- Step 8** Check **Log** to display a log of events for the current call.
- Step 9** Click **Connect** to connect the endpoint to a call at the specified address or with the selected endpoint.
- Step 10** Click **Dial Parameters** to specify the call type and whether the call is restricted to other incoming callers.
- Step 11** Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
- 

## Retrieving Configuration Parameters

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

You can retrieve configuration parameters from an endpoint and save configuration information to a file accessed from Settings > Endpoint Management > Configuration Files.

**Procedure**

- 
- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the endpoint you require in the tree.
- Step 3** Do one of the following:
- Click **Endpoints** and then click **Retrieve configuration file**.
  - Right-click the endpoint you require and select **Retrieve configuration file**.

The Retrieve configuration file button is available for Sony PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30 and PCS-TL50 endpoints. For PCS-1600 only the Update configuration button is available.

The Retrieve Configuration File window shows a list of the configuration files that were previously retrieved.

- Step 4** Enter the name that you would like to give to the configuration file.
  - Step 5** Enter a description of the file.
  - Step 6** Click **OK** to save the file in the Network Manager database.
- 

## How to Upgrade Endpoint Software

Network Manager enables you to manage software upgrade files for the endpoints on your network that support a software upgrade (PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30 or PCS-TL50).

- [Adding a Software Upgrade File, page 19-5](#)
- [Modifying a Software Upgrade File, page 19-6](#)
- [Removing a Software Upgrade File, page 19-6](#)

## Adding a Software Upgrade File

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Endpoint Management**.
  - Step 3** Click **Software Upgrade Files**.
  - Step 4** Select the type of endpoint you require in the Endpoint type field.
  - Step 5** Click **Add**.
  - Step 6** Enter the full path of the software upgrade file to be added to the Network Manager database, or browse to the file.
  - Step 7** Enter a name and description for the upgrade file in the relevant fields.
  - Step 8** Click **OK** to save your changes.
-

## Modifying a Software Upgrade File

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50

You can change the name and description of a software upgrade file that you have already added to Network Manager.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Endpoint Management**.
  - Step 3** Click **Software Upgrade Files**.
  - Step 4** Select the type of endpoint you require in the Endpoint type field.
  - Step 5** Do one of the following:
    - Double-click the software upgrade file you require.
    - Select the software upgrade file you require and click **Edit**.
    - Right-click the software upgrade file you require and select **Edit**.
  - Step 6** Enter a new name and description for the upgrade file in the relevant fields.
  - Step 7** Click **OK** to save your changes.
- 

## Removing a Software Upgrade File

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.

- Step 3** Click **Software Upgrade Files**.
- Step 4** Select the type of endpoint you require in the Endpoint type field.
- Step 5** Do one of the following:
- Select the software upgrade file you require and click **Delete**.
  - Right-click the software upgrade file you require and select **Delete**.
- Step 6** Click **OK** to save your changes.
- The software upgrade file is removed from the database.
- 

## How to Manage Endpoint Configuration Files

Network Manager enables you to manage endpoint configuration files for the endpoints on your network that support an update configuration (PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30, PCS-TL50 or PCS-1600).

- [Viewing Saved Endpoint Configuration Files, page 19-7](#)
- [Modifying an Endpoint Configuration File, page 19-8](#)
- [Removing an Endpoint Configuration File, page 19-8](#)

## Viewing Saved Endpoint Configuration Files

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.
- Step 3** Click **Configuration Files**.
- Step 4** Select the type of endpoint you require in the Endpoint type field.
- The Configuration Files tab displays the configuration files previously retrieved from endpoints and saved in the Network Manager database.
-

## Modifying an Endpoint Configuration File

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

You can change the name and description of an endpoint configuration file that you have already added to Network Manager.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Endpoint Management**.
  - Step 3** Click **Configuration Files**.
  - Step 4** Select the type of endpoint you require in the Endpoint type field.
  - Step 5** Do one of the following:
    - Double-click the endpoint configuration file you require.
    - Select the endpoint configuration file you require and click **Edit**.
    - Right-click the endpoint configuration file you require and select **Edit**.
  - Step 6** Enter a new name and description for the configuration file in the relevant fields.
  - Step 7** Click **OK** to save your changes.
- 

## Removing an Endpoint Configuration File

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.
- Step 3** Click **Configuration Files**.
- Step 4** Select the type of endpoint you require in the Endpoint type field.
- Step 5** Do one of the following:
- Select the log entry you require and click **Delete**.
  - Right-click the log entry you require and select **Delete**.
- Step 6** Click **OK** to save your changes.
- Step 7** Click **OK** to save your changes.
- The endpoint configuration file is removed from the database.
- 

## Updating Configuration for Selected Endpoints

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

The Update configuration button enables you to update selected endpoints with a configuration file that has been previously retrieved and saved at Settings > Endpoint Management > Configuration Files.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the endpoint you require in the tree.
- Step 3** Do one of the following:
- Click **Endpoints** and then click **Update configuration**.
  - Right-click the endpoint you require and select **Update configuration**.

The Update configuration button is available for Sony PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30 and PCS-TL50 endpoints. For PCS-1600 only the Update configuration button is available.

The Update configuration window shows a list of the configuration files stored in the Network Manager database that are associated with the selected endpoint types.

Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.

- Step 4** Select the file with which to update the selected endpoints.
- Step 5** Click **OK** to start updating endpoint configuration.
- 

## Upgrading Software for Selected Endpoints

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

The Upgrade software button enables you to upgrade the software version of selected endpoints with a software file that has been previously saved in the Network Manager database Settings > Endpoint Management > Software Upgrade Files.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the endpoint you require in the tree.
- Step 3** Do one of the following:
- Click **Endpoints** and then click **Upgrade software**.
  - Right-click the endpoint you require and select **Upgrade software**.

The Upgrade software button is available for Sony PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30 and PCS-TL50 endpoints. For PCS-1600 only the Update configuration button is available.

The Upgrade software window appears, showing a list of the software upgrade files stored in the Network Manager database that are associated with the selected endpoint types.

- Step 4** Select the file with which to update the selected endpoints.
- Step 5** Click **OK** to start upgrading endpoint software.
- 

## Upgrading Sony Endpoints

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50

- PCS-G70
- PCS-TL30
- PCS-TL50

#### Procedure

---

- Step 1** Request from your Sony distributor the software upgrade file that can be used with the Network Manager.
- Step 2** Save the file that you received from the distributor in the Network Manager database.
- Step 3** Upgrade the endpoints software with the file that was received from the distributor.



**Note** Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.

---

## How to Manage the Endpoint Upload Log

Network Manager enables you to manage the upload log for endpoints that support a software upgrade (PCS-1, PCS-11, PCS-G50, PCS-G70, PCS-TL30 or PCS-TL50) or an update configuration (all of these + PCS-1600).

- [Viewing Your Endpoint Configuration Upload History, page 19-11](#)
- [Uploading a File After a Failed Attempt, page 19-12](#)
- [Removing Entries from the Upload Log, page 19-12](#)

## Viewing Your Endpoint Configuration Upload History

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

#### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.
- Step 3** Click **Upload Log**.

**Step 4** Select the type of endpoint you require in the Endpoint type field.

The Upload Log tab displays the history of all your attempts to upload a software upgrade file, and shows all scheduled future upload attempts.

---

## Uploading a File After a Failed Attempt

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

**Step 1** Click **Settings** in the sidebar menu.

**Step 2** Click **Endpoint Management**.

**Step 3** Click **Upload Log**.

**Step 4** Select the type of endpoint you require in the Endpoint type field.

**Step 5** Do one of the following to attempt to upload an endpoint configuration file after a previous upload attempt has failed:

- Select the log entry you require and click **Retry**.
- Right-click the log entry you require and select **Retry**.

**Step 6** Click **OK** to save your changes.

---

## Removing Entries from the Upload Log

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G50
- PCS-G70
- PCS-TL30
- PCS-TL50
- PCS-1600

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Endpoint Management**.
- Step 3** Click **Upload Log**.
- Step 4** Select the type of endpoint you require in the Endpoint type field.
- Step 5** Do one of the following to remove a single log entry:
- Select the log entry you require and click **Delete**.
  - Right-click the log entry you require and select **Delete**.
- Step 6** Click **OK** to save your changes.
- Step 7** Click **Delete All** to remove all entries from the log.
- Step 8** Click **OK** to save your changes.
-





## CHAPTER 20

# Managing the Internal Gatekeeper in Network Manager

---

- [How to Manage Services, page 20-1](#)
- [How to Manage Prefixes, page 20-4](#)
- [How to Configure a Parent Gatekeeper, page 20-5](#)
- [How to Manage Parent Filters, page 20-6](#)
- [How to Configure a Child Gatekeeper, page 20-7](#)
- [How to Manage Child Prefixes, page 20-9](#)
- [How to Configure a Neighbor, page 20-10](#)
- [How to Manage Zones, page 20-11](#)
- [How to Manage Bandwidth Rules, page 20-12](#)
- [How to Manage Debug Flags, page 20-14](#)

## How to Manage Services

- [Viewing Internal Gatekeeper Supported Services, page 20-1](#)
- [Creating or Modifying a Service, page 20-2](#)
- [Viewing Global Services, page 20-3](#)
- [Creating or Modifying a Global Service, page 20-3](#)
- [Removing a Service, page 20-4](#)

## Viewing Internal Gatekeeper Supported Services

The Services tab displays the list of predefined and online services supported by the internal gatekeeper selected in the tree.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.

**Step 3** Click **Services**.

Table 20-1 describes the information displayed on the Services tab.

**Table 20-1 Services Tab Parameters**

| Parameter          | Description   |
|--------------------|---|
| Prefix             | Prefix used to access the service                                     |
| Description        | Service description   |
| Status             | Whether the service is predefined or online (meaning, service status) |
| Conference Hunting | Whether conference hunting is enabled for the service                 |
| In-Zone Default    | Default policy for in-zone endpoints                                  |
| Out of ZoneS       | Service policy for out-of-zone endpoints                              |

## Creating or Modifying a Service

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Services**.
- Step 4** Do one of the following to modify an existing service:
- Double-click the service you require.
  - Select the service you require and click **Edit**.
  - Right-click the service you require and select **Edit**.
- Step 5** Do one of the following to create a new service:
- Click **Add**.
  - Right-click any existing service and select **Add**.
- Step 6** Enter the prefix used to access the service.
- Step 7** Select the service type.
- Step 8** Enter a description of the service.
- Step 9** Select whether to enable conference hunting.
- Step 10** Select whether to allow access to in-zone endpoints.
- Step 11** Select whether to allow access to out-of-zone endpoints.
- Step 12** Click **OK** to save your changes.
-

## Viewing Global Services

The Global Services tab displays the list of global services which can be configured for the selected internal gatekeeper.

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Global Services**.

[Table 20-2](#) describes the information displayed on the Global Services tab.

**Table 20-2 Global Services Tab Parameters**

| Parameter        | Description  |
|------------------|--|
| Prefix           | Prefix used to access the service  |
| Description      | Service description  |
| Central Database | Indicates whether or not the global service was retrieved from the central database. |

---

## Creating or Modifying a Global Service

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Global Services**.
  - Step 4** Do one of the following to modify an existing global service:
    - Double-click the service you require.
    - Select the service you require and click **Edit**.
    - Right-click the service you require and select **Edit**.
  - Step 5** Do one of the following to create a new global service:
    - Click **Add**.
    - Right-click any existing service and select **Add**.
  - Step 6** Enter the prefix used to access the service.
  - Step 7** Enter a description of the service.
  - Step 8** Click **OK** to save your changes.
-

## Removing a Service

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Services** or **Global Services**.
- Step 4** Do one of the following:
- Select the service you require and click **Delete**.
  - Right-click the service you require and select **Delete**.
- Step 5** Click **OK** to save your changes.
- The service is removed from the database.
- 

## How to Manage Prefixes

The Prefixes tab enables you to assign prefixes to local and remote Cisco IOS H.323 Gatekeeper zones, configure the method for sending LRQ messages to each destination for address resolution and assign gateway priorities.

- [Creating or Modifying a Prefix, page 20-4](#)
- [Removing a Prefix, page 20-5](#)

## Creating or Modifying a Prefix

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Prefixes**.
- Step 4** Select the prefix you require and click **Edit** to modify an existing prefix.
- Step 5** Click **Add** to create a new prefix.
- Step 6** Configure prefixes with which the Cisco IOS H.323 Gatekeeper performs address resolution, sends LRQ messages simultaneously and configures gateway priorities per zone.
- Step 7** (Optional) Select a zone, enter a prefix number and select **Blast** to send LRQ messages simultaneously.
- Step 8** Click **Upload** to save your changes to the internal gatekeeper database.
-

## Removing a Prefix

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Prefixes**.
  - Step 4** Select the prefix you require and click **Delete**.
  - Step 5** Click **Yes** to remove the prefix from the internal gatekeeper database.
- 

## How to Configure a Parent Gatekeeper

The internal gatekeeper sends an LRQ to the parent gatekeeper when the zone prefix of the call matches one of the defined parent filters. If the internal gatekeeper fails to match the zone prefix of the call with any of the defined parent filters, the internal gatekeeper either rejects the call or forwards the call according to the Call Fallback settings configured in the internal gatekeeper element manager. Where no filters are defined, the internal gatekeeper passes the call to the parent gatekeeper. The internal gatekeeper allows a maximum of ten parent filters.

- [Enabling the Parent Tab, page 20-5](#)
- [Adding a Parent Manually, page 20-6](#)
- [Adding a Parent Automatically, page 20-6](#)

## Enabling the Parent Tab

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Configure**.
  - Step 4** Select **Version 2** in the Dial plan version field.
  - Step 5** Ensure that Use Central Database is unselected.
  - Step 6** Click **Upload** to save your changes.
-

## Adding a Parent Manually

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Parent**.
  - Step 4** Check **Enabled**.
  - Step 5** Enter the IP address, port number and description of the parent gatekeeper in the relevant fields.
  - Step 6** (Optional) Add a parent filter.
  - Step 7** Click **Upload** to save your changes.
- 

## Adding a Parent Automatically

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Drag and drop the internal gatekeeper element into the zone of the gatekeeper you wish to configure as the parent gatekeeper.  
The internal gatekeeper Parent tab is automatically updated with the parent gatekeeper details.
- 

## How to Manage Parent Filters

- [Creating or Modifying a Parent Filter, page 20-6](#)
- [Removing a Parent Filter, page 20-7](#)

## Creating or Modifying a Parent Filter

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Parent**.
- Step 4** Locate the Parent Filters section.
- Step 5** Select the parent filter you require and click **Edit** to modify an existing parent filter.
- Step 6** Click **Add** to create a new parent filter.

- Step 7** Enter a name for the parent filter and click **OK**.
- Step 8** Click **Upload** to save the filter to the internal gatekeeper database.
- 

## Removing a Parent Filter

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Parent**.
- Step 4** Locate the Parent Filters section.
- Step 5** Select the parent filter you require and click **Delete**.
- Step 6** Click **Yes** to remove the filter from the internal gatekeeper database.
- 

## How to Configure a Child Gatekeeper

- [Enabling the Children Tab, page 20-7](#)
- [Viewing Child Gatekeepers, page 20-8](#)
- [Adding a Child Automatically, page 20-9](#)
- [Adding a Child Manually, page 20-8](#)

## Enabling the Children Tab

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Configure**.
- Step 4** Select **Version 2** in the Dial plan version field.
- Step 5** Ensure that **Use Central Database** is unselected.
- Step 6** Click **Upload** to save your changes.
-

## Viewing Child Gatekeepers

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Children**.

[Table 20-3](#) describes the information displayed on the Children tab.

**Table 20-3** *Children Tab Parameters*

| Parameter        | Description  |
|------------------|--|
| Description      | Displays the child gatekeeper description in free text.  |
| Prefixes         | Displays the zone prefix.  |
| IP Address       | Displays the IP address of the child gatekeeper.   |
| Port             | Displays the port number of the child gatekeeper.  |
| Proxy            | Indicates whether or not the internal gatekeeper routes calls from this zone to the neighbor gatekeeper through the Cisco Proxy. |
| Central Database | Indicates whether or not the child gatekeeper was retrieved from the central database.   |

---

## Adding a Child Manually

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Children**.
  - Step 4** Click **Add**.
  - Step 5** Enter the IP address, port number and description of the parent gatekeeper in the relevant fields.
  - Step 6** (Optional) Select **Use Cisco Proxy** to route calls from this zone to the neighbor gatekeeper via the Cisco Proxy.
  - Step 7** Add required prefixes from the list of defined child prefixes.  
 The internal gatekeeper sends an LRQ to the child gatekeeper when the zone prefix of the call matches one of the defined child prefixes. If the internal gatekeeper fails to match the zone prefix of the call with any of the defined child gatekeeper prefixes, the internal gatekeeper passes the call to a neighbor gatekeeper.
  - Step 8** Click **Upload** to save your changes to the internal gatekeeper database.
-

## Adding a Child Automatically

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Drag and drop the internal gatekeeper element you wish to configure as the child gatekeeper into the zone of the current internal gatekeeper.
- The Children tab of the parent internal gatekeeper is automatically updated with the child gatekeeper details.
- 

## How to Manage Child Prefixes

- [Creating or Modifying a Child Prefix, page 20-9](#)
- [Removing a Child Prefix, page 20-9](#)

## Creating or Modifying a Child Prefix

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Children**.
- Step 4** Open the required child gatekeeper profile.
- Step 5** Select the prefix you require and click **Edit** to modify an existing prefix.
- Step 6** Click **Add** to create a new prefix.
- Step 7** Enter a name for the prefix and click **OK**.
- Step 8** Click **Upload** to save the prefix to the internal gatekeeper database.
- 

## Removing a Child Prefix

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Children**.
- Step 4** Open the required child gatekeeper profile.

- Step 5** Select the prefix you require and click **Delete**.
- Step 6** Click **Yes** to remove the prefix from the internal gatekeeper database.
- 

## How to Configure a Neighbor

Under the recommended Cisco architecture, configure the Cisco Unified Videoconferencing Manager internal gatekeeper as the neighbor of external Cisco IOS Gatekeepers.

For more information, refer to the Cisco Unified Videoconferencing Solution Reference Network Design (SRND) Guide at <http://cisco.com/en/US/docs/video/cuvc/design/guides/srnd/vc5xsrnd.html>.

- [Viewing Neighbor Gatekeepers, page 20-10](#)
- [Adding or Modifying a Neighbor Gatekeeper, page 20-11](#)

## Viewing Neighbor Gatekeepers

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Neighbors**.

[Table 20-4](#) describes the information displayed on the Neighbors tab.

**Table 20-4** *Neighbors Tab Parameters*

| Parameter   | Description  |
|-------------|--|
| Description | Displays the neighbor gatekeeper description.  |
| Prefix      | Displays the zone prefix.  |
| ID Address  | Displays the neighbor gatekeeper IP address.   |
| Port        | Displays the port number of the neighbor gatekeeper.   |
| Proxy       | Indicates whether or not the internal gatekeeper routes all calls from this zone to the neighbor gatekeeper through the Cisco Proxy. |
| GK ID       | Displays the neighbor gatekeeper identifier.   |
| Central DB  | Indicates whether or not the neighbor gatekeeper was retrieved from the central database.  |
| LDAP        | Indicates whether or not the neighbor gatekeeper was retrieved from the LDAP server.   |

---

## Adding or Modifying a Neighbor Gatekeeper

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Neighbors**.
- Step 4** Do one of the following to modify an existing neighbor gatekeeper:
- Double-click the internal gatekeeper you require.
  - Select the internal gatekeeper you require and click **Edit**.
  - Right-click the internal gatekeeper you require and select **Edit**.
- Step 5** Do one of the following to create a new service:
- Click **Add**.
  - Right-click any existing internal gatekeeper and select **Add**.
- Step 6** Enter the neighbor gatekeeper zone prefix.
- Step 7** Enter the description, IP address and port number of the neighbor gatekeeper in the relevant fields.
- Step 8** (Optional) Select **Use Cisco Proxy** to route calls from this zone to the neighbor gatekeeper via the Cisco Proxy.
- Step 9** Click **Upload** to save your changes to the internal gatekeeper database.
- 

## How to Manage Zones

- [Creating or Modifying a Local Zone, page 20-11](#)
- [Creating or Modifying a Remote Zone, page 20-12](#)
- [Removing a Zone, page 20-12](#)

## Creating or Modifying a Local Zone

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Local Zones**.
- Step 4** Select the zone you require and click **Edit** to modify an existing local zone.
- Step 5** Click **Add** to create a new local zone.

- Step 6** Enter a zone name and the zone domain.
- Step 7** Click **Upload** to save your changes to the internal gatekeeper database.
- 

## Creating or Modifying a Remote Zone

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Remote Zones**.
- Step 4** Select the zone you require and click **Edit** to modify an existing remote zone.
- Step 5** Click **Add** to create a new remote zone.
- Step 6** Enter a zone name, zone domain, IP address and port.
- Step 7** Click **Upload** to save your changes to the internal gatekeeper database.
- 

## Removing a Zone

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Local Zones** or **Remote Zones**.
- Step 4** Select the zone you require and click **Delete**.
- Step 5** Click **Yes** to remove the zone from the internal gatekeeper database.
- 

## How to Manage Bandwidth Rules

The BW Rules tab enables you control the bandwidth of H.323 traffic both in the Cisco IOS H.323 Gatekeeper zone and between the Cisco IOS H.323 Gatekeeper and other zones. Bandwidth rules per session or specific zones can also be specified. A default setting specifies a bandwidth rule for all zones with which the Cisco IOS H.323 Gatekeeper operates.

- [Viewing Bandwidth Rules, page 20-13](#)
- [Creating or Modifying a Bandwidth Rule, page 20-13](#)
- [Removing a Bandwidth Rule, page 20-14](#)

## Viewing Bandwidth Rules

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **BW Rules**.
- [Table 20-5](#) describes the information displayed on the BW Rules tab.

**Table 20-5** *BW Rules Tab Parameters*

| Parameter | Description  |
|-----------|--|
| Scope     |  |
| Total     | Indicates the total amount of bandwidth for H.323 traffic allowed in this zone.              |
| Remote    | Indicates the total amount of bandwidth for H.323 traffic from this zone to all other zones. |
| Interzone | Indicates the total amount of bandwidth for H.323 traffic from this zone to another zone.    |
| Session   | Indicates the maximum bandwidth allowed for a session in the zone.                           |
| Default   | Indicates the default value for all zones is configured in this rule.                        |

---

## Creating or Modifying a Bandwidth Rule

### Procedure

- 
- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **BW Rules**.
  - Step 4** Select the rule you require and click **Edit** to modify an existing bandwidth rule.
  - Step 5** Click **Add** to create a new bandwidth rule.
  - Step 6** Select the scope of the bandwidth rule, indicate whether the rule is the default for all zones, select a zone and maximum bandwidth rate.
  - Step 7** Click **Upload** to save your changes to the internal gatekeeper database.
-

## Removing a Bandwidth Rule

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **BW Rules**.
  - Step 4** Select the bandwidth rule you require and click **Delete**.
  - Step 5** Click **Yes** to remove the bandwidth rule from the internal gatekeeper database.
- 

## How to Manage Debug Flags

- [Creating or Modifying a Debug Flag, page 20-14](#)
- [Removing a Debug Flag, page 20-14](#)

## Creating or Modifying a Debug Flag

### Restriction

Too many debug flags might inhibit the performance of the Cisco IOS H.323 Gatekeeper on the network.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the internal gatekeeper you require in the tree.
  - Step 3** Click **Debug Flags**.
  - Step 4** Select the flag you require and click **Edit** to modify an existing debug flag rule.
  - Step 5** Click **Add** to create a new debug flag.
  - Step 6** Enter the debug flag name, a description and enable the flag.
  - Step 7** Click **Upload** to save your changes to the internal gatekeeper database.
- 

## Removing a Debug Flag

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the internal gatekeeper you require in the tree.
- Step 3** Click **Debug Flags**.

- Step 4** Select the debug flag you require and click **Delete**.
- Step 5** Click **Yes** to remove the debug flag from the internal gatekeeper database.
-





# CHAPTER 21

## Managing an MCU in Network Manager

---

MCU configuration options vary according to MCU version.

- [Setting Call Routing Devices, page 21-1](#)
- [Viewing Registered Multipoint Processors, page 21-1](#)
- [How to Manage Multipoint Processors, page 21-2](#)
- [Viewing MCU Supported Services, page 21-3](#)
- [Configuring MCU Unit Type and Addressing, page 21-3](#)

### Setting Call Routing Devices

#### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the MCU you require in the tree.
  - Step 3** Click **Protocols**.
  - Step 4** Click **Use H.323 Gatekeeper** or **Use SIP Server** to determine the MCU call routing device.
  - Step 5** Enter an IP address port value in the relevant fields.
  - Step 6** Click **Upload** to save your changes.
- 

### Viewing Registered Multipoint Processors

The term “Multipoint Processors” (MPs) refers to MCUs and EMPs.

#### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the MCU you require in the tree.
- Step 3** Click **Registered MPs** to view the list of MPs currently registered with the MCU.

Table 21-1 describes the information displayed on the Registered MPs tab.

**Table 21-1 Registered MPs Tab Parameters**

| Parameter   | Description  |
|-------------|--|
| Type        | Displays the type of MP unit registered with the current MCU. MP unit types supported include:   |
| MP          | The local MP component of the current MCU or an MCU operating in <i>MP Only</i> mode. Performs basic media processing such as audio transcoding, video processing and video switching. |
| EMP         | Unit performing advanced media processing such as video processing and video switching.  |
| Address     | Address of the MP unit. This might be the same as the current MCU if the MP is the media processing component of the current unit.   |
| Description | Version number and type.   |

## How to Manage Multipoint Processors

The MP List tab enables you to define the MPs being controlled by an MCU in a clustered layout (local MPs or MCUs configured as MP only). Up to six MPs can be controlled by a single MCU in this type of layout.

- [Creating and Modifying an MP Profile, page 21-2](#)
- [Removing an MP Profile, page 21-3](#)

## Creating and Modifying an MP Profile

### Procedure

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the MCU you require in the tree.
- Step 3** Click **MP List**.
- Step 4** Select the MP you require and click **Edit** to modify an existing MP profile.
- Step 5** Click **Add** to create a new MP profile.
- Step 6** Enter the IP address and optional description of MPs controlled by the selected MCU.
- Step 7** Select **Enable** to activate the MP profile.
- Step 8** Click **OK** to save your changes.

## Removing an MP Profile

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the MCU you require in the tree.
  - Step 3** Click **MP List**.
  - Step 4** Select the MP profile you require and click **Delete**.
  - Step 5** Click **Upload** to save your changes.
- 

## Viewing MCU Supported Services

The Services tab displays the list of services supported by the selected MCU. Services can be edited by clicking the link to the MCU element manager above the Services table.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the MCU you require in the tree.
  - Step 3** Click **Services**.
- 

## Configuring MCU Unit Type and Addressing

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the MCU you require in the tree.
- Step 3** Click **Configure**.

[Table 21-2](#) describes the information displayed on the Configure tab.

**Table 21-2**      **Configure Tab Parameters**

| <b>Parameter</b> | <b>Description</b>   |
|------------------|--|
| Unit Type        | <ul style="list-style-type: none"><li>• MCU—The MCU and MP components in the unit work together to provide Call Setup, conference control and media processing.</li><li>• MP Only—The MP (Multipoint Processor) unit works in a clustered arrangement operating under the control of an MCU.</li></ul> |
| Location         | Enter a string identifying the physical location of the MCU device.  |
| MCU IP Address   | MCU IP address. Configurable only on MP units.   |
| Port             | MCU communication port. Configurable only on MP units.   |



## CHAPTER 22

# Managing a Gateway in Network Manager

---

- [How to Manage Services, page 22-1](#)
- [Configuring Gateway Addressing, page 22-2](#)

## How to Manage Services

- [Viewing Gateway Supported Services, page 22-1](#)
- [Creating or Modifying a Service, page 22-1](#)
- [Removing a Service, page 22-2](#)

## Viewing Gateway Supported Services

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
  - Step 2** Select the gateway you require in the tree.
  - Step 3** Click **Services**.
- 

## Creating or Modifying a Service

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the gateway you require in the tree.
- Step 3** Click **Services**.
- Step 4** Do one of the following to modify an existing service:
  - Double-click the service you require.
  - Select the service you require and click **Edit**.

- Right-click the service you require and select **Edit**.
- Step 5** Do one of the following to create a new service:
- Click **Add**.
  - Right-click any existing service and select **Add**.
- Step 6** Enter the service prefix description.
- Step 7** Select the call type and bit rate.
- Step 8** Click **OK**.
- 

## Removing a Service

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the gateway you require in the tree.
- Step 3** Click **Services**.
- Step 4** Do one of the following:
- Select the service you require and click **Delete**.
  - Right-click the service you require and select **Delete**.
- Step 5** Click **OK** to save your changes.
- The service is removed from the database.
- 

## Configuring Gateway Addressing

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the gateway you require in the tree.
- Step 3** Click **Configure**.
- Step 4** Enter the IP address of the gatekeeper with which the gateway registers.
- Step 5** (Optional) Enter a string identifying the physical location of the gateway.
-



## CHAPTER 23

# Configuring a User Profile in Network Manager

---

- [Creating or Modifying a User Profile, page 23-1](#)
- [Removing a User Profile, page 23-2](#)
- [How to Define Network Subsets, page 23-2](#)

## Creating or Modifying a User Profile

Network Manager supports three types of network users:

- Administrator—Full read/write access to all managed elements and zones on the network.
- Read only—Read Only access to all elements and zones on the network.
- Local user—Restricted access to managed elements and zones on the network. This user profile is defined with specific read/write and read only access according to zones, elements and criteria for network subsets configured at Settings > Network Subsets.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Users**.
- Step 3** Do one of the following to modify an existing user profile:
  - Double-click the link in the User Name column for the user you require.
  - Select the user you require and click **Edit**.
  - Right-click the link in the User Name column for the user you require and select **Edit**.
- Step 4** Do one of the following to create a new user profile:
  - Click **Add**.
  - Right-click any link in the User Name column and select **Add**.
- Step 5** Enter a name and password for the user in the relevant fields, and select the appropriate user access level.
- Step 6** (For local users only) Select read/write access and read only access permissions according to zones and criteria for network subsets defined at Settings > Network Subsets.

- Step 7** (For local users only) Select **Can add elements** to enable a local user to add new elements to the Network Manager database throughout all network zones and subsets.
- Step 8** Click **OK** to save your changes.
- 

**Related Topics**

- [How to Define Network Subsets, page 23-2](#)

## Removing a User Profile

**Procedure**

- 
- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Users**.
- Step 3** Do one of the following:
- Select the user you require and click **Delete**.
  - Right-click the link in the User Name column for the user you require and select **Delete**.
- Step 4** Click **OK** to save your changes.
- The user profile is removed from the database.
- 

## How to Define Network Subsets

Network subsets enable you to define areas of the network according to zones and element types using include and exclude criteria for use with Local user access level profiles.

- [Creating or Modifying a Network Subset, page 23-2](#)
- [Removing a Network Subset, page 23-3](#)
- [Removing an Include or Exclude Criterion, page 23-4](#)

## Creating or Modifying a Network Subset

**Procedure**

- 
- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Network Subsets**.
- Step 3** Do one of the following to modify an existing network subset:
- Double-click the network subset you require.
  - Select the network subset you require and click **Edit**.
  - Right-click the network subset you require and select **Edit**.

- Step 4** Do one of the following to create a new network subset:
- Click **Add**.
  - Right-click any network subset and select **Add**.
- Step 5** Enter a name for the network subset.
- A subset contains all elements which match at least one include criterion but do not match any exclude criterion.
- Step 6** Do one of the following to modify an existing include or exclude criterion:
- Double-click the criterion you require.
  - Select the criterion you require and click **Edit**.
  - Right-click the criterion you require and select **Edit**.
- Step 7** Do one of the following to create a new include or exclude criterion:
- Click **Add**.
  - Right-click any criterion and select **Add**.
- Step 8** Select a zone and element type in the relevant fields, and indicate whether or not child zones of the specified zone are contained in the criterion.
- Step 9** Click **OK** to add the criterion to the relevant list in the Add Network Subset window.
- Step 10** Click **OK** to save your changes.
- 

#### Related Topics

- [Creating or Modifying a User Profile, page 23-1](#)

## Removing a Network Subset

#### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Network Subsets**.
- Step 3** Do one of the following:
- Select the network subset you require and click **Delete**.
  - Right-click the network subset you require and select **Delete**.
- Step 4** Click **OK** to save your changes.
-

## Removing an Include or Exclude Criterion

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Network Subsets**.
- Step 3** Do one of the following:
- Double-click the network subset you require.
  - Select the network subset you require and click **Edit**.
  - Right-click the network subset you require and select **Edit**.
- Step 4** Do one of the following:
- Select the criterion you require and click **Delete**.
  - Right-click the criterion you require and select **Delete**.
- Step 5** Click **OK** to save your changes.
-



## CHAPTER 24

# Managing Traps and Alarms in Network Manager

---

- [Sending Traps to Network Manager, page 24-1](#)
- [Creating or Modifying a Trap Forwarding Rule, page 24-2](#)
- [Disabling a Trap Forwarding Rule, page 24-2](#)
- [Removing a Trap Forwarding Rule, page 24-3](#)
- [Creating or Modifying an Alert Recipient Profile, page 24-3](#)
- [Removing an Alert Recipient Profile, page 24-4](#)
- [Viewing Generated Events, page 24-4](#)
- [Filtering Generated Events, page 24-5](#)
- [Viewing Events per Network Item, page 24-5](#)
- [Viewing and Sorting Supported Alarms, page 24-6](#)
- [Modifying Alarms, page 24-6](#)
- [Viewing and Sorting Generated Alarms, page 24-6](#)
- [Viewing Generated Alarms per Network Item, page 24-7](#)

## Sending Traps to Network Manager

You can configure the managed elements in the network to send SNMP traps to the Network Manager.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Traps**.
  - Step 3** Select **Receive traps from elements**.
  - Step 4** Click **Upload** to save your changes.
-

## Creating or Modifying a Trap Forwarding Rule

You can instruct Network Manager to forward traps received from managed elements to an address specified by a trap forwarding rule.

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Traps**.
  - Step 3** Do one of the following to modify an existing trap forwarding rule:
    - Double-click the trap rule you require.
    - Select the trap rule you require and click **Edit**.
    - Right-click the trap rule you require and select **Edit**.
  - Step 4** Do one of the following to create a new trap forwarding rule:
    - Click **Add**.
    - Right-click any trap rule and select **Add**.
  - Step 5** Enter a description in the Description field.
  - Step 6** Specify the IP address and port number for Network Manager to forward traps received from managed elements.
  - Step 7** Select **Enable trap forwarding**.
  - Step 8** Click **OK** to save your changes.
- 

## Disabling a Trap Forwarding Rule

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Traps**.
  - Step 3** Do one of the following to modify an existing trap forwarding rule:
    - Double-click the trap rule you require.
    - Select the trap rule you require and click **Edit**.
    - Right-click the trap rule you require and select **Edit**.
  - Step 4** Deselect **Enable trap forwarding**.
  - Step 5** Click **OK** to save your changes.
- The trap forwarding rule is disabled but remains in the database.
-

# Removing a Trap Forwarding Rule

## Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Traps**.
- Step 3** Do one of the following:
- Select the trap rule you require and click **Delete**.
  - Right-click the trap rule you require and select **Delete**.
- Step 4** Click **OK** to save your changes.
- The trap forwarding rule is removed from the database.
- 

# Creating or Modifying an Alert Recipient Profile

## Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Alert Recipients**.
- Step 3** Do one of the following to modify an existing alert recipient profile:
- Double-click the alert recipient you require in the Recipient Name column.
  - Select the alert recipient you require and click **Edit**.
  - Right-click the alert recipient you require in the Recipient Name column and select **Edit**.
- Step 4** Do one of the following to create a new alert recipient profile:
- Click **Add**.
  - Right-click any link in the Recipient Name column and select **Add**.
- Step 5** Enter the name and e-mail of the alert recipient in the relevant fields.
- Step 6** Select a user profile.
- The options in the Select user profile field reflect the user details defined at Settings > Users.
- If you select a user profile with Local user access level, the alert recipient receives notifications only for alarms that belong to elements that are part of the network subset defined for the user at Settings > Users.
- If you select a user profile with Administrator or Read only access level, the alert recipient receives notification of all alarms.
- Step 7** Select the minimum severity level of the alerts to be sent to the alert recipient.
- The severity level of alerts is defined by the profile selected in the Select user profile field.
- Step 8** (Optional) Select **Notify on alarms clearing** to enable the alarm recipient to receive an error report via e-mail when the alarms have been cleared.
- Step 9** (Optional) Select **Use custom subject line** to include a custom subject line in the e-mail and enter a string for the custom subject line.

- Step 10** (Optional) Select **Include element info** to include details of the elements reported in the alerts in the custom subject line.
- Step 11** Select **Enable alert** to activate the recipient.
- Step 12** Click **OK** to save your changes.
- 

## Removing an Alert Recipient Profile

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
- Step 2** Click **Alert Recipients**.
- Step 3** Do one of the following:
- Select the alert recipient you require and click **Delete**.
  - Right-click the alert recipient you require in the Recipient Name column and select **Delete**.
- Step 4** Click **OK** to save your changes.
- The alert recipient profile is removed from the database.
- 

## Viewing Generated Events

The Events tab enables you to sort the events reported by the system according to event severity, event time, event message and element.

### Procedure

---

- Step 1** Click **Alarms** in the sidebar menu.
- Step 2** Click **Events**.
- The Events tab displays the following information:
- Event severity level (Minor, Cleared, Intermediate, Warning, Minor, Major, Critical).
  - Date and time of the event.
  - Text message describing the event.
- Step 3** Click the column headings in the alarms table to sort the information displayed.
- Step 4** Double-click any element in the table to display the relevant element manager for that element.
-

# Filtering Generated Events

## Procedure

---

- Step 1** Click **Alarms** in the sidebar menu.
- Step 2** Click **Events**.
- Step 3** Do one of the following:
- Select **View > Filter events**.
  - Click the **Current filter** link above the table.
- Step 4** Define the time period and minimum severity levels of the events to display.
- Step 5** Enter filter criteria and click **OK**.
- The events that correspond to your selection are displayed in the table.
- 

# Viewing Events per Network Item

You can view a table of the events that have occurred in the system related to a specific item in your network.

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Click **Network** or a relevant custom view.
- For information on creating customized views, see the [“Creating a Custom Network Tree View” section on page 17-2](#).
- Step 3** Select the network item you require.
- Step 4** Click **Events**.
- The Events tab includes the event severity level, the date and time of the event and the event message.
- Step 5** (Optional) Double-click the link in the Element column to display the element manager for that element.
- Step 6** (Optional) Do one of the following to filter the events displayed by date and severity level:
- Select **View > Filter events**.
  - Click the **Current filter** link above the table.
-

## Viewing and Sorting Supported Alarms

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Alarms**.
  - Step 3** Click the **Alarm** heading in the alarms table to view alarms generated by the managed elements in the network in alphabetical order.
  - Step 4** Click the **Severity** heading in the alarms table to sort the alarms by increasing or decreasing order of severity.
- 

## Modifying Alarms

### Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Alarms**.
  - Step 3** Do one of the following to modify an alarm generated by the managed elements in the network:
    - Double-click the alarm you require.
    - Select the alarm you require and click **Edit**.
    - Right-click the alarm you require and select **Edit**.
  - Step 4** Modify the severity level, and enable or disable the alarm in the relevant fields.
  - Step 5** Select **Create event for this alarm** to instruct Network Manager to create a report at Alarms > Events every time this alarm occurs.
  - Step 6** Use the **Apply to all users** option to indicate whether the alarm properties apply only to the current user or to all users.
  - Step 7** Click **OK** to save your changes.
- 

## Viewing and Sorting Generated Alarms




The Alarms tab enables you to view and sort the alarms generated by the elements in the network according to alarm status, alarm message, date and time or element.

### Procedure

---

- Step 1** Click **Alarms** in the sidebar menu.
- Step 2** Click **Alarms**.

The Alarms tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:

-  Major/Minor/Critical
-  Information
-  Warning

**Step 3** Double-click any element in the table to display the relevant element manager for that element.

---

## Viewing Generated Alarms per Network Item

You can view a table of all current alarms related to a specific item in your network. Alarms can be viewed per element, network zone or the entire network in one view.

### Procedure

---

**Step 1** Click **Network Tree** in the sidebar menu.




**Step 2** Click **Network** or a relevant custom view.

For information on creating customized views, see the [“Creating a Custom Network Tree View” section on page 17-2](#).

**Step 3** Select the network item you require.

**Step 4** Click **Alarms**.

The Alarms tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:

-  Major/Minor/Critical
  -  Information
  -  Warning
-





## CHAPTER 25

# Managing Calls and Conferences in Network Manager

---

- [Viewing Current Call Details, page 25-1](#)
- [Viewing Current Call Details per Network Item, page 25-2](#)
- [Disconnecting Calls, page 25-2](#)
- [Searching for a Call, page 25-2](#)
- [Viewing Current Conferences, page 25-3](#)
- [Viewing Current Conferences per Network Item, page 25-3](#)
- [Searching for a Conference, page 25-4](#)
- [Accessing the Conference MCU, page 25-4](#)

## Viewing Current Call Details

The Calls tab displays a table providing details of each call currently taking place on the selected element including source and destination aliases, source and destination gatekeepers of the calling parties, call start time and allocated bandwidth.

### Procedure

---

- Step 1** Click **Calls** in the sidebar menu.
  - Step 2** Click **GK Calls**.
  - Step 3** To display extended details per call, click on the table row and click **Show call details**.
-

## Viewing Current Call Details per Network Item

You can view the current status of all calls currently being hosted on the network, zone or selected MCU.

- 
- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Click **Network** or a relevant custom view.  
For information on creating customized views, see the [“Creating a Custom Network Tree View” section on page 17-2](#).
- Step 3** Select the network item you require.
- Step 4** Click **Calls**.
- Step 5** To display extended details per call, click on the table row and click **Show call details**.
- 

## Disconnecting Calls

### Procedure

- 
- Step 1** Click **Calls** in the sidebar menu and then click **GK Calls**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Calls**.
- Step 2** Do one of the following:
- Select the calls you want to disconnect and click **Disconnect selected call**.
  - Click **Disconnect all calls**.
- 

## Searching for a Call

### Procedure

- 
- Step 1** Click **Calls** in the sidebar menu and then click **GK Calls**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Calls**.
- Step 2** Click **Find**.
- Step 3** Enter the call alias, IP address of the endpoint, or service ID.
- Step 4** Click **Find**.
-

## Viewing Current Conferences

The Conferences tab provides a table for viewing the current status of all conferences being hosted on the network, zone or selected MCU.

### Procedure

**Step 1** Click **Calls** in the sidebar menu.

**Step 2** Click **Conferences**.

[Table 25-1](#) describes the information displayed on the Conferences tab.

**Table 25-1** *Conferences Tab Parameters*

| Parameter             | Description  |
|-----------------------|--|
| MCU                   | IP address of the MCU on the which the conference is being hosted. Click on the link to view the element manager of the MCU (Administrator). |
| Conference ID         | Conference ID number. Click on the link to view the conference manager of the MCU (Conference Control).                                      |
| Layout                | Video layout configuration of the conference.  |
| Camera                | Indicates whether video is enabled for the conference.   |
| Speaker               | Indicates whether audio is enabled for the conference.   |
| Data                  | Indicates whether data support is enabled for the conference.  |
| Total Participants    | Number of current participants.  |
| Local Participants    | Number of local participants on this MCU.  |
| Reserved Participants | Number of reserved participants.   |
| Video Bit Rate        | Maximum bit rate for the conference.   |
| Zone                  | Zone in which the conference is taking place.  |

**Step 3** (Optional) Double-click the link in the MCU column to display the element manager for that element.

## Viewing Current Conferences per Network Item

You can view the current status of all conferences currently being hosted on the network, zone or selected MCU.

**Step 1** Click **Network Tree** in the sidebar menu.

**Step 2** Click **Network** or a relevant custom view.

For information on creating customized views, see the [“Creating a Custom Network Tree View”](#) section on page 17-2.

**Step 3** Select the network item you require.

**Step 4** Click **Conferences**.

[Table 25-1](#) describes the information displayed on the Conferences tab.

**Step 5** (Optional) Double-click the link in the MCU column to display the element manager for that element.

---

## Searching for a Conference

### Procedure

---

**Step 1** Click **Calls** in the sidebar menu and then click **Conferences**

–or–

Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Conferences**.

**Step 2** Click **Find** .

**Step 3** Enter the conference ID or the zone prefix.

**Step 4** (Optional) Use the [\*] wildcard to search for conferences.

**Step 5** Click **Find**.

The row in the table matching your search criteria is highlighted.

---

## Accessing the Conference MCU

### Procedure

---

**Step 1** Click **Calls** in the sidebar menu and then click **Conferences**

–or–

Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Conferences**.

**Step 2** To access the element manager of the MCU (Administrator), click the MCU link in the left column of each table row.

**Step 3** To access the MCU Conference Control interface, click the link in the Conference ID column.

This enables you to manage and take control of the conference.

---



## CHAPTER 26

# Configuring Logging for Network Manager

---

- [Viewing Logs for a Selected Element, page 26-1](#)
- [Defining Network Manager Logging Activity, page 26-2](#)
- [Saving Element Logs, page 26-2](#)

## Viewing Logs for a Selected Element

The information displayed on the Logs tab is dependent on the type of element that is selected in the tree. A log of operations is not available for endpoints supported by the Network Manager. A log tab is not available for endpoints when selected in the Network Tree view.

### Procedure

---

- Step 1** Click **Network Tree** in the sidebar menu.
- Step 2** Select the required network element.
- Step 3** Click **Logs**.
- Step 4** Define the log for the various elements, as follows:
- Internal Gatekeeper—Select **Save logs** and select the level of detail to include in the log.
  - MCU—Select **Save logs**, type the log file name and define the level of detail to include in the log.
  - Gateway—Select **Save logs**, type the log file name and define the level of detail to include in the log.
  - Cisco IOS H.323 Gatekeeper—Select **Save logs**, type the log file name and define the level of detail to include in the log.
- Step 5** To view the logs directory from any of the Log tabs described above, click the link.
-

# Defining Network Manager Logging Activity

## Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Logging**.
  - Step 3** Click **Network Manager Logs**.
  - Step 4** Select **Save iView Manager log** to enable logging.
  - Step 5** (Optional) Define the log file name, the maximum file size, the number of backup files to maintain, and the level of log detail in the relevant fields.
  - Step 6** Click the **View log directory** link to view a list of links to log files for Network Manager and managed network elements.
  - Step 7** Click **Upload** to save your changes.
- 

# Saving Element Logs

Network Manager can locally save log files for those elements, such as MCUs and gateways, that do not maintain a log of their own.

## Procedure

---

- Step 1** Click **Settings** in the sidebar menu.
  - Step 2** Click **Logging**.
  - Step 3** Click **Element Logs**.
  - Step 4** Define the maximum size of each log file and the number of backup files to maintain in the relevant fields.
  - Step 5** Click **Upload** to save your changes.
-



## **PART 3**

### **Desktop**



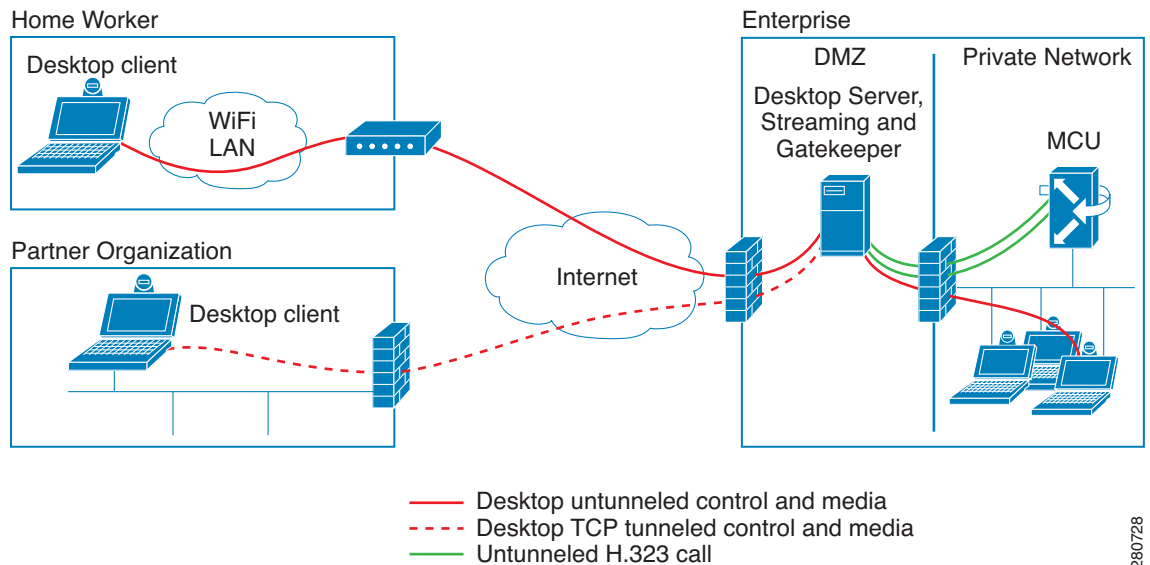


# CHAPTER 27

## Cisco Unified Videoconferencing Desktop Features

Cisco Unified Videoconferencing Desktop is a feature module of the Cisco Unified Videoconferencing Manager product which provides the ability to establish and participate in video conferences using personal computers with Webcams. The Desktop module of the Cisco Unified Videoconferencing Manager consists of a Desktop Server, a Desktop Client component, a Conference Server and a Desktop Recording Server as shown in [Figure 27-1](#).

**Figure 27-1 Basic Desktop Deployment**



[Table 27-1 on page 27-2](#) describes Desktop specifications.

280728

**Table 27-1 Desktop Features**

| Specification  | Description   |
|--|---|
| Client Connectivity Modes  | <ul style="list-style-type: none"> <li>• Live connection (audio, video, data, chat) for interactive participants</li> <li>• Data-only connection with moderation capabilities, optional call back</li> <li>• Streaming mode for non-interactive participants</li> </ul>   |
| Recording and Playback (Optional)  | <ul style="list-style-type: none"> <li>• Records audio, video, data and annotations</li> <li>• Auto posted for easy web access</li> <li>• PIN protected for access security</li> <li>• Permit anyone to record or restrict users<sup>1</sup> by administrator</li> </ul>  |
| Data Collaboration   | <ul style="list-style-type: none"> <li>• H.239 based data collaboration built into the client</li> <li>• Room system-compatible data collaboration format (H.263+ XGA)</li> <li>• Data shared from a room system visible in all other rooms and on desktops</li> <li>• Data shared from a desktop visible on all other desktops and in rooms</li> <li>• Share the entire screen or specific applications</li> <li>• Text chat with emoticons for desktop users</li> </ul> |
| Client Computer Requirements   | <ul style="list-style-type: none"> <li>• Operating System (OS): Windows 2003, Windows XP, Windows Vista, Mac OS X<sup>2</sup></li> <li>• Browsers: Internet Explorer 6, 7 or 8, Firefox 2 or 3, Safari3.1 (used for streaming on Mac OS X operating systems)</li> </ul>   |
| OS Language Supported for the Cisco Unified Videoconferencing Desktop Server | English   |

1. When working with Cisco Unified Videoconferencing Manager.

2. You can install and use Cisco Unified Videoconferencing Desktop Conference Client on computers using the Microsoft Windows and Mac. For the Mac OS, Cisco Unified Videoconferencing Desktop supports limited functionality allowing users to watch webcasts and recordings but not to participate in live meetings.

Table 27-2 describes Desktop features.

**Table 27-2 Desktop Features**

| Feature                             | Description  |
|-------------------------------------|--|
| Meeting Types                       | <ul style="list-style-type: none"> <li>• Unmoderated meetings—Anyone can control the meeting</li> <li>• Moderated meetings—Moderator PIN required to control the meeting</li> <li>• Personal virtual rooms</li> </ul>  |
| Built-In NAT and Firewall Traversal | <ul style="list-style-type: none"> <li>• Traverses local and remote firewall to ensure connectivity</li> <li>• Automatically handles local and remote NAT private networks</li> <li>• Automatic detection of optimal media path: UDP, TCP or tunneled TCP</li> </ul> |

**Table 27-2 Desktop Features (continued)**

| <b>Feature</b>             | <b>Description</b>   |
|----------------------------|--|
| Built-In Streaming         | <ul style="list-style-type: none"> <li>• Built-in streaming server supports ‘watch-only’ participants</li> <li>• Simultaneous streaming of audio, video and data</li> </ul>  |
| Scheduling and Reservation | <ul style="list-style-type: none"> <li>• Outlook plug-in for easy meeting scheduling</li> <li>• Web-based meeting scheduling from any browser</li> <li>• Ports can be reserved assuring availability for critical meetings</li> <li>• Lotus Notes-based scheduling</li> </ul>  |
| Security                   | <ul style="list-style-type: none"> <li>• SRTP encryption to ensure the privacy of media and signaling between Desktop Clients</li> <li>• Waiting room capability – Meeting will not start until moderator joins</li> <li>• Predefined virtual rooms – Optional mode where only predefined virtual rooms can be used for meetings</li> <li>• The Callback feature can be optionally disabled to avoid misuse</li> </ul> |
| Recording Meetings         | <ul style="list-style-type: none"> <li>• Recording meetings</li> <li>• Editing recorded meeting attributes</li> <li>• Managing recordings (moderators only)</li> <li>• Watching recorded meetings<sup>1</sup></li> <li>• Auto-recording scheduled via Cisco Unified Videoconferencing Manager</li> </ul>   |
| User Controls              | <ul style="list-style-type: none"> <li>• Mute/unmute</li> <li>• Enable/disable video camera</li> <li>• Turn on/off local self view</li> <li>• Choose your video layout (active speaker or continuous presence)</li> <li>• Have the system call my voice or video number (callback)</li> <li>• View consolidated conference roster (desktops and rooms)</li> <li>• Request permission to speak when muted</li> </ul>    |
| Moderator Controls         | <ul style="list-style-type: none"> <li>• Acquire moderator rights (may require moderator PIN)</li> <li>• Lock meeting</li> <li>• Terminate meeting</li> <li>• Invite any room system or phone (dial-out)</li> <li>• Start/stop streaming</li> <li>• Start/stop recording</li> <li>• Mute, unmute and disconnect any participant</li> <li>• DTMF keypad</li> <li>• Grant permission to speak</li> </ul>                 |

**Table 27-2 Desktop Features (continued)**

| <b>Feature</b>             | <b>Description</b>   |
|----------------------------|--|
| Layout Selection           | <ul style="list-style-type: none"> <li>• Mixed</li> <li>• Side-by-side video and data</li> <li>• Stacked</li> <li>• Full screen video or data</li> </ul>   |
| Client Interface Languages | <ul style="list-style-type: none"> <li>• Chinese (Simplified)</li> <li>• Chinese (Traditional)</li> <li>• English (US)</li> <li>• French</li> <li>• German</li> <li>• Italian</li> <li>• Japanese</li> <li>• Korean</li> <li>• Portuguese</li> <li>• Russian</li> <li>• Spanish (international)</li> </ul> |

1. Users watch recorded meetings through the Desktop web user interface.



## CHAPTER 28

# Configuring Cisco Unified Videoconferencing Desktop

---

- [Accessing the Administration Interface, page 28-1](#)
- [Viewing Server Status and Port Resource Usage, page 28-2](#)
- [How to Configure Cisco Unified Videoconferencing Desktop Server Settings, page 28-3](#)
- [Configuring Gatekeeper IP Address, page 28-4](#)
- [Configuring Client-Related Settings, page 28-5](#)
- [How to Configure Meeting Control Settings, page 28-6](#)
- [Defining Security Settings, page 28-8](#)
- [Configuring Meeting Features, page 28-9](#)
- [How to Configure Streaming Server Settings, page 28-10](#)
- [How to Configure Recording Server Settings, page 28-13](#)
- [How to Manage Recordings, page 28-19](#)
- [How to Restore Recordings, page 28-24](#)
- [How to Brand Desktop User Interface, page 28-25](#)
- [Viewing the Cisco Unified Videoconferencing Desktop Online Help, page 28-28](#)

## Accessing the Administration Interface

### Procedure

---

**Step 1** Open the Internet browser.

**Step 2** Enter the following URL:

[http://<host>\[:<port>\]/cuvm/admin](http://<host>[:<port>]/cuvm/admin)

where <host> is the location of your corporate Cisco Unified Videoconferencing Desktop Server.

**Step 3** On the Administration page, enter your user name and password.

**Step 4** Click **Sign In**.

The default user name and password are both “admin”.

---

## Viewing Server Status and Port Resource Usage

The Cisco Unified Videoconferencing Desktop Status tab displays status information about the Cisco Unified Videoconferencing Desktop Server and other servers with which it interacts:

- Gatekeeper—A Cisco IOS H.323 Gatekeeper.
- Streaming—The Cisco Unified Videoconferencing Streaming Server. This information appears only if the Desktop Server is configured to manage streaming.
- Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing Manager—An optional server used to moderate the Desktop meetings. If no server is configured to moderate Desktop meetings, no link appears on this tab.

**Note**

In the Desktop Server GUI, Cisco Unified Videoconferencing 3500 MCU is referred to as ‘CUV MCU’.

---

**Before You Begin**

- Navigate to the Desktop Server Administration web user interface.

**Procedure**

---

**Step 1** Click **Status** in the sidebar.

**Step 2** Click the **Cisco Unified Videoconferencing Desktop Server** tab.

**Step 3** Click the link showing the IP address of a server to display the settings for that server.

The indicator next to each link shows whether or not the connection to the target server or registration with the Gatekeeper is successful. When the indicator is red, a tooltip containing error details is available. Click the red indicator to view further error information.

---

**Related Topics**

- [How to Configure Streaming Server Settings, page 28-10](#)
- [How to Configure Meeting Control Settings, page 28-6](#)

# How to Configure Cisco Unified Videoconferencing Desktop Server Settings

- [Configuring Settings for Single/Multiple-NIC Deployments, page 28-3](#)
- [Configuring Desktop Server Network Interface, page 28-3](#)

## Configuring Settings for Single/Multiple-NIC Deployments

The Desktop Server can have multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you might want to control which NIC is used for various server communications.

For example, in secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with various servers, while using another NIC for Desktop Clients to connect to. In this case you must configure the Desktop network interface address to represent the NIC behind the firewall, and then in the Public Address field enter a DNS name which resolves to the NIC outside the firewall and is accessible both inside and outside the corporate network.

For single NIC deployments, the network interface address represents the Desktop Server IP address that clients use to connect to Cisco Unified Videoconferencing Desktop. In single NIC deployments with both internal and external clients, this value represents an external, statically-mapped Desktop Server IP address.

Desktop Clients can connect to the Desktop Server either by an IP or a DNS name. If a DNS name is not specified in the Public Address field, the Desktop network interface address is used. However, in many deployments the Desktop Server network interface address is not accessible to clients outside the intranet, due to NAT or firewall restrictions. Therefore, we recommend that you specify the Public Address, which must be a DNS name resolving to the correct Desktop Server IP address both inside and outside the corporate network.

## Configuring Desktop Server Network Interface

The Desktop Server communicates with the following types of servers in the deployment:

- Cisco Unified Videoconferencing 3500 MCU and Cisco IOS H.323 Gatekeeper—For media and call setup.
- Cisco Unified Videoconferencing Manager or Cisco Unified Videoconferencing 3500 MCU—For moderation and meeting control.
- Cisco Unified Videoconferencing Streaming Server—For media and control.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

- 
- Step 1** Click **Settings** in the sidebar.
- Step 2** Click the **Server** tab.

**Step 3** From the CUVC Desktop Network Interface list, choose the IP address that the Desktop Server must use to communicate with various servers.

The indicator next to the Address field shows whether connection to the Desktop Server is successful or not. When the indicator is red, a tooltip containing error details is displayed.

**Step 4** For secure multiple NIC deployments, enter a DNS name in the Public Address field.

**Step 5** Click the **Client** tab.

**Step 6** Click **OK** or **Apply**.

---

## Configuring Gatekeeper IP Address

Cisco Unified Videoconferencing Desktop is designed to work with either a single Cisco Unified Videoconferencing 3500 MCU, or with Cisco Unified Videoconferencing Manager which manages multiple MCUs. If Cisco Unified Videoconferencing Manager is configured to moderate Desktop meetings, use the IP address of a gatekeeper managed by Cisco Unified Videoconferencing Manager. If Cisco Unified Videoconferencing Manager manages more than one gatekeeper, use the IP address of a gatekeeper assigned to the same Cisco Unified Videoconferencing Manager zone as the Desktop Server.

If a single Cisco Unified Videoconferencing 3500 MCU is configured to moderate Desktop meetings, use the IP address of the same gatekeeper to which the MCU is registered. If no server is configured to moderate Desktop meetings, use the IP address of a gatekeeper configured for the Desktop deployment.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

**Step 1** Click **Settings** in the sidebar.

**Step 2** Click the **Server** tab.

**Step 3** Enter the required address in the Gatekeeper IP Address field.

The indicator next to the Address field shows whether registration to the Gatekeeper is successful. When the indicator is red, a tooltip containing error details is displayed.

**Step 4** Click **OK** or **Apply**.

---

# Configuring Client-Related Settings

During this procedure you choose the video quality:

- Standard Definition

This option limits Desktop Clients to a connection of standard definition at the maximum call rate you specify. If you define a service on the Cisco Unified Videoconferencing 3500 MCU that enables H.323 endpoints to use a higher bandwidth rate or high definition, Desktop calls using this service are transcoded down to the lower rate at standard definition (CIF resolution) for the Desktop Client. If you select a Cisco Unified Videoconferencing 3500 MCU service with a bandwidth rate lower than the value set in the Maximum Call Rate list, then the latter is used for the standard definition call to the Desktop Client.

- High Definition

This option allows Desktop Clients to connect to a conference in high definition mode. If you select this option, you must select a maximum call rate of at least 1 MB and a minimum video rate of 768 Kbps to enable the conference to continue in 720p high definition video resolution for all clients. The Desktop Client sends up to 512 Kbps of 480p video resolution and receives the maximum call rate or rate of the service selected (the lower value of the two) of 720p video resolution. If you select a lower maximum call rate you can force the high definition service to send 480p to all clients at the lower bandwidth. If you select a lower minimum video rate you can enable a 720p service to decrease to 480p if bandwidth limitations during the conference require it.

When in high definition mode and connected to a high definition service, Desktop limits fast update requests so that it does not request more than one keyframe within 30 seconds. This allows to avoid degradation of the video quality or frame rate to all the connected endpoints.

If a Desktop connects to a standard definition service, then the standard definition quality is used during a Desktop conference.

You can also configure the maximum transmission unit (MTU) size the Desktop Client uses for communicating with Desktop. The default value is 1360. This setting should match the setting on the Cisco Unified Videoconferencing 3545 MCU used and your network setting to avoid fragmentation.

## Before You Begin

- Navigate to the Desktop Server Administration web user interface.

## Procedure

---

**Step 1** Click **Settings** in the sidebar.

**Step 2** Click the **Client** tab.

**Step 3** To configure settings for standard definition:

- a. From the Maximum Video Quality list, choose **Standard Definition**.
- b. From the Maximum Call Rate list, choose a bandwidth rate.

The default call rate value defined for the Desktop service configured on the Cisco Unified Videoconferencing 3545 MCU is 384 Kbps.

**Step 4** To configure settings for high definition:

- a. From the Maximum Video Quality list, choose **High Definition**.

The Minimum Video Bandwidth list is automatically updated to display 512 Kbps as the lowest available value.

- b. From the Minimum Video Bandwidth list, choose a bandwidth rate.




---

**Note** Desktop does not flow control calls below the minimum video bandwidth rate. If this value is set to 512, Desktop negotiates a call down to 512 Kbps, which changes the video sent by Cisco Unified Videoconferencing 3545 MCU from 720 p to 480 p.

---

- c. From the Maximum Call Rate list, choose a bandwidth rate.

**Step 5** In the Maximum MTU Size field, enter a value.

**Step 6** Click **OK** or **Apply**.

---

## How to Configure Meeting Control Settings

- [Configuring Server Type, page 28-6](#)
- [Configuring Cisco Unified Videoconferencing 3500 MCU Server Settings, page 28-7](#)
- [Configuring Cisco Unified Videoconferencing Manager Server Settings, page 28-7](#)

## Configuring Server Type

Configure the type of server according to these recommendations:

- For a simple deployment including a single Cisco Unified Videoconferencing 3500 MCU, configure the MCU.
- For deployments containing Desktop with multiple Cisco Unified Videoconferencing 3500 MCUs but without Cisco Unified Videoconferencing Manager, you can connect to multiple MCUs but you do not have moderation control. Without Cisco Unified Videoconferencing Manager, the Cisco Unified Videoconferencing 3500 MCUs do not cascade MCUs into virtual meetings.
- For more complex deployments, select the Cisco Unified Videoconferencing Manager.




---

**Note** When you configure Desktop to work with Cisco Unified Videoconferencing Manager, participants can access their own virtual room settings via the Virtual Room button in the Preferences screen on the Desktop entry page.

---

### Related Topics

- [Configuring Settings for Single/Multiple-NIC Deployments, page 28-3](#)
- [Configuring Cisco Unified Videoconferencing 3500 MCU Server Settings, page 28-7](#)
- [Configuring Cisco Unified Videoconferencing Manager Server Settings, page 28-7](#)

## Configuring Cisco Unified Videoconferencing 3500 MCU Server Settings

This section describes how to configure a Cisco Unified Videoconferencing 3500 MCU to moderate your Cisco Unified Videoconferencing Desktop meetings.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Meeting Control** in the sidebar.
- Step 2** From the server type list, choose **CUV MCU**.
- Step 3** Enter the MCU IP address.
- The indicator next to the Address field shows whether or not the connection to the target server is successful.
- Step 4** Enter a user name and password for accessing the MCU Administration web user interface.
- Step 5** Re-enter the password in the Confirm field.
- The default user name is "admin". By default, there is no password.
- Step 6** From the CUVC Desktop Network Interface list, choose the IP address that the Desktop Server.
- The Desktop Server uses this IP address for MCU Server communications.
- Step 7** If necessary, click **Enable Raise Hand feature in Desktop meetings**.
- For deployments with multiple Desktop Servers, we recommend that you clear this check box. A moderator using one Desktop Server cannot see a request made by a participant using another Desktop Server.
- Step 8** Click **OK** or **Apply**.
- 

## Configuring Cisco Unified Videoconferencing Manager Server Settings

The source H.323 ID is used only for advanced routing with Cisco Unified Videoconferencing Manager. Cisco Unified Videoconferencing Manager contains a corresponding field and uses the source H.323 ID to identify clients from a particular Desktop Server, and then route clients to the appropriate Cisco Unified Videoconferencing 3500 MCU.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.
- To allow the Desktop clients to connect to the Desktop server via port 80, go to **Control Panel > Administrative Tools > Services** on the Cisco Unified Videoconferencing Manager server and disable the IIS Administration service, HTTP SSL service, and World Wide Web Publishing services. This can be done either before installing the CUV Desktop server software or when receiving the "ip address/ port is in use" error during the installation. After disabling these services, the installer will complete normally and the desktop clients will be able to connect to the desktop server using port 80.

**Procedure**

- 
- Step 1** Click **Meeting Control**.
- Step 2** From the server type list, choose Cisco Unified Videoconferencing Manager.
- Step 3** Enter the address of the Cisco Unified Videoconferencing Manager server.  
When using Single Sign-On (SSO) with the Cisco Unified Videoconferencing Manager, we recommend that you enter the local server name rather than the DNS name or IP address. For example, if the DNS name is <server1.company.com>, configure this setting to <server1>.
- Step 4** Enter the HTTP port of the Cisco Unified Videoconferencing Manager server.  
The default HTTP port is 8080.
- Step 5** Enter the source H.323 ID of the Desktop.
- Step 6** From the CUVC Desktop Network Interface list, choose the IP address. The Desktop Server uses this IP address for Cisco Unified Videoconferencing Manager Server communications.
- Step 7** If necessary, click **Enable Raise Hand feature in Desktop meetings**.  
For deployments with multiple Desktop Servers, we recommend that you clear this check box. A moderator using one Desktop Server cannot see a request made by a participant using another Cisco Unified Videoconferencing Desktop Server.
- Step 8** Click **OK** or **Apply**.  
The indicator next to the Address field shows whether or not the connection to the target server is successful.
- 

## Defining Security Settings

This section describes how to define access control to the Cisco Unified Videoconferencing Desktop Server Administration web user interface and to enable sRTP media encryption between Desktop Clients and the Desktop Server.

Encrypting media (audio, video, presentation) between Desktop Server and the Desktop Client might be used, for example, in a corporate deployment where the Desktop Server is used to bring in people from outside your network. Since this option only enables secure encryption of the media, you need also to secure the web portal. Choosing the **Allow Users to have CUVC Desktop call them back** option enables the video device callback option on the Desktop user entry page. When users select **Use my computer for presentation only** on connecting to a meeting, the **Callback my video device number** option becomes available. The **Callback my video device number** provides the option to call back the H.323 device when the users connect, so that users can connect in the “data only” mode to a meeting from their computers and automatically connect their H.323 devices at the same time.

**Note**

In the “data only” mode, users can see the participant list, moderate, chat, and show or view presentations. Users can view or send neither audio nor video.

---

The H.323 device can be disconnected automatically when users disconnect their computers from the call.

**Before You Begin**

- Navigate to the Desktop Server Administration web user interface.

**Procedure**

- 
- Step 1** Click **Settings** in the sidebar.
- Step 2** Click the **Security** tab.
- Step 3** Locate the Access Control area.
- Step 4** Enter the administrator login information in the relevant fields.
- Step 5** Locate the Security area.
- Step 6** If necessary, click **Encrypt Media (between Desktop and Server)**.
- Step 7** If necessary, click **Allow Users to have CUVC Desktop call them back**.  
This option is available only after you define a meeting control server for Cisco Unified Videoconferencing Desktop.
- Step 8** Click **OK** or **Apply**.
- 

**Related Topics**

- Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component

## Configuring Meeting Features

This section describes how to configure meeting features including the Desktop Sharing and Chat options and Push to Talk option as well as displaying an additional panel.

When the Desktop Sharing option is enabled, the Cisco Unified Videoconferencing Desktop participants can present applications and share their desktops with other participants. You can optionally allow only moderators to share their desktops. When desktop sharing is not enabled, the video display layout in the Desktop Client changes to display the local video in a small frame and the remote video in a large frame. The Present and PIP buttons are unavailable and participants cannot change this layout.

Configure the Push to Talk option to define how participants use the microphone button in the Desktop Live Meeting Console:

- Allow users to join a meeting with their microphone on—The microphone is on and the audio output is sent when participants enter a meeting. The participants must click the microphone button to mute themselves.
- Force users to join a meeting with their microphone off—The microphone is off and the audio output is not sent when participants enter a meeting. The participants must click the microphone button to unmute themselves.
- Force users to hold down their microphone button while speaking—Participants must click and hold down the microphone button to activate their microphones and to send their audio output.

You can enable the custom panel option to display an additional custom panel in the Desktop Live Meeting Console. The custom panel docking location is preconfigured and cannot be changed; meeting participants can move the panel after undocking it.

The URL parameters are passed to the custom URL as follows:

?meetingid=NNN&nickname=XXX, where NNN is the ID of the meeting that the user is connected to, and XXX is the nickname of the connected user.

You can also use the custom panel URL to specify additional URL parameters. You must use the URL-encoding for the additional URL parameters. For example, if the custom panel URL is "http://www.mycustompanel.com/myservlet?arg1" and the Desktop entry page or conference room is launched with the additional argument "?CUSTOM=arg2%26arg3%3D123", the custom panel opens to the URL "http://www.mycustompanel.com/myservlet?arg1&arg2&arg3=123".

#### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

#### Procedure

- 
- Step 1** Click **Settings** in the sidebar.
- Step 2** Click the **Meeting Features** tab.
- Step 3** Define the Enable Desktop Sharing and Enable Chat options as desired.
- For deployments with multiple Desktop Servers, we recommend that you do not enable the chat option. A participant using one Desktop Server cannot join the chat started by a participant using another Desktop Server.
- Step 4** Define the additional custom panel option as desired:
- Click the **Display an additional panel in the conference room** check box to enable the option.
  - Enter the URL in the field.
- Step 5** Define the Push to Talk option as desired.
- Step 6** Click **OK** or **Apply**.
- 

## How to Configure Streaming Server Settings

This section describes how to configure Cisco Unified Videoconferencing Desktop streaming settings of the Cisco Unified Videoconferencing Manager. Streaming can be managed either by a single Cisco Unified Videoconferencing Desktop Server or by multiple Desktop Servers. If a single Desktop Server is set to manage streaming, all other participants are directed to this server. If multiple Desktop Servers are configured to manage streaming, they manage streaming independently.

To designate a single Desktop Server to manage streaming, enable streaming on this Desktop Server. In this case you must disable streaming on other Desktop Servers in the same deployment. However, you can configure those server to allow watching of webcasts from the Cisco Unified Videoconferencing Desktop Server on which streaming is enabled.

To enable multiple Desktop Servers for managing streaming, enable streaming on each Desktop Server in this deployment.

**Note**

When multiple Desktop Servers manage streaming, streaming must be enabled or disabled on each individual Desktop Server. For example, if streaming is enabled for a meeting or virtual room, a moderator cannot disable it, because each Desktop Server manages streaming independently. If a moderator connected to one Desktop Server disables streaming, the other Desktop Server still continues to stream, unless it is disabled by its moderator as well.

Table 28-1 compares using a single Desktop Server to using multiple Cisco Unified Videoconferencing Desktop Servers for streaming.

**Table 28-1 Comparison of Deployment Characteristics**

| Characteristic            | Single Desktop Server enabled for streaming  | Multiple Desktop Servers enabled for streaming                            |
|---------------------------|--|---|
| HTTP performance          | Slower HTTP performance over the Internet between dispersed sites and the designated Desktop Server. | Faster HTTP performance within local sites.                               |
| Load on Streaming Server  | Many streaming clients at different sites sharing the resources of a single streaming server.        | Streaming clients at individual sites share a local streaming server.     |
| Desktop Server management | Single location for managing streaming.  | Streaming must be enabled or disabled on each individual Desktop Server.  |
| Participant count         | All participants connected to the central Desktop Server are shown in the meeting display.           | Only participants connected to a specific local Desktop Server are shown. |

- [Configuring This Desktop Server to Manage Streaming, page 28-11](#)
- [Configuring an Alternate Desktop Server for Watching Webcasts, page 28-12](#)

## Configuring This Desktop Server to Manage Streaming

This section describes how to enable this Desktop Server to manage streaming and to configure settings for this server.

The public address you define during this procedure performs a similar role to the public address defined for the Desktop Server. If the Streaming Server resides behind a NAT, the clients might not resolve the Streaming Server IP address. In this case the clients use the public address to connect to the Streaming Server.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

- 
- Step 1** Click **Streaming** in the sidebar.
- Step 2** Click the **Connection** tab.
- Step 3** Choose **Enable Streaming** from the list.

**Step 4** Enter the IP address of the Streaming Server.

**Step 5** From the CUVC Desktop Network Interface list, choose the IP address.

The Desktop Server uses this IP address for Cisco Unified Videoconferencing Streaming Server communications.

**Step 6** In the TCP Port field, enter a TCP streaming port.

The default port is 7070.



**Note** If you use a TCP port different from the default value of 7070, you must open this port on the firewall.  
For more information about configuring a UDP connection, refer to the “Configuring Streaming or Playback using the UDP connection” section of the Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component at [http://www.cisco.com/en/US/products/hw/video/ps1870/products\\_implementation\\_design\\_gui\\_des\\_list.html](http://www.cisco.com/en/US/products/hw/video/ps1870/products_implementation_design_gui_des_list.html).

**Step 7** In the Public Address field, enter a FQDN.

We recommend that you use a FQDN that clients can resolve.

**Step 8** Click **OK** or **Apply**.

**Step 9** Click the **Settings** tab.

**Step 10** Define the size of the video used for streaming by choosing one of the options: Small (QCIF) or Medium (CIF).

**Step 11** From the Rate list, choose a value to define the bit rate for the streaming feed between Cisco Unified Videoconferencing 3500 MCU and the Desktop Server.

**Step 12** Click **OK** or **Apply**.

The indicator next to the Address field shows whether not registration to the Cisco Unified Videoconferencing Streaming Server is successful. When the indicator is red, a tooltip containing error details is displayed.

#### Related Topics

- [Configuring Settings for Single/Multiple-NIC Deployments, page 28-3](#)
- [How to Configure Cisco Unified Videoconferencing Desktop Server Settings, page 28-3](#)

## Configuring an Alternate Desktop Server for Watching Webcasts

This section describes how to configure the Desktop Server to refer to an alternate Desktop Server which is used for streaming in order to watch webcasts.

#### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

- 
- Step 1** Click **Streaming** in the sidebar.
- Step 2** Click the **Connection** tab.
- Step 3** Choose **Disable Streaming** from the list.
- Step 4** Check the **Allow watching of webcasts from an alternate Desktop server** option.
- Step 5** In the Server URL field, enter the URL of the alternate Desktop Server.
- Step 6** Click **OK** or **Apply**.
- 

## How to Configure Recording Server Settings

Cisco Unified Videoconferencing Desktop allows users to record meetings and to view recorded meetings. A recording includes all media types: the audio, video and presentation. Servers used for recording meetings must have a recording license installed on them. Cisco Unified Videoconferencing Desktop supports up to 10 simultaneous recordings.

- [Viewing Recording Server Status, page 28-13](#)
- [About Configuring the Desktop Recording Server Connection, page 28-14](#)
- [Configuring Recording Parameters, page 28-16](#)
- [Modifying the Disk Space and Storage Location for Recordings, page 28-17](#)
- [Disabling Automatic Recording Feature, page 28-18](#)

## Viewing Recording Server Status

The Recording Status tab displays this information:

- **Recording Server**—Displays the address of the Desktop Recording Server.
- **Recorder**—Displays the connection status between the Desktop Recording Server and the Desktop Conference Server.
- **Gatekeeper**—Displays the address of the gatekeeper to which the Conference Server is registered. In the special case that the Desktop Recording Server is installed separately from the Cisco Unified Videoconferencing Desktop Server and has its own Conference Server, the Conference Server must be registered to the same gatekeeper as the Cisco Unified Videoconferencing Desktop Server.
- **NIC Address**—Displays the NIC address used by the Desktop Recording Server to communicate with the Cisco Unified Videoconferencing 3545 MCU.
- **Recordings Folder**—Displays the location of the folder on the Desktop Recording Server used for storing recordings.
- **Remaining Disk Space**—Shows how much space is remaining on the disk on which recordings are stored.

If the remaining disk space is less than the disk space allocated for recordings, a warning icon is displayed. Click the icon for details.

- **Disk Usage**—Shows the amount of disk space used by all recordings. The maximum value is configured during installation.

To change the maximum disk space, run the installer on the Desktop Recording Server in the modification mode.

- **Recordings in progress**—Shows the number of recordings being recorded at the present moment. The maximum value appears as specified in the recording license installed for this Desktop.
- **Completed recordings**—Shows the total number of completed recordings available for watching.
- **Reconstructed recordings**—Shows the number of reconstructed recordings.

Desktop saves actual recordings and recording attributes in different folders. If a user restores only a recording without restoring its attributes, the recording appears as reconstructed. In this case you need to manually define recording attributes, such as the name and the owner PIN, to finalize reconstruction of a recording. Only after the reconstruction is completed the recording appears on Watch Recording page of the Cisco Unified Videoconferencing Desktop portal. If recording attributes are not reconstructed, the yellow attention icon is displayed. Click the icon for more information.

- **Evaluation license**—Displays information about an evaluation license if it is used.

#### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

#### Procedure

- 
- Step 1** Click **Status** in the sidebar.
  - Step 2** Click the **Recording Status** tab.
  - Step 3** Click the link showing the IP address of the recording server to display the Recording Connection Settings page.

The indicator next to each link shows whether or not the connection to the target server or registration with the Gatekeeper is successful. When the indicator is red, a tooltip containing error details is available. Click the red indicator to view further error information.

---

## About Configuring the Desktop Recording Server Connection

This section describes how to configure Desktop Recording Server settings. Recording can be managed either by a single Cisco Unified Videoconferencing Desktop Server or by multiple Cisco Unified Videoconferencing Desktop Servers.

If a single Cisco Unified Videoconferencing Desktop Server is set to manage recording, only participants connected through that Cisco Unified Videoconferencing Desktop Server can start or stop recording. In this case, you can configure other Cisco Unified Videoconferencing Desktop Servers in the deployment to display the list of recordings from the Cisco Unified Videoconferencing Desktop Server configured to manage recording.

If you configure multiple Cisco Unified Videoconferencing Desktop Servers to manage recording, the servers manage recording independently causing each Desktop portal to display its own list of recordings.

To designate a single Cisco Unified Videoconferencing Desktop Server to manage recording, enable recording on this Cisco Unified Videoconferencing Desktop Server. In this case you must disable recording on other Cisco Unified Videoconferencing Desktop Server in the same deployment, and enable them to allow playback of recordings from an alternate Cisco Unified Videoconferencing Desktop Server in order to display a list of recordings in the portal.

To enable multiple Cisco Unified Videoconferencing Desktop Server for managing recording, enable recording on each Cisco Unified Videoconferencing Desktop Server in this deployment.

## Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording

The public address you define during this procedure performs a similar role to the public address defined for the Desktop Server. If the Desktop Recording Server resides behind a NAT, the clients might not resolve the Desktop Recording Server IP address. In this case the clients use the public address to connect to the Desktop Recording Server.

You can configure recording settings as well as manage recordings if you select this server to manage recording.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

**Step 1** Click **Recordings** in the sidebar.

**Step 2** Click the **Connection** tab.

**Step 3** From the list, choose **Enable recording**.

**Step 4** Enter the IP address of the Recording Server.

**Step 5** In the Public Address field, enter a FQDN.

We recommend that you use a FQDN that clients can resolve.

**Step 6** Enter the TCP port.

This port is used by clients to access the recording in case a UDP connection fails.

You must configure the TCP port on the Cisco Unified Videoconferencing Streaming Server and open this port on the firewall.

For more information about configuring a UDP connection, refer to the “Configuring Streaming or Playback using the UDP connection” section of the Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component.

**Step 7** From the CUVC Desktop Network Interface list, choose the IP address.

The Desktop Server uses this IP address for communications with Cisco Unified Videoconferencing Streaming Server and TCP Proxy.

**Step 8** Click **OK** or **Apply**.

The indicator next to the Address field shows whether not registration to the Cisco Unified Videoconferencing Streaming Server is successful. When the indicator is red, a tooltip containing error details is displayed.

---

**Related Topics**

- Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component at [http://www.cisco.com/en/US/products/hw/video/ps1870/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/video/ps1870/products_implementation_design_guides_list.html)

**Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording**

If you select an alternate server to manage recording, you can configure neither recording settings nor manage recordings.

**Before You Begin**

- Navigate to the Desktop Server Administration web user interface.

**Procedure**

- 
- Step 1** Click **Recordings** in the sidebar.
- Step 2** Click the **Connection** tab.
- Step 3** From the list, choose **Enable recording**.
- Step 4** In the Server URL field, enter the URL of the alternate Desktop Server.
- Step 5** Click **OK** or **Apply**.
- 

**Configuring Recording Parameters**

During the configuration described in this section you define the recording policy by enabling the recording option for Desktop users and by specifying the type of meetings the users can record.

If you disable recording for users, you do not need to choose a meeting type.

If Cisco Unified Videoconferencing Manager is configured to moderate Desktop Server meetings, both Cisco Unified Videoconferencing Manager and Cisco Unified Videoconferencing Desktop control recording. If the recording policy is differently configured on Cisco Unified Videoconferencing Manager and Cisco Unified Videoconferencing Desktop, the more restrictive settings overrule the less restrictive settings, creating a unified recording policy. For example, if the recording policy of Cisco Unified Videoconferencing Desktop is configured to allow recording of any meeting, while the policy of Cisco Unified Videoconferencing Manager is set to enable recording only for certain virtual rooms, recording of meetings in the specified virtual rooms will be allowed.

You also define the following parameters during this configuration:

- Video size and Recording bit rate—These parameters are used to control the quality of recordings. Setting the recording bit rate to a value lower than 256 Kbps can affect the quality and framerate of the H.239 Data in the live connection and streaming modes. We recommend that you set the recording bit rate to 384 Kbps.
- Maximum Recording Duration—The value set for this parameter controls maximum allowed duration for any recording.
- Send tone periodically during recording—This parameter defines the frequency of the tone played during a recording which serves to remind users that their meeting is being recorded.

**Before You Begin**

- Navigate to the Desktop Server Administration web user interface.

**Procedure**

- 
- Step 1** Click **Recordings** in the sidebar.
- Step 2** Click the **Settings** tab.
- Step 3** From the Video Size list, choose an option.
- Step 4** From the Recording bit rate list, choose a value.
- Step 5** Select the check box to enable recording for Desktop users.
- Step 6** If you enabled recording for users, choose a meeting type:
- Any meeting
  - Only moderated meetings—Users are allowed to record only meetings for which a moderator PIN is configured.
- Step 7** In the Maximum Storage Capacity field, enter a value.
- Step 8** In the Maximum Recording Duration field, enter a value.
- Step 9** From the Send tone periodically during recording list, choose an option.
- Step 10** Click **OK**.
- 

**Related Topics**

- [Modifying the Disk Space and Storage Location for Recordings, page 28-17](#)

## Modifying the Disk Space and Storage Location for Recordings

By default Cisco Unified Videoconferencing Desktop stores recordings at a location defined during Cisco Unified Videoconferencing Desktop Server installation, however, you can modify this location if required.

During this procedure all recording services are stopped. After the new location is defined, all new recordings are stored at it. You must manually transfer the existing recordings into the new location. The recordings that are left in the previous location do not appear on the Watch Recording page of the Cisco Unified Videoconferencing Desktop portal.

**Procedure**

- 
- Step 1** Insert the Cisco Unified Videoconferencing Desktop Server product CD-ROM and click the **Modify Cisco Unified Videoconferencing Desktop Server** button in the autorun application to access the Cisco Unified Videoconferencing Desktop Server installer.
- Step 2** In the Choose Setup Language screen, choose the installation language from the list, and click **Next**.
- Step 3** In the Welcome screen click **Next**.
- Step 4** In the License Agreement screen, choose I accept the terms in the license agreement, and click **Next**.
- Step 5** In the Desktop Serial Key screen, enter your Cisco Unified Videoconferencing Desktop Server serial key acquired from Cisco support, and then click **Next**.

- Step 6** In the Desktop Network Configuration screen, click **Next**.
- Step 7** In the Desktop Hostname Configuration screen, click **Next**.  
In the Desktop Recording Configuration screen is displayed.
- Step 8** To modify the storage location, perform the following:
- Click **Change**.
  - Navigate to a new location.
  - Click **OK**.
- Step 9** To modify the maximum amount of disk space, enter new value in the field.
- Step 10** Click **Next**.
- Step 11** Click **Install**.
- 

## Disabling Automatic Recording Feature

You can use the Cisco Unified Videoconferencing Manager to automatically record either a virtual room or a scheduled meeting when the meeting begins. In this case Desktop records the meeting unless one of the following problems interferes with recording:

- There are not enough available recording ports on the Desktop at the time when the meeting is scheduled
- There is not enough disk space the disk on which recordings are stored
- The maximum number of simultaneous recordings is reached

If the deployment in use comprises multiple Cisco Unified Videoconferencing Desktop Servers, automatic recording is performed on all Cisco Unified Videoconferencing Desktop Servers and several identical recordings are created. In this case we recommend that you allow one of the Cisco Unified Videoconferencing Desktop Servers to perform automatic recording, while disabling the automatic recording feature on the rest of the Cisco Unified Videoconferencing Desktop Servers in the deployment. The procedure in this section describes how to disable the automatic recording feature on a Cisco Unified Videoconferencing Desktop Server.

### Procedure

---

- Step 1** Stop the service "Desktop - Apache Tomcat".
- Step 2** Modify the ctmx.ini file:
- Using either the Microsoft Notepad or the Microsoft Wordpad application, open the following file:  
<installDir>\tomcat\webapps\WEB-INF\data\ctmx.ini  
where <installDir> represents the actual installation directory.
  - Locate the section [meetingmgr].
  - Find the entry for autorecord and set the value to "false".

- d. Save the file.
- e. Close the application you used for editing the file.

**Step 3** Start the service "Desktop - Apache Tomcat".

---

## How to Manage Recordings

- [Viewing Recording List, page 28-19](#)
- [Editing Recording Attributes, page 28-20](#)
- [Setting Categories for Multiple Recordings, page 28-21](#)
- [Deleting Recordings, page 28-21](#)
- [Stopping Recordings in Progress, page 28-22](#)
- [Recording Meetings, page 28-22](#)

## Viewing Recording List

You can review the list of recordings made on this Cisco Unified Videoconferencing Desktop using the Recordings tab. The following information is displayed:

- Meeting ID
- Name
- Start Time
- Duration

For meetings that are currently being recorded, the “In progress” indication is displayed.

- PIN-protected indicator

You can also access for the following additional information for a specific recording:

- Description
- Categories—Keywords associated with recordings.
- Recording URL

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

**Step 1** Click **Recordings** in the sidebar.

**Step 2** Click the **Recordings** tab.

The Recordings tab is displayed showing a list of recordings. By default all recordings are displayed.

**Step 3** To filter recordings, select a category from the Show list.

- Step 4** To sort recordings, click one of the columns:
- Meeting ID
  - Name
  - Start Time
  - Duration
- Step 5** To search for a specific recording by an attribute:
- Meeting ID—Click the **Meeting ID** column, enter the meeting ID in the Search field, and then click the **Search** button.
  - Meeting Name—Click any column except the Meeting ID column, enter the meeting name in the Search field, and then click the **Search** button.
- Step 6** To display additional information for a specific recording, click the **Information** icon. The Meeting Information window opens.
- 

## Editing Recording Attributes

You can assign an owner and an access PIN for recording protection. The access PIN is optional and is used for watching a recording. In the list of recorded meetings protected by an access PIN are marked by a key icon. The owner PIN is used only for editing a recording.

You can define what part of a recorded meeting is played by setting offsets. In this case while the playback of a recording changes, the duration of the recording itself is not shortened. For example, to omit the first five minutes of a recording, set the Start offset to 5 minutes.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recording** in the sidebar.
- Step 2** Click the **Recordings** tab.
- Step 3** Locate the required recording in the list.
- Step 4** Click the **Edit** icon.
- The Edit Recording window is displayed.
- Step 5** To modify the recording name and description, enter new text in relevant fields.
- Step 6** To set offsets:
- Pull sliders
- Or
- Edit values in the fields.
- Step 7** To modify categories for the recording, select a category in the relevant pane and click the **Transfer** button.
- Step 8** To set the owner PIN for the recording, enter the owner PIN.

- Step 9** To set the access PIN, enter the access PIN.
- Step 10** Click **OK**.
- 

## Setting Categories for Multiple Recordings

You can set categories for multiple recordings at one time.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recording** in the sidebar.
- Step 2** Click the **Recordings** tab.
- Step 3** In the recording list, click check boxes to select recordings.
- Step 4** Click **Categorize**.
- The Categorize Recordings window opens.
- Step 5** To assign a category, which is not currently assigned to selected recordings:
- a. In the left pane, click the check box for this category.
  - b. Click **Assign**.
- Step 6** To remove a category, which is currently assigned to selected recordings:
- a. In the right pane, click the check box for this category.
  - b. Click **Remove**.
- 

## Deleting Recordings

You can permanently remove a recording from Cisco Unified Videoconferencing Desktop by deleting it from the recording list.

When you delete a recording which is in progress, the meeting participants are notified that the recording is stopped. The meeting moderator receives a notification that the recording is deleted by the administrator.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recordings** in the sidebar.
- Step 2** Click the **Recordings** tab.
- Step 3** In the recording list, click the check box for recordings you wish to delete.

- Step 4** Click **Delete**.
- Step 5** Click **Yes** in the confirmation message.
- 

## Stopping Recordings in Progress

You can stop any recording that is in progress. When you stop a recording in progress, meeting participants are notified that the recording is stopped. The meeting moderator receives a notification that the recording is stopped by the administrator.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recording** in the sidebar.
- Step 2** Click the **Recordings** tab.
- Step 3** In the recording list, click the check box for recordings you want to stop.
- Step 4** Click **Stop**.
- Step 5** Click **Yes** in the confirmation message.
- 

## Recording Meetings

You can record meetings using the Desktop Server Administration web user interface.

### Before You Begin

- Verify that you have the ID of a meeting you want to record.
- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recording** in the sidebar.
- Step 2** Click the **Recordings** tab.
- Step 3** In the Start recording meeting ID field, enter ID.
- Step 4** Click **Record**.
- The Start Recording window is displayed.
- Step 5** Enter recording name and description.
- Step 6** Assign categories as necessary.
- Step 7** To set the owner PIN for the recording:
- a. Choose either the **Use the moderator PIN as the Owner PIN** or **Specify an Owner PIN** option.

- b. Enter the owner PIN.
  - c. Enter the owner PIN in the Confirm field.
- Step 8** To set the meeting PIN:
- a. Choose the **Use the meeting PIN as the Access PIN** or **Specify an Owner PIN** option.
  - b. Enter the access PIN.
  - c. Enter the access PIN in the Confirm field.
- Step 9** Click **Start Recording**.
- The meeting appears in the list, and its duration is indicated as “In Progress”.
- 

## Managing Categories

Apart from standard attributes like an ID, name, and duration, Cisco Unified Videoconferencing Desktop provides a category—a special attribute that can help organizing and searching recordings. Both users and administrators can assign categories to recordings. Administrators manage categories by modifying a list of existing categories, while users can only select categories from this list to associated them with recordings.

If you rename an existing category, Cisco Unified Videoconferencing Desktop automatically updates attributes for all recordings belonging to the modified category. Deleting a category does not cause Cisco Unified Videoconferencing Desktop to delete recordings belonging to the deleted category.

### Before You Begin

- Navigate to the Desktop Server Administration web user interface.

### Procedure

---

- Step 1** Click **Recording** in the sidebar.
- Step 2** Click the **Categories** tab.
- Step 3** To create a new category:
- a. In the Create a new category field, enter the name.
  - b. Click **Create**.
- The new category appears in the list.
- Step 4** To edit an existing category:
- a. Click the **Edit** icon.
  - b. Enter the new name for the category.
  - c. Click **OK**.
- Step 5** To delete an existing category:
- a. Click the **Delete** icon.
  - b. Click **Yes**.
-

# How to Restore Recordings

Desktop saves actual recordings and recording attributes in different folders. In order to restore a recording you need to restore both folders.

- [Backing up Recordings, page 28-24](#)
- [Restoring Recordings, page 28-24](#)

## Backing up Recordings

Perform the backup procedure described in this section on the Desktop Recording Server. During the backup procedure, you copy the xml file that contains the database of categories configured, the recordings folder containing recording attributes, and the folder containing actual recordings to a location outside the installation directory.

### Procedure

---

- Step 1** Navigate to the following directory: <installdir>\CSAgent\data.
- Step 2** Copy recorder\_categories.xml file into a location outside the installation directory.
- Step 3** Copy the recordings folder into a location outside the installation directory.
- Step 4** Navigate to the folder where recordings are stored.
- By default, the recordings are stored in the <installdir>\recordings, if not configured otherwise.
- Step 5** To check the location where recordings are stored:
- a. Access the Cisco Unified Videoconferencing Desktop Server Administration web interface.
  - b. Click **Status** in the sidebar.
  - c. Click the **Recording Status** tab.
- The Recordings Folder information is displayed on the tab.
- Step 6** Copy that folder into a location outside the installation directory.
- 

## Restoring Recordings

### Procedure

---

- Step 1** Stop the service "Desktop - Apache Tomcat".
- Step 2** Stop the service "Desktop- TCP Proxy".
- Step 3** Navigate to the following directory: <installdir>\csagent\data.
- Step 4** Replace recorder\_categories.xml file with the backup file.
- Step 5** Replace the recordings folder with the backup folder.
- Replacing the recordings folder with the backup folder erases any categories that are currently defined in Desktop.

- Step 6** Navigate to the folder in which recordings are stored.
- Step 7** By default, this will be <installdir>\recordings, but this can be changed.  
By default, the recordings are stored in the <installdir>\recordings, if not configured otherwise.
- Step 8** To check the location where recordings are stored:
- Access the Cisco Unified Videoconferencing Desktop Server Administration web interface.
  - Click **Status** in the sidebar.
  - Click the **Recording Status** tab.
- The Recordings Folder information is displayed on the tab.
- Step 9** Replace that folder with the backup folder.
- Step 10** Start the service "Desktop - Apache Tomcat".
- Step 11** Start the service "Desktop - TCP Proxy".
- 

## How to Brand Desktop User Interface

Cisco Unified Videoconferencing Desktop Server is released with a set of default images appearing in the Desktop user interface. However, you can change images and strings displaying irrelevant branding information using the Desktop Branding application.

- [Replacing Images, page 28-25](#)
- [Modifying Strings, page 28-26](#)
- [Saving or Restoring Branding-related Changes, page 28-27](#)
- [Restoring Default Images and Strings, page 28-28](#)

### Replacing Images

You can replace images appearing in the Desktop user interface by using the Branding application on Cisco Unified Videoconferencing Desktop Server. Replacement takes affect immediately, therefore we recommend that you should not replace images on a server that is currently in service. Replacement does not affect the proper function of the Desktop user interface.

Most web browsers store local copies of images to accelerate future views of the same image. This practice is called caching. Any browser that has previously loaded an image that you replace might display its local copy of the old image rather than your replacement image. If an image in the Desktop user interface does not appear to be the same as the one displayed as the currently installed image, then you must clear your browser's cache.

Cisco Unified Videoconferencing Desktop Server is released with a set of default images that you can restore at any time.

### Procedure

---

- Step 1** Click **Start**.
- Step 2** Choose **Programs > Desktop > Branding Application**.  
The branding application starts.
- Step 3** Click the **Images** tab.  
The images that can be replaced are displayed together with the recommended size and a brief description of each image.  
If an image has a transparent background, it appears with a gray and white “checkerboard” background in the preview fields.
- Step 4** From the list, choose the image you want to replace.  
A brief description of the image is displayed along with the recommended image size. The Default image area shows the image that was originally distributed with the product. The Currently installed image shows the image that appears in the user interface.
- Step 5** Click **Select File**, and then choose the replacement image.  
A preview of the image is displayed.  
If you use an image that the application indicates as not properly sized, a warning appears below the image description. Using an image that does not match the original image size might result in incorrect image display.
- Step 6** If you use an image that is not properly sized, verify that the image is displayed correctly:
- a. Verify that the Cisco Unified Videoconferencing Desktop Server is running.
  - b. Review the Desktop user interface after replacement to verify that the image appears correctly.
- Step 7** Click **Install Image** to use the replacement image.  
This image is replaced.  
If an old image still appears, see your browser's documentation for information about removing temporary internet files.
- Step 8** To restore a default image, click **Restore Original Image**.
- Step 9** Repeat [Step 4](#) through [Step 7](#) for other images.
- 

## Modifying Strings

You can modify some strings appearing in the Desktop user interface. New string values you set using the Branding application appear in the user interface only after Cisco Unified Videoconferencing Desktop Server starts and reads these values. Therefore, you can see modified strings only after the changes are applied and after the server is restarted if it was running when you made the changes.

### Procedure

---

- Step 1** Click **Start**.
- Step 2** Choose **Programs > Desktop > Branding Application**.
- Step 3** Click the **Strings** tab.

The strings that can be replaced are displayed along with their values:

- The Rebranded Value column displays values that are currently saved. When the Cisco Unified Videoconferencing Desktop Server is restarted, these are the values that appear in the user interface.
- The Default Value column displays values that are the original strings that were distributed with Desktop.

**Step 4** Click the relevant cell in the New Value column and type in the new string you want to use.

Or

Double-click a value in the Rebranded Value column or the Default column to copy it into the New Value column.

**Step 5** Repeat [Step 4](#) for other strings if necessary.

**Step 6** Click **Apply**.

The new values are saved. The modified values appear in the Rebranded Value column.

**Step 7** Restart the “Desktop - Apache Tomcat” service for the changes to take effect.

**Step 8** To restore default strings:

- a. Click **Restore All Default Strings**.
  - b. Click **Apply**.
  - c. Restart the “Desktop - Apache Tomcat” service for the changes to take effect.
- 

## Saving or Restoring Branding-related Changes

You can save modified images and strings by exporting them to a file. You can later use this file to import values from it, thus restoring them.

### Procedure

---

**Step 1** Click **Start**.

**Step 2** Choose **Programs > Desktop > Branding Application**.

**Step 3** To save modified images and strings:

- a. From the File menu, choose **Export**.
- b. Specify the location in which you want to save the file.
- c. Click **Save**.

**Step 4** To restore the modified images and strings from the file:

- a. From the File menu, choose **Import**.
- b. Navigate to the export file.
- c. Click **Import**.

**Step 5** Restart the “Desktop - Apache Tomcat” service for the changes to take effect.

---

## Restoring Default Images and Strings

Cisco Unified Videoconferencing Desktop Server is released with a set of default images and string values. You can restore both default images and default string values in one go. Restoring default images and strings overwrites currently used images and string values with default ones.

### Procedure

---

- Step 1** Click **Start**.
  - Step 2** Choose **Programs > Desktop > Branding Application**.
  - Step 3** From the File menu, choose **Restore all**.
  - Step 4** Restart the “Desktop - Apache Tomcat” service for the changes to take affect.
- 

## Viewing the Cisco Unified Videoconferencing Desktop Online Help

### Procedure

---

- Step 1** Access the Desktop Server Administration web interface.
  - Step 2** Click the **Help** icon in the top right corner of the Administration web user interface.
- 

### Related Topics

- [Accessing the Administration Interface, page 28-1](#)



## INDEX

---

### A

- Adding Multipoint Processors [21-2](#)
- Adding Services [22-1](#)

---

### B

- bandwidth [13-4](#)
- Bandwidth Rules [20-13](#)
- billing [13-6](#)

---

### C

- CDR
  - file naming [14-17](#)
- Children [20-7](#)
- columns
  - sorting [13-2](#)
- Conferences and Calls view
  - Calls tab [25-1](#)
  - Conferences tab [25-3](#)
- Configuration Tool
  - CDR [14-17](#)
  - e-mail server settings [14-4](#)
  - endpoint
    - unresponsive to connection request [14-4](#)
  - MCU command delay [14-5](#)
  - meeting settings [14-7](#)
  - passwords [14-5](#)
  - security settings [14-14](#)
- Configuring
  - Gateway [22-2](#)
- Configuring Protocols [21-1](#)

---

### D

- Default Dialing Mode [13-5](#)
- delay [13-4](#)

---

### G

- Gatekeeper
  - local zones [20-11](#)
  - Prefixes [20-13](#)
- Gatekeeper hierarchy
  - children [20-7](#)
  - neighbors [20-10](#)
  - parent [20-5](#)

---

### H

- host [13-6](#)

---

### I

- IP Topology tab [1-2](#)
  - Bandwidth [1-2](#)
  - Distance [1-2](#)
- ISDN
  - cost of call [1-2](#)

---

### L

- Logs
  - Gateway [26-1](#)
  - MCU [26-1](#)

---

## M

### MCU

- command delay [14-5](#)
- local [13-4](#)

### MCU access [25-4](#)

### Meeting Scheduling

- One Button [13-7](#)
- Recurrence [13-7](#)

### Meeting Scheduling button [13-7](#)

### My Meetings

- Status indicators [12-2](#)

---

## N

### Name Display Format [13-2](#)

### Neighbors [20-10](#)

### Network Tree view [17-1](#)

- Elements tab [18-3](#)

---

## P

### Parent [20-5](#)

---

## R

### recording meetings [6-2](#)

### Registering MPs [21-1](#)

### report

- information categories [12-4](#)

### reports

- generating [12-4](#)

---

## S

### Services

- MCU [21-3](#)

### Settings view

### Element Logs tab [26-2](#)

---

## V

### Views

- Network Tree [17-1](#)

### virtual room [10-2](#)

---

## X

### XML

- CDR file naming [14-17](#)