Configuration Guide for Cisco Unified Videoconferencing Manager Release 7.1

February 2010

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: 0L-21622-01

Configuration Guide for Cisco Unified Videoconferencing Manager Release 7.1

CONTENTS

CHAPTER 1 **Introducing Cisco Unified Videoconferencing Manager** 1-1

Overview 1-1

Accessing the Resource Manager User Interface 1-2

Accessing the Network Manager User Interface 1-2

Resource Manager User Types 1-2

Administrative Permissions 1-3

PART 1 **Resource Manager**

CHAPTER 2 **Managing Network Topologies in Resource Manager** 2-1

How to Enable the Network Management Tab 2-1

Launching the Cisco Unified Videoconferencing Manager Configuration Tool 2-1

Viewing IP and ISDN Network Topologies 2-2

How to Create a Network Topology with Device Islands 2-2

Adding a Device Island 2-3

Modifying Device Island Settings 2-4

Removing Connectivity Between Device Islands 2-4

Removing a Device Island 2-4

Modifying Your Network Topology View 2-5

CHAPTER 3 **Configuring a Gatekeeper Profile in Resource Manager** 3-1

About Gatekeeper Types 3-1

Cisco IOS H.323 Gatekeepers 3-1

External Gatekeepers 3-1

How to Create or Modify a Gatekeeper Profile 3-2

Defining Gatekeeper Address Details 3-2

Defining Dialing Plan Settings 3-3

Defining Resource Manager as the Gatekeeper Authorization Server 3-3

Removing a Gatekeeper Profile 3-4

Searching for a Gatekeeper Profile 3-4

Accessing Meetings from an External Gatekeeper 3-5

CHAPTER 4 **Configuring a SIP Server Profile in Resource Manager** 4-1

Creating or Modifying a SIP Server Profile 4-1

Setting the DTMF Signaling Method 4-2
Removing a SIP Server Profile 4-2
Searching for a SIP Server Profile 4-3
Configuring the MCU to Work in SIP Mode 4-3
Disabling the SIP Back-to-Back User Agent 4-4

CHAPTER 5 **Managing an MCU Profile in Resource Manager** 5-1
Configuring Cascading 5-1
Creating or Modifying an MCU Profile 5-2
Taking an MCU Offline 5-3
Removing an MCU Profile 5-4
Searching for an MCU Profile 5-4
Synchronizing MCU Information with Cisco Unified Videoconferencing Manager 5-5
How to Manage Meeting Types 5-5
Viewing Available Meeting Types on Network MCUs 5-6
Viewing Built-in Meeting Types 5-7
Removing a Meeting Type 5-7
Searching for a Meeting Type 5-8
Downloading a Meeting Type to Resource Manager 5-8
Resolving Meeting Type Conflicts Between MCUs 5-8
Resolving Meeting Type Conflicts Between Resource Manager and an MCU 5-9
Uploading a Meeting Type to Network MCUs 5-9
Viewing Meeting Type Details 5-10
Modifying Meeting Type Details 5-10
Accessing an MCU from the Meeting Type Details Screen 5-10
Viewing a List of MCUs Containing a Specified Meeting Type 5-11
Customizing MCU Delimiters 5-11
Designating a Service for Cisco TelePresence Use 5-11
Designating a Service for IVR Use 5-12

CHAPTER 6 **Configuring a Gateway Profile in Resource Manager** 6-1
Creating or Modifying a Gateway Profile 6-1
Taking a Gateway Offline 6-3
Removing a Gateway Profile 6-4
Searching for a Gateway Profile 6-4

CHAPTER 7 **Configuring a Cisco Unified Videoconferencing Desktop Profile in Resource Manager** 7-1
Creating or Modifying a Desktop Profile 7-1

Removing a Desktop Profile 7-2
Searching for a Desktop Profile 7-2
How to Stream Meetings Using Cisco Unified Videoconferencing Desktop 7-3
Enabling Streaming on Desktop 7-3
Enabling Streaming for a Virtual Room 7-3
Allowing Recording by Specified Roles 7-3
Allowing Recording by Specified Users 7-4
Enabling Recording for Specified Virtual Rooms 7-4

CHAPTER 8 **Configuring a Meeting Room Profile in Resource Manager** 8-1
Enabling Meeting Room Support 8-1
Creating or Modifying a Meeting Room Profile 8-2
Sending Meeting Details by Email 8-2
Removing a Meeting Room Profile 8-3
Searching for a Meeting Room Profile 8-3

CHAPTER 9 **Configuring a Terminal Profile in Resource Manager** 9-1
How to Create or Modify a Terminal Profile 9-1
Defining H.323 IP Terminal Details 9-1
Defining SIP IP Terminal Details 9-2
Defining ISDN/PSTN H.320 Terminal Details 9-3
Defining Mobile Terminal Details 9-4
Defining Dual H.320 and H.323 Terminal Details 9-4
Removing a Terminal Profile 9-5
Searching for a Terminal Profile 9-5

CHAPTER 10 **Defining Resource Manager Call Routing Modes** 10-1
Call Routing in H.323 Deployments 10-1
Call Routing in SIP Deployments 10-2
Masking Conference Topology with the Virtual MCU Feature 10-2
Creating a Centralized Conference 10-2
Creating a Distributed Conference 10-3

CHAPTER 11 **Viewing Network Device Performance and Availability** 11-1
Viewing Device Usage and Failure by Time Interval 11-1
Viewing Device Usage and Failure by Time Interval and Period 11-2
Viewing MCU Port Availability 11-3
Generating a Report 11-4

CHAPTER 12 **Viewing Real-time Meeting Statistics in Resource Manager** 12-1

Viewing the Number of Ongoing Meetings and Calls 12-1
Viewing Port Utilization Information 12-2
Viewing Organization Meetings and Calls 12-2
Viewing the Creation Status of Meetings 12-2
Searching for a Meeting 12-3
Monitoring a Meeting or Call 12-4
Generating Reports 12-4
Modifying Upcoming Meetings 12-6
Viewing Host MCUs 12-6
Terminating Meetings 12-6

CHAPTER 13 **Creating Statistical Reports of Meetings and Calls in Resource Manager** 13-1

Creating a Call Information Report 13-1
Creating a Port Usage Report 13-2
Creating a Resource Usage Report 13-3
Viewing the Use of Ad Hoc and Scheduled Meetings 13-3
Viewing Average Meeting Size 13-4
Viewing Average Meeting Duration 13-4
Generating Reports for Finished Meetings 13-5
Viewing Finished Meetings 13-6
Viewing the Termination Status of Meetings 13-6
Searching for a Finished Meeting 13-7
Viewing Host MCUs 13-8
Removing Meetings from the History Tab 13-8

CHAPTER 14 **Managing Resource Manager Users and User Groups without an External Directory** 14-1

Creating or Modifying a User Profile 14-1
Removing a User Profile 14-2
Searching for a User Profile 14-3
Updating User Profiles 14-3
Creating a User Group 14-4
Modifying a User Group 14-4
Removing a User Group 14-4
Limiting Individual User Access to Meeting Types 14-5
Limiting Group Access to Meeting Types 14-5

Configuring Multiple Settings for User Groups 14-5

CHAPTER 15 **Provisioning Resource Manager Users Using a Directory Server 15-1**

Synchronization of User Information 15-1
Accessing User Information in Active Directory Server 15-2
Synchronizing Resource Manager with Active Directory Server 15-2
Configuring a Connection to an LDAP Server 15-3
Mapping Resource Manager User Roles to ADS Users 15-4
Defining Virtual Rooms for All LDAP Users 15-5
Forcing Resource Manager to Use a Virtual Room 15-6
Resource Manager LDAP Information Attributes 15-6

CHAPTER 16 **Modifying Default Organization Settings for Resource Manager Users and Meetings 16-1**

Settings Priorities 16-1
How to Define Default Settings for Organization Users 16-1
Defining Which Meeting Types are Available to New Users 16-2
Defining a Default Time Zone for a User 16-2
Defining Display Formats 16-2
Defining Date Display Formats 16-3
Defining Your Meeting Display Preferences 16-3
Defining Default Recording Permissions 16-3
How to Define Default Settings for Meetings 16-4
Defining a Default Meeting Type 16-4
Defining the Default Cascading Mode 16-5
Defining the Maximum Number of Ports for an Ad Hoc Meeting 16-5
Defining How to End a Meeting 16-5
Defining the Meeting Default Length 16-6
Defining the Default Dialing Mode 16-6
Defining a Billing Destination 16-7
Defining Required Default Resources 16-7
Defining the Auto Attendant Dial-in Number 16-7
Enabling Automatic Routing 16-8
Customizing Invitation Email 16-8
Modifying the Look and Feel of the Resource Manager Web User Interface 16-9

CHAPTER 17 **Using the Cisco Unified Videoconferencing Manager Configuration Tool 17-1**

Setting Up the Java Runtime Environment 17-2
Launching the Cisco Unified Videoconferencing Manager Configuration Tool 17-2

Retrieving an Administrator Password 17-3
Uninstalling the Cisco Unified Videoconferencing Manager Configuration Tool 17-3
How to Modify General Settings 17-3
Defining Email Server Settings 17-4
Defining the Unconnected Endpoint Time Period 17-4
Defining User Provisioning Options 17-5
Defining Table Row Display 17-5
Defining the Command Delay 17-6
Defining the Parent Zone Authorization Filter 17-6
Defining the Log Level 17-7
Defining the Resource Manager Server Name and Web Port 17-7
How to Modify Scheduling Settings 17-7
Changing Call Authorization Settings 17-8
Dynamically Cascading Multiple EMPs for a Single Conference 17-9
Modifying Resource Manager Default Meeting Settings 17-9
Modifying Default Recurring Meeting Settings 17-10
Hiding Resource Manager User Interface Screens 17-11
How to Manage Custom Time Zones 17-11
Selecting a Time Zone Profile 17-12
Viewing a Time Zone Profile 17-12
Adding Daylight Saving to a Time Zone Profile 17-12
Creating a Customized Time Zone Profile 17-13
Removing a Customized Time Zone Profile 17-13
Reverting to Default Time Zone Settings 17-14
Customizing Product and Vendor Logos 17-14
Creating a Customized Billing Field 17-14
Defining Database Server Settings 17-15
How to Define Security Settings 17-15
Defining Password Settings 17-16
Defining a Login Message 17-16
Unlocking a User Account 17-16
How to Configure SNMP Trap Server Profiles 17-17
Adding an SNMP Trap Server Profile 17-17
Modifying an SNMP Trap Server Profile 17-17
Removing an SNMP Trap Server Profile 17-18
Defining Utilization Thresholds 17-18
How to Define Call Data Record (CDR) Settings 17-19
Creating CDR Information in XML Format 17-19

Defining Required Terminal Connection Duration 17-19
Defining a CDR File Prefix 17-20
Defining How Often CDRs Are Produced 17-20
Enabling Streaming to a RADIUS Server 17-21

CHAPTER 18 **Configuring Cisco Unified Videoconferencing Manager Redundancy** 18-1
About Redundant Mode 18-1
Configuring the Redundant Mode 18-1
Viewing Redundancy Status 18-2
Disabling the Redundant Mode 18-3

CHAPTER 19 **Resource Manager CDR XML Tags and Attributes** 19-1
Accessing the CDR XML Files 19-1
Index of CDR XML Tags 19-2
Understanding the CDR XML Tags 19-9

CHAPTER 20 **Enabling Resource Manager to Use Secure Sockets Layer Connections on a JBoss Application Server** 20-1
Component Identity via SSL 20-1
How to Generate Certificates 20-1
Methods for Creating a New Certificate 20-1
Prerequisites 20-2
Using Keytool to Generate a Certificate 20-2
Configuring JBoss to use SSL 20-4
Accessing Resource Manager Using HTTPS 20-5

PART 2 **Network Manager**

CHAPTER 21 **Network Manager Overview** 21-1
About the Network Manager 21-1
System Requirements 21-1
What the Network Manager Provides 21-1
Viewing Network Status 21-2
Viewing Calls and Conferences 21-2
Using Auto-Detect 21-3
Configuring Basic Elements 21-3
Viewing Alarms and Events 21-4
Connecting to Element Managers 21-4
Connecting to Terminal Managers 21-4

Managing a Centralized Log 21-4
Viewing Multiple Networks 21-5
Configuring Offline Elements 21-5
Defining Network Subsets 21-5
Supporting Cisco IOS H.323 Gatekeeper 21-5
Dragging and Dropping 21-5
Monitoring Calls 21-5

CHAPTER 22 **Viewing Your Network in Network Manager** 22-1
How to View the Network as a Tree 22-1
Configuring Network Hierarchy 22-1
Creating a Custom Network Tree View 22-2
Viewing the Network as a Table 22-2
Viewing the Network as a Map 22-3

CHAPTER 23 **Managing Elements in Network Manager** 23-1
Displaying General Element Information 23-1
Management Status of Elements 23-2
Viewing all Network Elements 23-2
Creating or Modifying an Element Profile 23-3
Removing an Element Profile 23-4
Searching for an Element Profile 23-4
Defining Default Element Access Settings 23-5
Overriding Default Element Access Settings 23-5
How to Upgrade Element Software 23-6
Adding a Software Upgrade File 23-6
Modifying a Software Upgrade File 23-7
Removing a Software Upgrade File 23-7
Cancelling Pending Offline Configuration Settings 23-8
How to Manage the Element Software Upgrade Upload Log 23-8
Viewing Your Software Upgrade Upload History 23-8
Uploading a File After a Failed Attempt 23-8
Removing Entries from the Upload Log 23-9
How to Automatically Detect New Elements on the Network 23-9
Running the Auto-detect Mechanism Manually 23-10
Running the Auto-detect Mechanism Automatically 23-10
Adding or Modifying Auto-detect Element Access Information 23-11
Removing an Element Type from the Auto-detect Mechanism 23-11

Accessing an Element Web User Interface 23-12
Accessing the Monitor Tab for a Specified Element 23-12

CHAPTER 24 **Managing Endpoints in Network Manager** 24-1
Defining Default Endpoint Access Settings 24-1
How to Override Default Endpoint Settings 24-2
Overriding Default Endpoint Addressing 24-2
Overriding Default Access Settings for a Selected Endpoint 24-2
Configuring Endpoint Dialing 24-3
Retrieving Configuration Parameters 24-3
How to Manage Endpoint Software Upgrade Files 24-4
Adding a Software Upgrade File 24-4
Modifying a Software Upgrade File 24-5
Removing a Software Upgrade File 24-5
How to Manage Endpoint Configuration Files 24-6
Viewing Saved Endpoint Configuration Files 24-6
Modifying an Endpoint Configuration File 24-6
Removing an Endpoint Configuration File 24-7
How to Upgrade Software for Selected Endpoints 24-7
Upgrading Software for Sony Endpoints 24-7
Upgrading Software for TANDBERG and Polycom Endpoints 24-8
How to Update Configuration for Selected Endpoints 24-8
Updating Configuration for Sony Endpoints 24-8
Updating Configuration for TANDBERG and Polycom Endpoints 24-9
Setting the Managed Status of TANDBERG and Polycom Endpoints 24-9
Manually Adding a New Managed Endpoint 24-10
How to Manage the Endpoint Upload Log 24-10
Viewing Your Endpoint Configuration Upload History 24-11
Uploading a File After a Failed Attempt 24-11
Removing Entries from the Upload Log 24-11

CHAPTER 25 **Managing an MCU in Network Manager** 25-1
Setting Call Routing Devices 25-1
Viewing Registered Multipoint Processors 25-1
Viewing MCU Supported Services 25-2
How to Back Up and Restore MCU Configuration Settings 25-2
Backing Up MCU Configuration Settings 25-3
Restoring MCU Configuration Settings 25-3

Modifying MCU Configuration File Information 25-3
Deleting a Configuration File 25-4
Configuring MCU Location 25-4

CHAPTER 26 **Managing the Internal Gatekeeper in Network Manager** 26-1
How to Manage Services 26-1
Viewing Internal Gatekeeper Supported Services 26-2
Creating or Modifying a Service 26-2
Viewing Global Services 26-3
Creating or Modifying a Global Service 26-3
Removing a Service 26-4
How to Manage Prefixes 26-4
Creating or Modifying a Prefix 26-4
Removing a Prefix 26-5
How to Configure a Parent Gatekeeper 26-5
Enabling the Parent Tab 26-5
Adding a Parent Manually 26-6
Adding a Parent Automatically 26-6
How to Manage Parent Filters 26-6
Creating or Modifying a Parent Filter 26-7
Removing a Parent Filter 26-7
How to Configure a Child Gatekeeper 26-7
Enabling the Children Tab 26-8
Viewing Child Gatekeepers 26-8
Adding a Child Manually 26-9
Adding a Child Automatically 26-9
How to Manage Child Prefixes 26-9
Creating or Modifying a Child Prefix 26-10
Removing a Child Prefix 26-10
How to Configure a Neighbor Gatekeeper 26-10
Viewing Neighbor Gatekeepers 26-10
Adding or Modifying a Neighbor Gatekeeper 26-11
How to Manage Zones 26-12
Creating or Modifying a Local Zone 26-12
Creating or Modifying a Remote Zone 26-12
Removing a Zone 26-13
How to Manage Bandwidth Rules 26-13
Viewing Bandwidth Rules 26-13
Creating or Modifying a Bandwidth Rule 26-14

Removing a Bandwidth Rule 26-14
How to Manage Debug Flags 26-14
Creating or Modifying a Debug Flag 26-15
Removing a Debug Flag 26-15

CHAPTER 27 **Managing a Gateway in Network Manager** 27-1
How to Manage Services 27-1
Viewing Gateway Supported Services 27-1
Creating or Modifying a Service 27-1
Removing a Service 27-2
Configuring Gateway Addressing 27-2

CHAPTER 28 **Configuring a User Profile in Network Manager** 28-1
Creating or Modifying a User Profile 28-1
Removing a User Profile 28-2
How to Define Network Subsets 28-2
Creating or Modifying a Network Subset 28-2
Removing a Network Subset 28-3
Removing an Include or Exclude Criterion 28-3

CHAPTER 29 **Managing Traps and Alarms in Network Manager** 29-1
Sending Traps to Network Manager 29-1
Creating or Modifying a Trap Forwarding Rule 29-2
Disabling a Trap Forwarding Rule 29-3
Removing a Trap Forwarding Rule 29-3
Creating or Modifying an Alert Recipient Profile 29-3
Removing an Alert Recipient Profile 29-4
Viewing Generated Events 29-5
Filtering Generated Events 29-5
Viewing Events per Network Item 29-6
Viewing and Sorting Supported Alarms 29-6
Modifying Alarms 29-6
Viewing and Sorting Generated Alarms 29-7
Viewing Generated Alarms per Network Item 29-7

CHAPTER 30 **Managing Calls and Conferences in Network Manager** 30-1
Viewing Current Call Details 30-1
Viewing Current Call Details per Network Item 30-2

Disconnecting Calls 30-2
Searching for a Call 30-2
Viewing Current Conferences 30-3
Viewing Current Conferences per Network Item 30-4
Searching for a Conference 30-4
Accessing the Conference MCU 30-5

CHAPTER 31 **Configuring Logging for Network Manager** 31-1
Viewing Logs for a Selected Element 31-1
Defining Network Manager Logging Activity 31-1
Saving Element Logs 31-2
Collecting Logs from a Cisco IOS H.323 Gatekeeper Element 31-2

PART 3 **Desktop**

CHAPTER 32 **How to Configure Cisco Unified Videoconferencing Desktop Server** 32-1
Accessing the Administration Interface 32-1
How to View Status of Servers and Directory 32-2
Viewing Server Status and Port Resource Usage 32-2
Viewing Directory Status 32-3
Viewing Recording Server Status 32-4
How to Configure Deployments 32-5
Deployment Types 32-5
Configuring Settings for Single/Multiple-NIC Deployments 32-5
Configuring Basic Deployment 32-6
Configuring Advanced Deployment 32-7
How to Configure Client-Related Settings 32-8
Configuring Client Connection and Video Quality 32-8
Configuring Meeting Features 32-10
How to Configure Recording Server 32-11
About Configuring the Desktop Recording Server Connection 32-12
Adding Recording Server to Deployment 32-12
Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording 32-13
Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording 32-15
Modifying the Disk Space and Storage Location for Recordings 32-15
How to Manage Recordings 32-16
Viewing Recording Information 32-16

Editing Recording Attributes 32-17
Managing Categories 32-18
Setting Categories for Multiple Recordings 32-19
Recording Meetings 32-20
Stopping Recordings in Progress 32-20
Deleting Recordings 32-21
How to Configure Streaming Server Settings 32-21
Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Streaming 32-22
Configuring an Alternate Desktop Server for Watching Webcasts 32-24
How to Configure Messages and Invitations 32-24
Configuring Meeting Access Messages 32-24
Configuring Meeting Access Instructions 32-26
How to Configure Dial String Rules 32-26
Configuring Sametime Settings 32-33
Configuring a Local Administrator Account 32-33
Configuring Local Directory of Terminals 32-34
Increasing Cisco Unified Videoconferencing Desktop Server Memory 32-34
Generating a PKCS12 Certificate Using Microsoft Certificate Service 32-35
Verifying That the Certificate Installed 32-36
Exporting the Certificate 32-36
Adding the Certificate to Cisco Unified Videoconferencing Desktop Configuration Tool and Enabling HTPPS 32-37

CHAPTER 33 **How to Customize The User Interface** 33-1
Replacing Images 33-1
Modifying Strings 33-2
Saving or Restoring Branding- Related Changes 33-3
Restoring Default Images and Strings 33-4

CHAPTER 34 **How to Backup and Restore Recordings and Settings** 34-1
Backing up Recordings 34-1
Backing up Settings 34-2
Restoring Recordings 34-3
Restoring Settings 34-3

INDEX

CHAPTER 1

Introducing Cisco Unified Videoconferencing Manager

Revised: January 27, 2010/OL-21622-01

- Overview, page 1-1
- Accessing the Resource Manager User Interface, page 1-2
- Accessing the Network Manager User Interface, page 1-2
- Resource Manager User Types, page 1-2

Overview

Cisco Unified Videoconferencing Manager is a single-installation product that contains the following components:

- Resource Manager is a simple-to-use, web-based application for managing visual communications in multi-site organization deployments. It provides resource management of network devices for video and audio meetings as well as scheduling, call-routing, and conference control functionalities.

  Resource Manager optionally includes an internal ITU-T H.323 version 4-compliant gatekeeper to provide call control for IP telephony and multimedia communication networks.

  Resource Manager also contains an internal SIP Back-to-Back User Agent to provide call control for IP telephony and multimedia communication on the SIP network.
- Network Manager provides a central management interface, enabling network administrators to easily and intuitively control, configure, and maintain collaborative Cisco-based communication networks and equipment.

Accessing the Resource Manager User Interface

Procedure

Step 1 Open your Web browser

Step 2 Enter the following URL:

http://<host ip/name>:8080/cuvcmrm

or

Step 3 Select **Start > Programs > Cisco Unified Videoconferencing Manager > Login to Resource Manager component of CUVC-M**.

Accessing the Network Manager User Interface

Procedure

Step 1 Open your Web browser

Step 2 Enter the following URL:

http://<host ip/name>:8080/cuvcmnm

or

Step 3 Select **Start > Programs > Cisco Unified Videoconferencing Manager > Login to Network Manager component of CUVC-M**.

Resource Manager User Types

The following user types are used by the system. Each user type has its own set of permissions.

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

Administrative Permissions

Each user type has a default set of permissions and a default view of the user interface. Table 1-1 outlines the different permissions for the user types.

Table 1-1 Resource Manager User Types and Default Permissions

	Organization Administrator	Meeting Operator	Meeting Organizer	Regular User
View and manage multiple organizations				
View and manage all network devices across multiple organizations				
View and manage all network devices, room terminals, and users and their virtual rooms within the organization	Allowed			
View and manage all meetings across multiple organizations				
View and manage all meetings within the organization	Allowed	Allowed		
Create and manage meetings for others	Allowed	Allowed	Allowed	
Manage personal address book	Allowed	Allowed	Allowed	
Manage own virtual room	Allowed	Allowed	Allowed	
Create and manage own meetings	Allowed	Allowed	Allowed	Allowed
View scheduled meetings	Allowed	Allowed	Allowed	Allowed
Receive and respond to meeting notices	Allowed	Allowed	Allowed	Allowed
Attend meetings	Allowed	Allowed	Allowed	Allowed
Moderate meetings	Allowed	Allowed	Allowed	Allowed
Modify own profile	Allowed	Allowed	Allowed	Allowed

PART 1

Resource Manager

CHAPTER 2

Managing Network Topologies in Resource Manager

Revised: February 7, 2010/OL-21622-01

This section is for Organization Administrators.

- How to Enable the Network Management Tab, page 2-1
- How to Create a Network Topology with Device Islands, page 2-2
- Modifying Your Network Topology View, page 2-5

How to Enable the Network Management Tab

The Network Management tab is hidden by default. Display the Network Management tab as described here.

- Launching the Cisco Unified Videoconferencing Manager Configuration Tool, page 2-1
- Viewing IP and ISDN Network Topologies, page 2-2

Launching the Cisco Unified Videoconferencing Manager Configuration Tool

The Cisco Unified Videoconferencing Manager Configuration Tool is accessible from any client computer 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 Select **Launch CUVCM RM Configuration Tool**.

The Cisco Unified Videoconferencing Manager Configuration Tool checks for the latest version of the Java Web Start application on the client computer, and then starts the Cisco Unified Videoconferencing 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, select **Run**.

To avoid the appearance of this message upon launch of the Cisco Unified Videoconferencing Manager Configuration Tool from the same site address, in the message window, select **Always trust content from this publisher**, and then select **Run**.

Step 4 Select **Launch CUVCM RM Configuration Tool** on the Resource Manager launch page.

Step 5 Enter the login and password of the Service Provider Administrator or an Organization Administrator.

Step 6 Select **Login**.

The Cisco Unified Videoconferencing Manager Configuration Tool window opens.

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 Select **Network Management** in the sidebar menu of the Resource Manager web user interface.

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 2-3
- Modifying Device Island Settings, page 2-4

- Removing Connectivity Between Device Islands, page 2-4
- Removing a Device Island, page 2-4

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.

Note Make sure that the bandwidth of the device island is set to an equal of, or greater value than, the default service prefix under meeting types. A lower value can prevent desktop clients from creating a meeting.

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 Select **Network Management** in the sidebar menu.

Step 2 Select **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 Select **OK** to save your changes.

Modifying Device Island Settings

Procedure

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

Step 2 Modify the distance and bandwidth in the appropriate cell.

Step 3 Select **OK** to save your changes.

Removing Connectivity Between Device Islands

Procedure

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

Step 2 Delete the distance and bandwidth values for the required device island pair.

Step 3 Select **OK** to save your changes.

Removing a Device Island

Procedure

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

Step 2 Select 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 select **OK**.

Step 4 Select **OK** in the Network Management screen to save your changes.

Modifying Your Network Topology View

Procedure

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

Step 2 Select **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 Select **Search**.

Step 5 The selected device islands appear in the grid display.

CHAPTER 3

Configuring a Gatekeeper Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- About Gatekeeper Types, page 3-1
- How to Create or Modify a Gatekeeper Profile, page 3-2
- Removing a Gatekeeper Profile, page 3-4
- Searching for a Gatekeeper Profile, page 3-4
- Accessing Meetings from an External Gatekeeper, page 3-5

About Gatekeeper Types

Cisco Unified Videoconferencing Manager supports the following types of gatekeeper:

- Cisco IOS H.323 Gatekeepers, page 3-1
- External Gatekeepers, page 3-1

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, Cisco Unified Videoconferencing 5000 Series MCUs and Cisco Unified Videoconferencing 3500 Series 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 3-2
- Defining Dialing Plan Settings, page 3-3
- Defining Resource Manager as the Gatekeeper Authorization Server, page 3-3

Defining Gatekeeper Address Details

During this procedure you define the management IP address of the gatekeeper. The real-time IP address is extracted automatically using either the device SNMP interface or the XML interface. The real-time IP address is used for zone matching. Each time a new element is added to the network Network Manager uses the real-time IP address to check whether the new element is registered to this gatekeeper or not.

If the added element management IP does not match the real-time IP address of the gatekeeper, you need to add a new zone on the gatekeeper, creating an inferred gatekeeper. Once a user tries to connect to this new element Network Manager tries to use the management IP address for connection and if it does not exist it tries to connect using a signaling IP address.

For a redundant gatekeeper use the same settings as for the main one.

Procedure

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

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the link in the Name column for the gatekeeper you require, or select **Add** to create a new gatekeeper profile.

Step 4 Locate the General section.

Step 5 Enter the name and the management 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 Select **OK** to save your changes.

Defining Dialing Plan Settings

Procedure

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

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the link in the Name column for the gatekeeper you require, or select **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 select Hierarchical, the Parent Gatekeeper list becomes active. Select a parent zone for the gatekeeper from the list. **None** is automatically selected in the list if the gatekeeper is a parent at the top of the hierarchy.

Do not select 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 Select **Add Zone Prefix** to add a zone prefix that matches the configuration of the gatekeeper.

Step 8 Select **OK** to save your changes.

Defining Resource Manager as the Gatekeeper Authorization Server

Procedure

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

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the link in the Name column for the gatekeeper you require.

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.

This option is checked by default if you are using 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 Select **OK** to save your changes.

Removing a Gatekeeper Profile

Procedure

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

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the gatekeeper entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **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 Select **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 select **Search**.

Accessing Meetings from an External Gatekeeper

If Resource Manager 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 Add the Resource Manager internal gatekeeper as a neighbor to this external gatekeeper in the external gatekeeper interface, and define the zone prefix for the internal gatekeeper according to the dial plan.

Step 2 Define the following forwarding rules in the external gatekeeper interface:

- 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 4

Configuring a SIP Server Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Creating or Modifying a SIP Server Profile, page 4-1
- Removing a SIP Server Profile, page 4-2
- Searching for a SIP Server Profile, page 4-3
- Configuring the MCU to Work in SIP Mode, page 4-3
- Disabling the SIP Back-to-Back User Agent, page 4-4

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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the link in the Name column for the SIP server you require, or select **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 2005/OCS 2007 or other third-party SIP servers. Resource Manager is interoperable with the following external SIP servers:

- Cisco Unified Communications Manager Release 5.0 or later
- Microsoft Live Communications Server 2005 with Service Pack 1
- Microsoft Office Communications Server 2007

- Microsoft Office Communications Server 2007 R2
- 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. Make sure that in the Cisco Unified Videoconferencing Manager, the DTMF Signaling Method is set to **No Preference** for the SIP trunk used in this deployment. For more information see "Setting the DTMF Signaling Method".

Step 9 (Optional) Enter the name of a preferred and an alternative DNS server in the relevant fields.

Step 10 Select **OK** to save your changes.

Setting the DTMF Signaling Method

Procedure

Step 1 Sign in to the Cisco Unified Videoconferencing Manager Administration web user interface.

Step 2 Select **Device > Trunk**.

Step 3 Select the SIP trunk added for this deployment.

Step 4 Under SIP Information, set the DTMF Signaling Method to **No Preference**.

Step 5 Save and apply the new configuration to the SIP trunk.

Removing a SIP Server Profile

Procedure

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

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the SIP server entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **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 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of SIP servers, clear the Name field, and then select **Search**.

Configuring the MCU to Work in SIP Mode

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

Procedure

Step 1 Select **Configuration**.

Step 2 Select **Protocols**.

Step 3 Locate the SIP section.

Step 4 Select **SIP** to enable MCU communication with the SIP proxy.

Step 5 Enter the SIP domain of the MCU in the **Default SIP domain** field as defined in the SIP server.

An example of a SIP domain is company.com.

Step 6 Select **Locate automatically** to instruct the MCU to automatically locate one of the SIP proxy servers that are present in the domain,

or

Select **Specify** and enter the following:

- An IP address or host name of the SIP proxy, for example proxy.company.com.
- The communication port number of the SIP proxy address. The default port is 5060.
- The transport connection type for sending messages to the SIP proxy according to the type supported by the SIP proxy—UDP or TCP.

  This field is mandatory. The default is UDP.

Note The Locate automatically option works only if you have configured a valid IP address at Configuration > Setup > Network > DNS server1 or DNS server2.

Step 7 Select **Use registrar** to instruct the MCU to register with a SIP registrar and to send service information to the registrar.

Step 8 Enter the following information:

- The IP address or the host name of the SIP registrar in the **IP address** field.

  This field is mandatory.

- The communication port number of the SIP registrar address.
- The transport connection type for sending registration requests to the registrar according to the type supported by the SIP registrar—UDP or TCP.

  This field is mandatory. The default is UDP.

Step 9 Select **More**.

Step 10 Enter the number of the signaling port on which the MCU communicates with the SIP proxy.

The default is 5060.

Step 11 Select **Use proxy digest authentication** to enable MCU authentication with a SIP proxy server using user name and password.

Authentication is performed as defined in RFC 2617. This field is disabled by default.

Step 12 Enter the Cisco Unified Videoconferencing 3515 MCU user name and password.

The user name and password must match the name and password defined on the SIP proxy server.

Step 13 Select **Use registrar digest authentication** to enable MCU authentication with a SIP registrar using user name and password.

Authentication is performed as defined in RFC 2617. This field is disabled by default.

Step 14 Select **Use 'Empty Invite' when sending Invite messages to endpoints** to enable the remote endpoint to indicate preferred audio and video channels.

Step 15 Select **Using Microsoft OCS** to enable the MCU to work with Microsoft Office Communications Server (OCS).

Step 16 Select **Apply**.

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\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 5

Managing an MCU Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Configuring Cascading, page 5-1
- Creating or Modifying an MCU Profile, page 5-2
- Taking an MCU Offline, page 5-3
- Removing an MCU Profile, page 5-4
- Searching for an MCU Profile, page 5-4
- Synchronizing MCU Information with Cisco Unified Videoconferencing Manager, page 5-5
- How to Manage Meeting Types, page 5-5
- Customizing MCU Delimiters, page 5-11
- Designating a Service for Cisco TelePresence Use, page 5-11
- Designating a Service for IVR Use, page 5-12

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 Go to **Admin > Advanced Settings** from the sidebar menu.

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, select 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 Select **OK** to save the preferred behavior as the default.

Creating or Modifying an MCU Profile

The MCU is where a multipoint video conference 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 using the profiles defined under Admin > Resource Management.

During this procedure you specify the management IP of the gateway. The real-time IP is extracted automatically using either the device SNMP interface or its XML interface.

Procedure

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

Step 2 Select **MCU**.

Step 3 Select the link in the Name column for the MCU you require, or select **Add** to create a new MCU profile.

Step 4 Enter the name and the management IP address of the MCU in the relevant fields.

Step 5 Select the MCU model.

Step 6 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 7 Select the device island from the **Location** list 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 sign in name and password of the MCU in the relevant fields.

These must match the MCU web interface sign in name and password.

Step 9 Define SNMP communities, user name and password, communication port and signaling port (MCU version 4.x only) 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 10 Select **OK** to save your changes.

Step 11 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 select **OK**.

Taking an MCU Offline

Procedure

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

Step 2 Select **MCU**.

Step 3 Select 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 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **MCU**.

Step 3 Select the MCU entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **MCU**.

Step 3 Enter the partial or complete name of the MCU in the **Name** field.

Step 4 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of MCUs, clear the Name field, and then select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **MCU**.

Step 3 Select the MCU entry you want to update in the Name column.

Step 4 Select **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 5-6
- Viewing Built-in Meeting Types, page 5-7
- Removing a Meeting Type, page 5-7
- Searching for a Meeting Type, page 5-8
- Downloading a Meeting Type to Resource Manager, page 5-8
- Resolving Meeting Type Conflicts Between MCUs, page 5-8
- Resolving Meeting Type Conflicts Between Resource Manager and an MCU, page 5-9
- Uploading a Meeting Type to Network MCUs, page 5-9
- Viewing Meeting Type Details, page 5-10
- Modifying Meeting Type Details, page 5-10
- Accessing an MCU from the Meeting Type Details Screen, page 5-10
- Viewing a List of MCUs Containing a Specified Meeting Type, page 5-11

Viewing Available Meeting Types on Network MCUs

Procedure

Step 1 Select **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 .

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 5-1 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	Select **Details** to display a list of all MCUs defined in Cisco Unified Videoconferencing Manager containing the specified meeting type.
Maximum Available Ports	Displays the maximum number of allowed ports for the specified meeting type.

Viewing Built-in Meeting Types

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

Procedure

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

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

The built-in meeting types listed in are available.

Table 5-2 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

You must deactivate an active meeting type before you can permanently remove it from the system. Once a meeting type is inactive, you can no longer used it to schedule a meeting; however, you must wait until all current or future meetings that use this meeting type are finished, or you must cancel them. When there are no longer any scheduled meetings that require this meeting type, the meeting type is marked not in use and you can remove it.

This process is irreversible. You can never reactivate a meeting type that you have deactivated. When you clear a deactivated meeting type from the Resource Manager, the meeting type is also removed from all MCUs in the system which have a service with the same prefix as the deactivated meeting type.

Procedure

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

Step 2 Select the meeting type you want to delete.

Step 3 Select **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 Select **Meeting Types** in the sidebar menu.

Step 2 Enter the partial or complete name of the meeting type in the Name field.

Step 3 Select **Search**.

Search results are listed.

Step 4 To return to the complete list of meeting types, clear the Name field, and then select **Search**.

Downloading a Meeting Type to Resource Manager

Procedure

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

Step 2 Select **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 3 Enter a unique name for each meeting type.

Step 4 Select **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 may have prefix 80, which is the default prefix for an audio service.

Procedure

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

Step 2 Select **Download**.

MCU services are downloaded from all network MCUs.

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

Step 3 Scroll down to the Meeting Type (Service) Conflicts section on the Download Meeting Types (Services) screen.

Step 4 Select the entry that you want to keep in the **Use Meeting Type 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 5 Enter a unique name for each meeting type.

Step 6 Select **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 meeting types are displayed in the Missing Meeting Types table. When a user selects a service that already exists in Resource Manager from the User Meeting Type Definition From list, this meeting type is uploaded to the MCU that formerly used this server.

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 does not support mixed deployments of MCUs version 7 and other version MCUs.

If you have defined MCU services to support High Definition Continuous Presence (HP CP) conferences, then you cannot synchronize to an MCU that is not enabled for HD CP. If you try to perform such an operation, you receive a warning message.

Procedure

Step 1 Select **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 Select **Upload**.

Step 4 Use the arrows to select the target MCUs.

Only MCUs that support this type of service are available.

Step 5 Select **OK**.

Since MCU services are uploaded using SNMP, the process may take some time if there are many MCUs to connect to.

Viewing Meeting Type Details

Procedure

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

Step 2 Select 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 Select **Meeting Types** in the sidebar menu.

Step 2 Select the link in the Name column for the meeting type you require on the Active Meeting Types.

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.

Use the default connection rate 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, select **Lecture Mode Support** to enable this support.

Step 6 (Optional) Select **Auto Attendant Support** to specify this meeting type as the Auto Attendant meeting type.

Step 7 (Optional) Select Telepresence Support.

Step 8 Select **OK** to save your changes.

Accessing an MCU from the Meeting Type Details Screen

Procedure

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

Step 2 Select 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 Select **Meeting Types** in the sidebar menu.

Step 2 Select **Detail** in the MCU column to see a list of MCUs containing the specified meeting type.

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 using the MCU web user interface configuration, you need to configure MCU delimiters accordingly in Resource Manager.

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\Cisco Unified Videoconferencing Manager\CUVCMRM\jboss.

Designating a Service for Cisco TelePresence Use

Procedure

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

Step 2 Select **Active Meeting Types**.

Step 3 Select the name of the service you want to use for Cisco TelePresence meetings.

Step 4 Select **TelePresence Support** to enable this meeting type for Cisco TelePresence interoperability.

Step 5 Enter the number of ports you want to reserve for traditional room systems once the meeting begins in the **Reserved ports for traditional endpoints** field.

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

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

Designating a Service for IVR Use

You can define the MCU service for entry into the IVR audio and video message utility. When users dial the auto attendant session number they receive video with a list of all active conferences on all MCU in the farm. Resource Manager then routes calls based on input from users to an existing conference, or users can create a new conference.

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.

When you use Resource Manager with several MCUs (collectively known as a "farm"), you must define which MCU is the host for the video IVR.

Procedure

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

Step 2 Select **Active Meeting Types**.

Step 3 Select the name of the service you want to use for entry to the IVR.

Step 4 Select **Auto Attendant Support** to specify this meeting type as the Auto Attendant meeting type.

Step 5 When using Cisco IOS H.323 Gatekeeper, create a remote zone prefix with the auto attendant session number that points to the Resource Manager zone.

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

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

CHAPTER 6

Configuring a Gateway Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Creating or Modifying a Gateway Profile, page 6-1
- Taking a Gateway Offline, page 6-3
- Removing a Gateway Profile, page 6-4
- Searching for a Gateway Profile, page 6-4

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.

During this procedure you specify the management IP of the gateway. The real-time IP is extracted automatically using either the device SNMP interface or its XML interface.

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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gateway**.

Step 3 Select the link in the Name column for the gateway you require, or select **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 the management 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 Select the gatekeeper from the Registered To list to which the gateway is registered.

Step 7 Select the device island from the Location list to which the gateway 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 Select **Add Service** and select 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 Enter a gateway phone number.

a. Enter a description of the phone number for the gateway in the Description field.

b. Enter the numeric prefix required to make an international long distance call in the International Access Code field.

c. Enter the numeric prefix required to make a long distance call within the same country in the Domestic Long Distance Prefix field.

d. Enter the country code for the gateway phone number in the Country Code field. 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.

e. If Allow Out of Area Calls is not selected, only endpoints with the same area code as the gateway are allowed to reach Resource Manager using the gateway.

f. If you select 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.

g. Enter the domestic area code of the gateway number in the Area Code field.

h. Specify a local telephone number in the Telephone Number field that you want to assign to the specific port.

i. 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.

j. 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.

k. 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 10 Select **Add Service** to add or modify the gateway service.

Note If you select Restricted Mode in the Bandwidth section, 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 11 Set the Advanced Settings.

- Set the gateway port used for signaling in the Signaling Port field. By default, it is left blank and signaling port will be negotiated dynamically on the fly.
- Set the SNMP community name required by Resource Manager to communicate with the gateway in the SNMP Get/Set Community fields.
- Select **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 12 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gateway**.

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

Step 4 To take the gateway 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 gateway offline permanently, select **Take this gateway offline and reschedule all meetings currently on this gateway**.

Step 6 Select **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 a gateway offline before you can remove it from the Cisco Unified Videoconferencing Manager database.

Procedure

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

Step 2 Select **Gateway**.

Step 3 Select the gateway entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gateway**.

Step 3 Enter the partial or complete name of the gateway in the Name field.

Step 4 Select **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 select **Search**.

CHAPTER 7

Configuring a Cisco Unified Videoconferencing Desktop Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Creating or Modifying a Desktop Profile, page 7-1
- Removing a Desktop Profile, page 7-2
- Searching for a Desktop Profile, page 7-2
- How to Stream Meetings Using Cisco Unified Videoconferencing Desktop, page 7-3

Creating or Modifying a Desktop Profile

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

Procedure

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

Step 2 Select **CUVC Desktop**.

Step 3 Select the link in the Name column for the Desktop you require, or select **Add** to create a new Desktop profile.

Step 4 Enter the name and management IP address of the Desktop in the relevant fields.

Step 5 Enter the URL used by participants to join a meeting via Desktop in the **Web Access URL** field.

The URL must be in the format http://<web URL>:<port number>/cuvm.

Step 6 Enter an H.323 ID used to identify connections from Desktop in MCU conferences in the H.323 ID field.

Ensure that the same H.323 ID is configured in the Desktop administrator web interface.

Make sure that the H.323 protocol is enabled on the MCU as the Desktop Server communicates with the MCU in the H.323 mode only.

Configuring this field allows Resource Manager to route calls from this Cisco Unified Videoconferencing Desktop Server based on the predefined IP topology.

Step 7 Select a topology setting from the Location list. The default value is Home.

The Location field is visible only when the IP Topology tab is activated in the 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 email invitations sent to meeting participants. Select Direct Access URL to add a URL that allows accessing the meeting directly, without entering the meeting ID.

Step 9 Enter the maximum capacity allowed by your Desktop license in the Maximum Capacity field.

Step 10 (Optional) Select **Secure Connection using TLS** to secure the transport link between Cisco Unified Videoconferencing Manager and Desktop.

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

Removing a Desktop Profile

Procedure

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

Step 2 Select **CUVC Desktop**.

Step 3 Select the Desktop entry you want to delete in the Name column.

Step 4 Select **Delete** and then **OK**.

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

Searching for a Desktop Profile

Procedure

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

Step 2 Select **CUVC Desktop**.

Step 3 Enter the partial or complete name of the Desktop in the **Name** field.

Step 4 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of Desktops, clear the Name field, and then select **Search**.

How to Stream Meetings Using Cisco Unified Videoconferencing Desktop

- Enabling Streaming on Desktop, page 7-3
- Enabling Streaming for a Virtual Room, page 7-3
- Allowing Recording by Specified Roles, page 7-3
- Allowing Recording by Specified Users, page 7-4
- Enabling Recording for Specified Virtual Rooms, page 7-4

Enabling Streaming on Desktop

Procedure

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

Step 2 Select **Look and Feel**.

Step 3 Set Streaming to **Visible**.

Step 4 Select **OK** to save your changes.

Enabling Streaming for a Virtual Room

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select the link in the Name column for the user you require, or select **Add** to create a new user profile.

Step 3 Select **Virtual Room Setting**.

Step 4 Set Streaming to **Enabled**.

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

Allowing Recording by Specified Roles

Procedure

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

Step 2 Select **Default User Settings**.

Step 3 Select the user types that you want to allow to record meetings from the list in the Default Recording Permissions section.

Step 4 Select **OK** to save your changes.

Allowing Recording by Specified Users

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require.

Step 4 Select **Advanced**.

Step 5 (Optional) Select **Allow user to record meetings** to enable this user to record meeting regardless of the global policy.

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

Enabling Recording for Specified Virtual Rooms

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require.

Step 4 Select **Virtual Room Setting**.

Step 5 Select **Record the meeting when 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 when the meeting is scheduled.

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

CHAPTER 8

Configuring a Meeting Room Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

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

- Enabling Meeting Room Support, page 8-1
- Creating or Modifying a Meeting Room Profile, page 8-2
- Sending Meeting Details by Email, page 8-2
- Removing a Meeting Room Profile, page 8-3
- Searching for a Meeting Room Profile, page 8-3

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 Select **Advanced Settings** in the sidebar menu.

Step 2 Select **Look and Feel**.

Step 3 Deselect **Hide Meeting Rooms**.

Step 4 Select **OK** to save your changes.

Creating or Modifying a Meeting Room Profile

Procedure

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

Step 2 Select **Meeting Rooms**.

Step 3 Select the link in the Name column for the meeting room you require, or select **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 Select **OK** to save your changes.

Sending Meeting Details by Email

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

By default, this option is hidden.

Procedure

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

Step 2 Select **Look and Feel**.

Step 3 Deselect **Hide Meeting Notification E-mail for meeting rooms and terminals**.

Step 4 Select **OK** to save your changes.

Step 5 Select **Resource Management** in the sidebar menu.

Step 6 Select **Meeting Rooms**.

Step 7 Select the link in the Name column for the meeting room you require.

Step 8 Select **Meeting e-mail notification address** and enter the email 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 Select **OK** to save your changes.

Removing a Meeting Room Profile

Procedure

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

Step 2 Select **Meeting Rooms**.

Step 3 Select the meeting room entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Meeting Rooms**.

Step 3 Enter the partial or complete name of the meeting room in the Name field.

Step 4 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of meeting rooms, clear the Name field, and then select **Search**.

CHAPTER 9

Configuring a Terminal Profile in Resource Manager

Revised: January 27, 2010/OL-21622-01

- How to Create or Modify a Terminal Profile, page 9-1
- Removing a Terminal Profile, page 9-5
- Searching for a Terminal Profile, page 9-5

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 video conferencing.

- Defining H.323 IP Terminal Details, page 9-1
- Defining SIP IP Terminal Details, page 9-2
- Defining ISDN/PSTN H.320 Terminal Details, page 9-3
- Defining Mobile Terminal Details, page 9-4
- Defining Dual H.320 and H.323 Terminal Details, page 9-4

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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Terminals**.

Step 3 Select the link in the Name column for the terminal you require, or select **Add** to create a new terminal profile.

Step 4 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.

Step 5 Select **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 Enter the E.164 IP phone number of the terminal registered on the gatekeeper in the IP Phone Number field 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 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 Define the default bandwidth for the terminal in the Bandwidth field. Resource Manager uses the bandwidth number to reserve resources for this terminal.

Step 11 (Optional) Select an entry from the Meeting Room field to associate this terminal with a meeting room defined in Cisco Unified Videoconferencing Manager.

Step 12 (Optional) Select **VIP** to provide enhanced quality video to this terminal.

Step 13 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Terminals**.

Step 3 Select the link in the Name column for the terminal you require, or select **Add** to create a new terminal profile.

Step 4 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.

Step 5 Select **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(SIP)** from the Terminal Type list.

Step 8 Define the terminal name or terminal number in the SIP URI field, 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 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 (Optional) Select **VIP** to provide enhanced quality video to this terminal.

Step 12 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Terminals**.

Step 3 Select the link in the Name column for the terminal you require, or select **Add** to create a new terminal profile.

Step 4 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.

Step 5 Select **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 **ISDN/PSDN(H.320)** from the Terminal Type list.

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 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.

Step 11 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 12 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Terminals**.

Step 3 Select the link in the Name column for the terminal you require, or select **Add** to create a new terminal profile.

Step 4 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.

Step 5 Select **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 **Mobile** from the Terminal Type list.

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 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 Select **3G** for 3G terminals.

Step 12 Select **OK** to save your changes.

Defining Dual H.320 and H.323 Terminal Details

Procedure

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

Step 2 Select **Terminals**.

Step 3 Select the link in the Name column for the terminal you require, or select **Add** to create a new terminal profile.

Step 4 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in Resource Manager.

Step 5 Select **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 **Dual(H.320 and H.323)** from the Terminal Type list.

Step 8 Enter the E.164 IP phone number of the terminal registered on the gatekeeper in the IP Phone Number field 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 IP Bandwidth and ISDN Bandwidth fields. 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 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.

Step 12 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 13 (Optional) Select **VIP** to provide enhanced quality video to this terminal.

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

Removing a Terminal Profile

Procedure

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

Step 2 Select **Terminals**.

Step 3 Select the terminal entry you want to delete in the Name column.

Step 4 Select **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 Select **Resource Management** in the sidebar menu.

Step 2 Select **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 (Optional) Select **Display All** to include in the terminals displayed in the list all the terminals that are currently in the global address book.

Terminals in the global address book are indicted by a book icon after the terminal name.

Step 5 (Optional) Select **Conceal All** to remove from the terminals displayed in the list all the terminals that are currently in the global address book.

Terminals in the global address book are indicted by a book icon after the terminal name.

Step 6 Select **Search**.

Search results are listed.

Step 7 To return to the complete list of meeting rooms, clear the Name and Dialing Info fields, and then select **Search**.

CHAPTER 10

Defining Resource Manager Call Routing Modes

Revised: January 27, 2010/OL-21622-01

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 10-1
- Call Routing in SIP Deployments, page 10-2
- Masking Conference Topology with the Virtual MCU Feature, page 10-2

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 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gatekeeper/SIP server**.

Step 3 Select the link in the Name column for the gatekeeper you require, or select **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 Select **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 that spans 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, page 10-2
- Creating a Distributed Conference, page 10-3

Creating a Centralized Conference

This section describes how to use the Virtual MCU feature to establish 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 Select **OK** to save your changes.

Creating a Distributed Conference

This section describes how to use the Virtual MCU feature to establish 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 Select **OK** to save your changes.

CHAPTER 11

Viewing Network Device Performance and Availability

Revised: January 27, 2010/OL-21622-01

- Viewing Device Usage and Failure by Time Interval, page 11-1
- Viewing Device Usage and Failure by Time Interval and Period, page 11-2
- Viewing MCU Port Availability, page 11-3
- Generating a Report, page 11-4

Viewing Device Usage and Failure by Time Interval

You can view historical usage and failure information for all MCUs and gatekeepers configured in Resource Manager during a designated time period (the default time interval is 1 hour).

Procedure

Step 1 Select **Device Monitoring** in the sidebar menu.

Step 2 Select **Performance Monitor**.

Table 11-3 describes the information displayed on the Performance Monitor tab.

Table 11-3 Performance Monitor Tab Parameters

Parameter	Description
Device Name	Displays the alias name of the MCU or gatekeeper.
Model	Displays the device model.
Total Meetings	Displays the total number of meetings hosted on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created using Resource Manager.
Failed Meetings	Displays the total number of meetings that were unable to start on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created using Resource Manager.
% Failed Meetings	Displays the number of failed meetings divided by the total number of meetings.
Total Connections	Displays the total number endpoints involved in meetings hosted on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created using Resource Manager.
Failed Connections	Displays the total number of endpoints involved in meetings on the MCU that were unable to start during the designated time interval. These totals only include ad hoc and scheduled meetings created using the Resource Manager.
% Failed Connections	Displays the number of failed connections divided by the total number of connections.

Viewing Device Usage and Failure by Time Interval and Period

You can view historical usage and failure information by time interval for all MCUs and gatekeepers configured in Resource Manager during a designated time period. For example, usage per hour over a 15-day period.

Procedure

Step 1 Select **Device Monitoring** in the sidebar menu.

Step 2 Select **Statistics**.

Table 11-4 describes the information displayed on the Statistics tab.

Table 11-4 Statistics Tab Parameters

Parameter	Description
Device Name	Displays the name of the MCU or gatekeeper.
Model	Displays the device model.
Start Time	Displays the beginning of the time interval.
End Time	Displays the end of the time interval.
Meetings	Displays the total number of multipoint meetings hosted on the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created using Resource Manager. Gatekeeper information is not displayed.
Peak Connections	Displays the peak number of endpoint connections for MCU or gatekeeper during the designated time interval. Figures include only ad hoc and scheduled meetings created using Resource Manager. Gatekeeper information is not displayed.
Failed Meetings	Displays the total number of meetings unable to start on the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created using Resource Manager. Gatekeeper information is not displayed.
Failed Connections	Displays the number of endpoints involved in meetings that were unable to connect with the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created using Resource Manager. Gatekeeper information is not displayed.

Viewing MCU Port Availability

You can view MCU resource availability information during a designated time period.

Procedure

Step 1 Select **Device Monitoring** in the sidebar menu.

Step 2 Select **Resource Availability**.

Step 3 Select a meeting type and a starting date.

Step 4 Select **Previous** or **Next** to move between start times.

Step 5 Select the time interval at which you want to view resource availability information.

Information about reserved MCU ports for a designated time interval is displayed in the Reserved MCU Ports section.

Generating a Report

You can generate a report in .xls format, showing statistics about device usage between selected dates. Once you have saved the report, you can view it using Microsoft Excel.

Procedure

Step 1 Select **Device Monitoring** in the sidebar menu.

Step 2 Select **Resource Availability** or **Statistics**.

Step 3 Select the calendar icons by the From and To fields to select a start and end period within which to generate the report.

Step 4 Select **Generate Report**.

Information about each device is included in the report.

Step 5 Select **Save** to save the report.

Step 6 Browse to the location in which you want to save the file, enter the file name and type, and then select **Save**.

CHAPTER 12

Viewing Real-time Meeting Statistics in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Viewing the Number of Ongoing Meetings and Calls, page 12-1
- Viewing Port Utilization Information, page 12-2
- Viewing Organization Meetings and Calls, page 12-2
- Viewing the Creation Status of Meetings, page 12-2
- Searching for a Meeting, page 12-3
- Generating Reports, page 12-4
- Modifying Upcoming Meetings, page 12-6
- Viewing Host MCUs, page 12-6
- Terminating Meetings, page 12-6

Viewing the Number of Ongoing Meetings and Calls

You can see the total number of meetings, multipoint calls and point-to-point calls currently in progress, and the following additional statistics:

- Meetings—scheduled, ad hoc and recorded
- Multipoint calls—audio, video and total bandwidth
- Point-to-point calls—audio, video and total bandwidth

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Overall Status**.

Step 3 (Optional) Select **Number of Meetings** in the Ongoing Meetings Status section to jump to the Ongoing Meetings tab where you can see further details of all meetings that are currently in progress.

Step 4 (Optional) Select **Number of Calls** in the Ongoing Point-to-Point Calls Status section to jump to the Ongoing Point-to-Point Calls tab where you can see further details of all point-to-point calls that are currently in progress.

Viewing Port Utilization Information

You can see port utilization information for MCUs, gateways and Desktops configured in the system.

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Overall Status**.

Step 3 Locate the System Utilization Status section.

Viewing Organization Meetings and Calls

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings** to see all meetings that are currently in progress.

Step 3 Select **Ongoing Point-to-Point Calls** to see all point-to-point calls that are currently in progress.

Step 4 Select **Upcoming** to see all meetings that have not yet started.

Viewing the Creation Status of Meetings

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings** to see all meetings that are currently in progress.

Step 3 Select **Ongoing Point-to-Point Calls** to see all point-to-point calls that are currently in progress.

Step 4 Select **Upcoming** to see all meetings that have not yet started.

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 the 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, select the red status indicator, and then select **Retry** to resend the meeting information to the MCU.

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

Searching for a Meeting

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings**, **Ongoing Point-to-Point Calls** or **Upcoming**, 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.
- Select 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.

- Select 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 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of meetings, clear each of the fields.

Step 6 Select **Search**.

Monitoring a Meeting or Call

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings** or **Ongoing Point-to-Point Calls**.

Step 3 Select the link in the Subject field for the meeting or call you want to monitor.

Step 4 Enter the moderator PIN if one is used for this meeting or call.

Step 5 Select the Become Moderator icon.

The In-meeting Control interface is not available for meetings or calls in which you are not a participant or the organizer.

Generating Reports

On the Upcoming tab, you can generate a report in .xls 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 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Upcoming**.

Step 3 Select the calendar icon in the From and To fields to choose a start and end date for information in the generated report.

Step 4 Select **Generate Report**.

Table 12-5 describes the information categories that are included in a generated report.

Table 12-5 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)	MCU(s) 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.
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 Select **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 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Upcoming**.

Step 3 Select the subject of the meeting you want to modify.

Step 4 Enter the required information in the Meeting Detail page.

Viewing Host MCUs

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings** or **Upcoming**, as required.

All host MCUs are listed in the MCU column with an indication of whether the meeting is cascaded.

Terminating Meetings

Procedure

Step 1 Select **Meeting Monitoring** in the sidebar menu.

Step 2 Select **Ongoing Meetings** or **Ongoing Point-to-Point Calls**.

Step 3 Select the icon in the Terminate column for the meeting you want to terminate.

CHAPTER 13

Creating Statistical Reports of Meetings and Calls in Resource Manager

Revised: January 27, 2010/OL-21622-01

- Creating a Call Information Report, page 13-1
- Creating a Port Usage Report, page 13-2
- Creating a Resource Usage Report, page 13-3
- Viewing the Use of Ad Hoc and Scheduled Meetings, page 13-3
- Viewing Average Meeting Size, page 13-4
- Viewing Average Meeting Duration, page 13-4
- Generating Reports for Finished Meetings, page 13-5
- Viewing Finished Meetings, page 13-6
- Viewing the Termination Status of Meetings, page 13-6
- Searching for a Finished Meeting, page 13-7
- Viewing Host MCUs, page 13-8
- Removing Meetings from the History Tab, page 13-8

Creating a Call Information Report

Organization Administrators can create a report for calls based on any one of these criteria:

- Multipoint calls
- Point-to-point calls
- Gateway calls
- Calls per terminal
- Calls per virtual room

Service Provider Administrators can create a report for calls based on any one of these criteria:

- Multipoint calls
- Point-to-point calls
- Gateway calls

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **Create New Report**.

Step 3 Select an option from the Report Type field.

Step 4 Select the time period to be covered by the report in the Graph X-Axis field.

Step 5 Select a start and end time for the report in the relevant fields.

Step 6 Select **Total Number** or **Total Duration (Minutes)** in the Graph Y-Axis field.

Step 7 Select a week range and hour range where relevant.

Step 8 (Optional) Select **Recent Report** to see the last call report generated.

Step 9 Select **Generate**.

The report appears on the in the Usage tab.

Step 10 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Creating a Port Usage Report

You can create a report of the ports used by these network elements:

- MCU
- Gateway
- Desktop

The reports provide this information:

- System utilization peaks
- Terminal utilization
- Virtual room utilization

Procedure

Step 1 Select **Reports System and Statistics** in the sidebar menu.

Step 2 Select **Utilization**.

Step 3 Select **Create New Report**.

Step 4 Select an option from the Report Type field.

Step 5 Select the time period to be covered by the report in the Graph X-Axis field.

Step 6 Select a start and end time for the report in the relevant fields.

Step 7 Select a week range and hour range where relevant.

Step 8 (Optional) Select **Recent Report** to see the last port utilization report generated.

Step 9 Select **Generate**.

The report appears on the in the Utilization tab.

Step 10 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Creating a Resource Usage Report

This section is for Organization Administrators only.

You can create a report of how terminals and virtual rooms are being used on your network.

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **Utilization**.

Step 3 Select **Create New Report**.

Step 4 Select **Terminals Utilization** or **Virtual Room Utilization** from the Report Type field.

Step 5 Select up to 3 terminals or virtual rooms from the pop-up list and select **OK**.

Step 6 Select the time period to be covered by the report in the Graph X-Axis field.

Step 7 Select the start and end points for the report in the relevant fields.

Step 8 (Optional) Select **Recent Report** to see the last port utilization report generated.

Step 9 Select **Generate**.

The report appears on the in the Utilization tab.

Step 10 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Step 11 (Optional) Select **Generate Excel Report** to print your report to an Excel file.

Viewing the Use of Ad Hoc and Scheduled Meetings

You can see the proportion of your network meetings that are ad hoc or scheduled.

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **Statistics**.

Step 3 Select **Create New Report**.

Step 4 Select **Generate Meeting Statistics** from the Report Type field.

Step 5 Set the period of time the report will cover.

Step 6 (Optional) Select **Recent Report** to display the last generated port utilization report.

Step 7 Select **Generate**.

The report is displayed.

Step 8 (Optional) Select **Generate PDF Report** to convert the report into the pdf file.

Step 9 (Optional) Select **Generate Excel Report** to convert the report into the excel file.

Viewing Average Meeting Size

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **Statistics**.

Step 3 Select **Create New Report**.

Step 4 Select **Generate Average Meeting Size** from the Report Type field.

Step 5 Set the period of time the report will cover.

Step 6 (Optional) Select **Recent Report** to display the last generated port utilization report.

Step 7 Select **Generate**.

The report is displayed.

Step 8 (Optional) Select **Generate PDF Report** to convert the report into the pdf file.

Step 9 (Optional) Select **Generate Excel Report** to convert the report into the excel file.

Viewing Average Meeting Duration

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **Statistics**.

Step 3 Select **Create New Report**.

Step 4 Select **Average Meeting Duration** from the Report Type field.

Step 5 Set the period of time the report will cover.

Step 6 (Optional) Select **Recent Report** to display the last generated port utilization report.

Step 7 Select **Generate**.

The report is displayed.

Step 8 (Optional) Select **Generate PDF Report** to convert the report into the pdf file.

Step 9 (Optional) Select **Generate Excel Report** to convert the report into the excel file.

Generating Reports for Finished Meetings

You can generate a report in .xls 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.

If the generated report contains more than 10,000 records including meetings and calls, Cisco Unified Videoconferencing Manager asks whether you want the report to contain only the last 10,000 entries, or whether you prefer to abandon the current generating operation.

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **History**.

Step 3 Select the calendar icon in the From and To fields to choose a start and end date for information in the generated report.

Step 4 Select **Report**.

Table 13-6 describes the information categories that are included in a generated report.

Table 13-6 Generated Report Information Categories

Category	Description
Meeting ID/Party Number	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.
Meeting Subject/Party Name	Corresponds to Subject field in Meeting Scheduling.
Meeting Description	Description provided by a meeting initiator.
Location	Description provided by a meeting initiator.
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.

Table 13-6 Generated Report Information Categories (continued)

Category	Description
Services	MCU service used for the meeting.
MCU Name(s)	MCU(s) 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.
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 Select **Save** to save the report to a location of your choice.

Viewing Finished Meetings

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **History**.

Viewing the Termination Status of Meetings

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **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 the meeting.

Step 3 Select the red status indicator to view the Reason Failed error message.

Searching for a Finished Meeting

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **History**.

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.
- Select 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.
- Select 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 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of meetings, clear each of the fields.

Step 6 Select **Search**.

Viewing Host MCUs

Procedure

Step 1 Select **Reports and Statistics** in the sidebar menu.

Step 2 Select **History**.

All host MCUs are listed in the MCU column with an indication of whether the meeting is cascaded.

Removing Meetings from the History Tab

You can define a rule to instruct Video Admin 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 Select **Save**.

CHAPTER 14

Managing Resource Manager Users and User Groups without an External Directory

Revised: January 27, 2010/OL-21622-01

- Creating or Modifying a User Profile, page 14-1
- Removing a User Profile, page 14-2
- Searching for a User Profile, page 14-3
- Updating User Profiles, page 14-3
- Creating a User Group, page 14-4
- Modifying a User Group, page 14-4
- Removing a User Group, page 14-4
- Limiting Individual User Access to Meeting Types, page 14-5
- Limiting Group Access to Meeting Types, page 14-5
- Configuring Multiple Settings for User Groups, page 14-5

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, email, 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 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require, or select **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, email address and password for the user in the relevant fields, and confirm the password.

Step 6 (Optional) Select **Virtual Room Setting** to add or modify virtual room settings for the user.

Step 7 Select **Advanced**.

Step 8 Select a user type and enter telephone numbers in the relevant fields.

Step 9 Select **Select Terminal** to assign a default terminal to this user.

Step 10 Select **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 Select the group to which this user belongs from the Groups list.

Step 12 Select a default time zone.

Local time zones are used by default at User > My Meetings and User > All Meetings.

Step 13 Select **Enabled** in the Account Status field to activate the user account and allow the user to log in to Resource Manager.

Step 14 Select a recording policy option for this user from the Recording Policy list.

Step 15 Select a location preference for this user.

Step 16 Enable the user to log in to Desktop, if required.

Step 17 Select an allowed bandwidth for Desktop calls.

Step 18 Select **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

You cannot remove a user profile if:

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

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the user profile you want to delete in the Name column.

Step 4 Select **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 Select **User Management** in the sidebar menu.

Step 2 Select **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 Select **Search**.

Search results are listed.

Step 6 To return to the complete list of users, clear the Name or Virtual Room field, and then select **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 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select **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 Select **User Management** in the sidebar menu.

Step 2 Select **Groups**.

Step 3 Select **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 select the right-arrow button to move them to the Selected Contacts list.

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

The group appears in the Groups tab list.

Modifying a User Group

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Groups**.

Step 3 Select the link in the Name column for the user group you require.

Step 4 Modify the name of the user group.

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

Removing a User Group

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Groups**.

Step 3 Select the group you want to delete.

Step 4 Select **Delete** and then **OK**.

The user group is deleted from the scheduler.

Limiting Individual 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 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require, or select **Add** to create a new user profile.

Step 4 Select **Advanced**.

Step 5 Select **Select next to the Allowed Meeting Types** field.

Step 6 Select the required meeting types and select **OK**.

Step 7 Select **OK** to save your changes.

Limiting Group Access to Meeting Types

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Provisioning**.

Step 3 Select one or any of the groups listed in the Available Groups list and select the right-pointing arrow.

Step 4 Select **Allowed Meeting Types** and select Select.

Step 5 Select the required meeting types and select **OK**.

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

Configuring Multiple Settings for User Groups

The Provisioning tab offers a convenient way to set multiple parameters for large groups of users.

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Provisioning**.

Step 3 Select a group in the Available Groups list and select the right-pointing arrow to move the group to the Selected Groups list.

The following default groups are listed as well as any other groups that you have manually defined or imported from your directory server:

- All Users
- System Administrators
- Operators
- Meeting Organizers
- Regular Users

You can select more than one group at a time using the Crtl button on your keyboard.

Step 4 Select and configure the parameters you want to apply to the groups you have selected.

Step 5 Select **Update**.

CHAPTER 15

Provisioning Resource Manager Users Using a Directory Server

Revised: January 27, 2010/OL-21622-01

- Synchronization of User Information, page 15-1
- Accessing User Information in Active Directory Server, page 15-2
- Synchronizing Resource Manager with Active Directory Server, page 15-2
- Configuring a Connection to an LDAP Server, page 15-3
- Mapping Resource Manager User Roles to ADS Users, page 15-4
- Defining Virtual Rooms for All LDAP Users, page 15-5
- Forcing Resource Manager to Use a Virtual Room, page 15-6
- Resource Manager LDAP Information Attributes, page 15-6

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.

Accessing User Information in Active Directory Server

This section describes how to access user information in Microsoft Active Directory Server (ADS) 2000 and 2003.

Procedure

Step 1 Select one of the following paths to view information for a user in the host Active Directory Server (ADS), depending on the Active Directory version you are using:

- **Start > Programs > Administrative Tools > Active Directory Users and Computers**
- **Start > Settings > Control Panel > Administrative Tools > Active Directory Users and Computers**

Step 2 Open the **User** folder to access the user list.

Step 3 Right-click the required user in the user list and then select **Properties**.

Step 4 Select the **General** tab to view the user ID for the selected user.

Step 5 Select the **Account** tab to view the sign in name for the selected user.

Synchronizing Resource Manager with Active Directory Server

For the purposes of this topic, assume that Active Directory Server (ADS) includes an organizational unit (OU) called “China” with a sub-OU called “User”.

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
- Email 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 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.
- Email address.
- Belong to an OU.
- Belong to a group (if you want to assign user role based on group).

Step 4 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 5 To map specific Resource Manager user roles to ADS users, see the "Configuring a Connection to an LDAP Server" section on page 15-3.

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 video conferencing devices and terminals before defining LDAP server settings for user provisioning.

For deployments using Microsoft Active Directory you can secure user credentials in the bind requests which the Cisco Unified Videoconferencing Manager server sends using the LDAP server. In this case user credentials are encrypted using MD5 algorithm ensuring the highest security level.

For deployments using Microsoft Active Directory or IBM Domino you can secure the entire connection between the Cisco Unified Videoconferencing Manager server and the LDAP server.

Before You Begin

If you need to enable the Secure User Credentials feature, select the **Password never expires** and **Store password using reversible encryption** options in the Properties window of your Microsoft Active Directory. This way users who do not use a "strong password" cannot log into Resource Manager.

Procedure

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

Step 2 Select **LDAP Configurations**.

Step 3 Select **Add** to add a new LDAP server, or select 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.

Step 5 Enter the directory server domain or directory server URL in the Domain/URL field.

Note For the secure connection between the Cisco Unified Videoconferencing Manager and LDAP server use the Idaps:// prefix. For regular connection use the Idap:// prefix.

Step 6 Enter the directory server sign in ID and password in the relevant fields.

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 Select **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 Select **Close**.

The selected OUs are displayed in the LDAP Search Base field.

Step 10 (Optional) Select the **Secure User Credentials** check box.

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

Mapping Resource Manager User Roles to ADS Users

Procedure

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

Step 2 Select **LDAP Configurations**.

Step 3 Select **Advanced**.

Step 4 Select **Select next to each user type** to assign LDAP user groups to a specific Resource Manager user role.

You can assign multiple LDAP user groups to each Resource Manager user role.

The following user types are available:

- Organization Administrator
- Meeting Operator

- Meeting Organizer
- Regular User

By default, all users are assigned the Meeting Organizer 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.

Step 5 (Optional) Set the Default User Type field to **Don't download** to instruct Resource Manager not to download users that are not assigned to any listed Resource Manager user role.

Step 6 Select **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 Select **Advanced Settings** in the sidebar menu.

Step 2 Select **LDAP Configurations**.

Step 3 Select **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 Select **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 Go to **System Configuration > Scheduling Settings** in the Resource Manager Configuration Tool.

Step 2 Select **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 selected.

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 selected.

Resource Manager LDAP Information Attributes

Table 15-7 lists the LDAP information attributes used by Resource Manager.

Table 15-7 Resource Manager LDAP Information Attributes

Identifier	Attribute	Description
1	uid	User identifier
2	email	User email 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

Table 15-7 Resource Manager LDAP Information Attributes (continued)

Identifier	Attribute	Description
15	description	Description
16	zipCode	Zip code
17	address	Address

CHAPTER 16

Modifying Default Organization Settings for Resource Manager Users and Meetings

Revised: January 27, 2010/OL-21622-01

- Settings Priorities, page 16-1
- How to Define Default Settings for Organization Users, page 16-1
- How to Define Default Settings for Meetings, page 16-4
- Modifying the Look and Feel of the Resource Manager Web User Interface, page 16-9

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 16-2
- Defining a Default Time Zone for a User, page 16-2
- Defining Display Formats, page 16-2
- Defining Date Display Formats, page 16-3
- Defining Your Meeting Display Preferences, page 16-3
- Defining Default Recording Permissions, page 16-3

Defining Which Meeting Types are Available to New Users

Procedure

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

Step 2 Select **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 Select **OK** to save your changes.

Defining a Default Time Zone for a User

Procedure

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

Step 2 Select **Default User Settings**.

Step 3 Select a default time zone for the selected meeting types.

Step 4 Select **OK** to save your changes.

Defining Display Formats

Procedure

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

Step 2 Select **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 Select **OK** to save your changes.

Defining Date Display Formats

Procedure

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

Step 2 Select **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 Select **OK** to save your changes.

Defining Your Meeting Display Preferences

Procedure

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

Step 2 Select **Default User Settings**.

Step 3 Select **Display all meeting records on My Meetings screens** to display all meetings within the organization in My Meetings.

Step 4 Select **OK** to save your changes.

Defining Default Recording Permissions

Procedure

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

Step 2 Select **Default User Settings**.

Step 3 Select any or all of the user roles in the Default Recording Permissions section.

Step 4 Select **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 16-4
- Defining the Default Cascading Mode, page 16-5
- Defining the Maximum Number of Ports for an Ad Hoc Meeting, page 16-5
- Defining How to End a Meeting, page 16-5
- Defining the Meeting Default Length, page 16-6
- Defining the Default Dialing Mode, page 16-6
- Defining a Billing Destination, page 16-7
- Defining Required Default Resources, page 16-7
- Defining the Auto Attendant Dial-in Number, page 16-7
- Enabling Automatic Routing, page 16-8
- Customizing Invitation Email, page 16-8

Defining a Default Meeting Type

During this procedure you configure a default meeting type and a fallback meeting type which Resource Manager uses if it fails to create a meeting of the default type due to the lack of resources. The fallback mechanism is relevant only for ad hoc meeting creation and scheduled meeting upon creation.

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Select a default meeting type from the list or all new meeting templates and new meetings.

We recommend that you select a default meeting type which is available to all users.

Step 4 Select a fallback meeting type from the list.

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

Defining the Default Cascading Mode

Procedure

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

Step 2 Select **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 Media BladeEMP. 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 Select the priority from the Prioritize list 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

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

Defining the Maximum Number of Ports for an Ad Hoc Meeting

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Select a value from the Maximum number of ports option.

Step 4 Select **OK** to save your changes.

Defining How to End a Meeting

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Locate the Default settings for scheduled meetings section.

Step 4 Select **At scheduled time** in the Termination policy field to terminate the meeting according to the termination time define for the meeting.

Step 5 Enter a value in the **Alert n minutes before the meeting ends** 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 6 Select **n minutes after all participants have left the meeting** 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 7 Enter the required value in the **n minutes after all participants have left the meeting** field.

By default, you cannot automatically extended Resource Manager meetings to last more than 4 hours. Administrators can change this default via the Resource Manager Configuration Tool.

Step 8 Select **OK** to save your changes.

Defining the Meeting Default Length

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Enter the default length of a meeting in minutes in the Duration field.

Step 4 Select **OK** to save your changes.

Defining the Default Dialing Mode

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Select **Dial-out** or **Dial-in** from the Default Dialing Mode list.

Step 4 Select **OK** to save your changes.

Defining a Billing Destination

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Select **Meeting host**, **Meeting organizer** or **All participants** in the Bill To field.

If the host and the organizer are the same person, the Meeting 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 Select **OK** to save your changes.

Defining Required Default Resources

Procedure

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

Step 2 Select **Default Meeting Settings**.

Select the default resources from the Required list 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 3 Select **OK** to save your changes.

Defining the Auto Attendant Dial-in Number

The Auto Attendant feature enables you to define the MCU service for entry into the IVR audio and video message utility.

This option is available only if you have selected the Use in Auto Attendant sessions option for one of the meeting types listed under Admin > Meeting Types > Active Meeting Types.

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Locate the Advanced Routing section.

Step 4 Select **Please specify the auto attendant number** and enter the dial-in number for the Auto Attendant feature.

Verify that this number does not begin with any MCU or Gateway service or internal gatekeeper zone prefix, or is the same as the number of an IP terminal

Step 5 (Optional) Select **Allow creating new meetings** to allow users to create new meetings using this auto attendant number.

Step 6 (Optional) Select **Prompt for a meeting PIN while creating new meetings** if you want users to enter a PIN when creating or entering a conference using this service.

Step 7 (Optional) Select **Display all meeting records on the Auto Attendant menu** to enable users to see all meeting records when creating or entering a conference using this service.

Step 8 Select **OK** to save your changes.

Enabling Automatic Routing

Procedure

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

Step 2 Select **Default Meeting Settings**.

Step 3 Locate the Routing section.

Step 4 Select **Automatically route incoming calls according to schedule. Please specify the auto route number.** and enter an e.164 number containing up to10 characters.

When an endpoint dials to the specified e.164 number, Cisco Unified Videoconferencing Manager reviews all ongoing meeting and meetings due to start in 5 minutes, and routes the call to the destination meeting according to the source number of the call and the meeting schedule.

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

Customizing Invitation Email

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

Procedure

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

Step 2 Select **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 email.

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 email.

Step 6 (Optional) Select **Override IP Terminal Access Information** and enter your text to override default access information for IP terminals.

Step 7 (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 8 (Optional) Select **Hide the Attendees list** to hide the attendees section in the invitation email.

Step 9 (Optional) Select **Hide in-meeting control access information** to hide the instructions for accessing the meeting via the in-meeting control interface from the invitation email.

Step 10 (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 11 Select **OK** to save your changes.

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

Procedure

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

Step 2 Select **Look and Feel**.

Step 3 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
- 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 4 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 5 Use the Invite Attendees By field to indicate whether to invite attendees in groups or per terminal at Meeting Scheduling > Invite.

Step 6 Select **Visible** or **Hidden** to determine whether the Reserved Ports field is displayed or hidden at Meeting Scheduling > Invite.

Step 7 Select **Visible** or **Hidden** to determine whether the PSTN/ISDN and Dial-in columns are displayed or hidden at Meeting Scheduling > Attendees Settings.

Step 8 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 9 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.

Step 10 Select the following options as required:

- 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 email and time zone fields for meeting rooms and terminals are enabled. If meeting rooms and terminals are enabled, they can directly receive notification emails.
- 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—If chosen, there is 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 11 Select **OK** to save your changes.

CHAPTER 17

Using the Cisco Unified Videoconferencing Manager Configuration Tool

Revised: January 27, 2010/OL-21622-01

During the 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 Cisco Unified Videoconferencing Manager Configuration Tool, a client-server application based on Java Web Start, enables the system administrator to configure Cisco Unified Videoconferencing Manager system settings, set Call Data Record (CDR) preferences, and modify default value settings.

- Setting Up the Java Runtime Environment, page 17-2
- Launching the Cisco Unified Videoconferencing Manager Configuration Tool, page 17-2
- Retrieving an Administrator Password, page 17-3
- Uninstalling the Cisco Unified Videoconferencing Manager Configuration Tool, page 17-3
- How to Modify General Settings, page 17-3
- How to Modify Scheduling Settings, page 17-7
- Hiding Resource Manager User Interface Screens, page 17-11
- How to Manage Custom Time Zones, page 17-11
- Customizing Product and Vendor Logos, page 17-14
- Creating a Customized Billing Field, page 17-14
- Defining Database Server Settings, page 17-15
- How to Define Security Settings, page 17-15
- How to Configure SNMP Trap Server Profiles, page 17-17
- Defining Utilization Thresholds, page 17-18
- How to Define Call Data Record (CDR) Settings, page 17-19

Setting Up the Java Runtime Environment

Install Java Runtime Environment on the client computer before using the Cisco Unified Videoconferencing 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 computer.

If Java Runtime Environment is not installed on the client computer, a download message appears.

Step 2 Select **Install Java Runtime Environment**.

Step 3 Select **download on the Java download web page**.

The Java Runtime Environment is installed on the client computer.

Step 4 To return to the Cisco Unified Videoconferencing Manager Configuration Tool, select **previous page on the Java download web page**.

Launching the Cisco Unified Videoconferencing Manager Configuration Tool

The Cisco Unified Videoconferencing Manager Configuration Tool is accessible from any client computer 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 Select **Launch CUVCM RM Configuration Tool**.

The Cisco Unified Videoconferencing Manager Configuration Tool checks for the latest version of the Java Web Start application on the client computer, and then starts the Cisco Unified Videoconferencing 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, select **Run**.

To avoid the appearance of this message upon launch of the Cisco Unified Videoconferencing Manager Configuration Tool from the same site address, in the message window, select **Always trust content from this publisher**, and then select **Run**.

Step 4 Select **Launch CUVCM RM Configuration Tool** on the Resource Manager launch page.

Step 5 Enter the login and password of the Service Provider Administrator or an Organization Administrator.

Step 6 Select **Login**.

The Cisco Unified Videoconferencing Manager Configuration Tool window opens.

Retrieving an Administrator Password

Procedure

Step 1 In the login window, select the down arrow to open the lower part of the login window in the Cisco Unified Videoconferencing Manager Configuration Tool login window.

Step 2 Enter the administrator login ID in the Send Admin Password for Login ID field.

Step 3 Select **Send** to send the administrator password to the email address associated with the login ID.

Uninstalling the Cisco Unified Videoconferencing Manager Configuration Tool

Procedure

Step 1 Go to **Settings > Control Panel > Add or Remove Programs** on the client computer.

Step 2 Select Cisco Unified Videoconferencing Manager **Configuration Tool**, and select **Remove**.

How to Modify General Settings

- Defining Email Server Settings, page 17-4
- Defining the Unconnected Endpoint Time Period, page 17-4
- Defining User Provisioning Options, page 17-5
- Defining Table Row Display, page 17-5
- Defining the Command Delay, page 17-6
- Defining the Parent Zone Authorization Filter, page 17-6
- Defining the Log Level, page 17-7
- Defining the Resource Manager Server Name and Web Port, page 17-7

Defining Email Server Settings

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

Procedure

Step 1 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter the email server IP address or domain name in the Host field.

Step 3 Enter the email server communications port number in the Port field.

Step 4 Enter the email server login ID and password in the relevant fields to enable access to the email server.

Step 5 Select **E-mail meeting organizer upon** to send an email 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 select **EP connection**.

  If you select **Dial-in considered**, dial-in connections are considered as endpoints and email notifications are sent in the case of a dial-in connection failure.

Step 7 Select **Save**.

Defining the Unconnected Endpoint Time 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 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter a value in seconds in the EP Unconnected Time Out field.

Step 3 Select **Save**.

Defining User Provisioning Options

This section is for Organization Administrators.

Procedure

Step 1 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select **Enable integration with directory server** to change the user provisioning mode if no integration was selected during Cisco Unified Videoconferencing Manager installation.

Note Changing the user provisioning mode removes current users from the Cisco Unified Videoconferencing Manager database.

Step 3 Select **Enable Single Sign On (SSO)** to allow users to log in without entering a user name or password.

When SSO is enabled, a user who is logged into the organization domain and then tries to access the Cisco Unified Videoconferencing Manager Web login window, is authenticated transparently according to the ADS domain account and password credentials that the user enters in the Cisco Unified Videoconferencing Manager Web login window.

Step 4 Select **Save**.

Defining Table Row Display

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

Procedure

Step 1 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter a value in the Number of table rows per page field.

Step 3 Select **Save**.

Defining the Command Delay

You can define the time interval that Resource Manager waits when sending sequential internal messages to the MCU.

Procedure

Step 1 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Release 5.x MCUs only.

Enter 100 for deployments containing Release 4.x MCUs.

Step 3 Select **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 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select the Enable Parent Zone Authorization Filter field.

Step 3 Select **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 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select one of the following options in the Log Level field:

- WARN—This is the standard setting that we recommend 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 Select **Save**.

Defining the Resource Manager Server Name and Web Port

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

Procedure

Step 1 Select **System Configuration > General Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter the server name, port, login ID and password in the relevant fields.

Step 3 Select **Save**.

How to Modify Scheduling Settings

- Changing Call Authorization Settings, page 17-8
- Dynamically Cascading Multiple EMPs for a Single Conference, page 17-9
- Modifying Resource Manager Default Meeting Settings, page 17-9
- Modifying Default Recurring Meeting Settings, page 17-10

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 Select **System Configuration > Scheduling Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Deselect **Allow Endpoint Initiated Point to Point Calls** to prevent endpoint-initiated point-to-point calls.

Step 3 Deselect Allow Endpoint Initiated Multipoint Calls to prevent endpoint-initiated MCU calls

Step 4 Select **Allow Only Endpoint Initiated Virtual Room Meetings** to ensure that 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 selected.

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

Step 5 Select **Allow Advanced Virtual Room Management for Meeting Organizer** to enable Meeting Organizers to have multiple virtual rooms. When selected, 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 deselected. 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 deselected, a full list of the virtual rooms that belong to the user is displayed as well as all of the configuration tabs for each virtual room.

Step 6 Select **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 Select **System Configuration > Scheduling Settings** in the Resource Manager Configuration Tool interface.

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

We recommend 1 or 2 ports.

Step 3 Select **Save**.

Modifying Resource Manager Default Meeting Settings

Procedure

Step 1 Select **System Configuration > Scheduling Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 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 hoc participants not on the original invited list to be removed from 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 deselect this field, and disconnected participants remain 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.

The meeting ends if the host does not join within the specified time.

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 Select **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 Select **System Configuration > Scheduling Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter a value in days in the Schedule Recurring Meetings field.

The maximum value is 730 days (2 years).

Step 3 Select **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.
- Meeting Monitoring 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 Virtual Room sections accessible via the User sidebar menu.
- My Meetings section accessible via the User sidebar menu.

Procedure

Step 1 Select **System Configuration > UI Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select the screens you wish to show.

Step 3 Deselect the screens you wish to hide.

Step 4 Select **Save**.

How to Manage Custom Time Zones

- Selecting a Time Zone Profile, page 17-12
- Viewing a Time Zone Profile, page 17-12
- Adding Daylight Saving to a Time Zone Profile, page 17-12
- Creating a Customized Time Zone Profile, page 17-13
- Removing a Customized Time Zone Profile, page 17-13
- Reverting to Default Time Zone Settings, page 17-14

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 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select a time zone in the Available Time Zones list.

Step 3 Select the right-pointing arrow to move the time zone to the Selected Time Zones list.

Step 4 Select **Save**.

Viewing a Time Zone Profile

Procedure

Step 1 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Save**.

Creating a Customized Time Zone Profile

Procedure

Step 1 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select **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 in 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 Select **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 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select a custom defined time zone from either the Available Time Zones list or the Selected Time Zones list.

Step 3 Select **Remove** below the Available Time Zones list or the Selected Time Zones list.

Step 4 Select **Yes**.

Step 5 Select **Save**.

Reverting to Default Time Zone Settings

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

Procedure

Step 1 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Move, modify or create time zone profiles.

Step 3 Select **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 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter the name of a file that contains the logo in the Product logo file name field, or select **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 Select **Save**.

Creating a Customized Billing Field

Procedure

Step 1 Select **System Configuration > Customized Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Save**.

Defining Database Server Settings

Procedure

Step 1 Select **System Configuration > Database Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Test** to verify that the database configuration is correct.

A message window shows the test results.

Step 6 Select **Reset** to revise your configured database server settings.

Step 7 Select **Save**.

Step 8 Restart Resource Manager to apply your changes.

How to Define Security Settings

- Defining Password Settings, page 17-16
- Defining a Login Message, page 17-16
- Unlocking a User Account, page 17-16

Defining Password Settings

Procedure

Step 1 Select **System Configuration > Security Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Save**.

Defining a Login Message

Procedure

Step 1 Select **System Configuration > Security Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select **Display login message** and enter a login message in the text box that becomes active.

Step 3 Select **Save**.

Unlocking a User Account

Procedure

Step 1 Select **System Configuration > Security Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Unlock**.

Step 4 Select **Save**.

How to Configure SNMP Trap Server Profiles

- Adding an SNMP Trap Server Profile, page 17-17
- Modifying an SNMP Trap Server Profile, page 17-17
- Removing an SNMP Trap Server Profile, page 17-18

Adding an SNMP Trap Server Profile

Procedure

Step 1 Select **System Configuration > SNMP Trap Servers Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Enter the required IP address for the SNMP trap server in the Server IP Address field.

Step 3 Enter the port used by the SNMP trap server in the Server Port field.

Step 4 Select **Add**.

Step 5 Select **Save** at the bottom of the screen.

Step 6 Select **Yes**.

Modifying an SNMP Trap Server Profile

Procedure

Step 1 Select **System Configuration > SNMP Trap Servers Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select the SNMP trap server entry that you want to modify.

Step 3 Enter the new SNMP trap server IP address and port number as required.

Step 4 Select **Edit**.

Step 5 Select **Save** at the bottom of the screen.

Step 6 Select **Yes**.

Removing an SNMP Trap Server Profile

Procedure

Step 1 Select **System Configuration > SNMP Trap Servers Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select the SNMP trap server that you want to remove.

Step 3 Select **Delete**.

You cannot delete a server if it is the only server in the list.

Step 4 Select **Save** at the bottom of the screen.

Step 5 Select **Yes**.

Defining Utilization Thresholds

You can define any of the following threshold limits:

- Utilization threshold for MCU audio ports
- Utilization threshold for MCU video ports
- Utilization threshold for gateway ports
- Utilization threshold for Desktop ports
- Utilization threshold for net bandwidth

Procedure

Step 1 Select **System Configuration > SNMP Trap Servers Settings** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Locate the Utilization Threshold Settings section.

Step 3 Enter the required values in the relevant threshold fields.

Step 4 Select **Save** at the bottom of the screen.

Step 5 Select **Yes**.

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 17-19
- Defining Required Terminal Connection Duration, page 17-19
- Defining a CDR File Prefix, page 17-20
- Defining How Often CDRs Are Produced, page 17-20
- Enabling Streaming to a RADIUS Server, page 17-21

Creating CDR Information in XML Format

Procedure

Step 1 Select **CDR Configuration** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

Step 2 Select **Enable XML CDR**.

Step 3 Enable CDRs for meeting scheduling, rescheduling and/or cancellation.

Step 4 Select **Save**.

Defining Required Terminal Connection Duration

Procedure

Step 1 Select **CDR Configuration** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **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 Select **CDR Configuration** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Save**.

Defining How Often CDRs Are Produced

Procedure

Step 1 Select **CDR Configuration** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **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 Select **CDR Configuration** in the Cisco Unified Videoconferencing Manager Configuration Tool interface.

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 Select **Save**.

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

CHAPTER 18

Configuring Cisco Unified Videoconferencing Manager Redundancy

January 27, 2010/OL-21622-01

- About Redundant Mode, page 18-1
- Configuring the Redundant Mode, page 18-1
- Viewing Redundancy Status, page 18-2
- Disabling the Redundant Mode, page 18-3

About Redundant Mode

The Cisco Unified Videoconferencing Manager redundant solution is based on two Cisco Unified Videoconferencing Manager servers which act as a master/slave hot swap mechanism. The redundant solution supports an internal gatekeeper and an internal database.

Configuring the Redundant Mode

The Cisco Unified Videoconferencing Manager redundant solution is based on two Cisco Unified Videoconferencing Manager servers which act as a master/slave hot swap mechanism. The redundant solution supports an internal gatekeeper and an internal database.

Before You Begin

- For an existing redundant deployment, verify that Cisco Unified Videoconferencing Manager is installed on an additional server.
- Verify that two MS-SQL databases are installed and configured to work in the Mirror failover mode.
- For a new redundant deployment, verify that Cisco Unified Videoconferencing Manager products are installed on two separate MCS servers.
- Decide which Cisco Unified Videoconferencing Manager server will act as a master in the deployment.

Procedure

Step 1 On the Cisco Unified Videoconferencing Manager server which you want to be a master, select **Start > Programs > Cisco Unified Videoconferencing Manager > Redundant Cisco Unified Videoconferencing Manager Configuration**.

The redundancy tool starts.

Step 2 Select **Master**, and then select **Next**.

Step 3 In the next screen enter the Public Server IP address (Virtual IP address reachable by both of the Cisco Unified Videoconferencing Manager servers), Probe IP address (Gateway IP address), and the IP address for this server and the remote server. If the MS SQL Database is used, specify the database-related settings. Select **Next**.

Step 4 Select **Next** to start the configuration. At this stage the Resource Manager service is stopped.

The configuration process on this service is paused until you run the redundancy tool on the other Cisco Unified Videoconferencing Manager server.

Step 5 On the other Cisco Unified Videoconferencing Manager server select **Start > Programs > Cisco Unified Videoconferencing Manager > Redundant Cisco Unified Videoconferencing Manager Configuration.**

The redundancy tool starts.

Step 6 Select **Slave**, and then select **Next**.

Step 7 Select **Next** to start the configuration. At this stage the Resource Manager service is stopped.

The redundancy tool on the master server communicates with the redundancy tool on the slave server and configures redundancy.

When the configuration is completed successfully the success message is displayed.

Step 8 In the redundancy tool window on the master Cisco Unified Videoconferencing Manager server, select **Finish**.

Step 9 In the redundancy tool window on the slave Cisco Unified Videoconferencing Manager server, select **Finish**.

Viewing Redundancy Status

Once the redundancy mode is configured you can view the redundancy real-time status at any time by selecting the redundant deployment status on the Resource Manager toolbar  .

You can view the following information:

- Virtual IP
- Probe IP
- Master Server Native IP
- Slave Server Native IP
- Last Hot Swap
- Slave Server Status

Disabling the Redundant Mode

Procedure

Step 1 On the master Cisco Unified Videoconferencing Manager server select **Start > Programs > Cisco Unified Videoconferencing Manager > Redundant** Cisco Unified Videoconferencing Manager **Configuration**.

The redundancy tool starts.

Step 2 Select **Yes**, and then select **Next**.

The configuration process starts. When the redundant mode is disabled the success message is displayed.

Step 3 Select **Finish**.

Step 4 Repeat this procedure on the slave Cisco Unified Videoconferencing Manager server.

CHAPTER 19

Resource Manager CDR XML Tags and Attributes

Revised: January 27, 2010/OL-21622-01

The production and storage of Call Data Records (CDRs) in Resource Manager is enabled using 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 19-1
- Index of CDR XML Tags, page 19-2
- Understanding the CDR XML Tags, page 19-9

Note All references to "VCS" in this section are equivalent to "Resource Manager".

Accessing the CDR XML Files

Procedure

Step 1 Select **Programs > Cisco Unified Videoconferencing Manager > CDR files** from the Windows Start menu.

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 the "Index of CDR XML Tags" section on page 19-2.

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”.

Table 19-8 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/>

Table 19-8 Index of CDR XML Tags (continued)

<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>
<Resources>
<Conference-Service>
<Service-Id />
<MCU-Service-Prefix />
<Min-Video-Layout />
<Max-Video-Layout />
<Max-Bit-Rate-In />
<Max-Bit-Rate-Out />
<Max-Frame-Rate-In />
<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>

Table 19-8 Index of CDR XML Tags (continued)

<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>

Table 19-8 Index of CDR XML Tags (continued)

<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>

Table 19-8 Index of CDR XML Tags (continued)

<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 />

Table 19-8 Index of CDR XML Tags (continued)

<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 />

Table 19-8 Index of CDR XML Tags (continued)

<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>
<ConnectedMCUs>
<Connected-GWs>
<Gateway-information>
<ID />
<Phone-Number />
<Service-Prefix />
<Service-Bandwidth />

Table 19-8 Index of CDR XML Tags (continued)

<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 19-9 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 19-9 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.			

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Conference> </Conference>	Contains basic meeting scheduling information.			
<Basic-Information></Basic-Information>	Contains basic meeting scheduling information.			
<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.			
<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) using Resource Manager or an endpoint. Possible values: Scheduled, Ad Hoc, Endpoint Initiated Ad Hoc.	value	String	<Scheduled- Adhoc value="Ad Hoc" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Start-Time />	Contains the scheduled start time of the meeting.	value	yyyy-mm-ddTh h-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:X X (Integer + 'Minutes')	<Server-Time Zone value="GMT+08:0 0"/>
<Auto-Extend />	Determines whether or not Auto Extend is selected during meeting scheduling.	value	Boolean	<AutoExtend value="true"/>
<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/></Ad vanced-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 using the Resource Manager.	value	yyyy-mm-ddTh h-m m-ssZ	<DateTime-Scheduled value="2003-03-29 T11:35:47Z" />
<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-ddTh h-m m-ssZ	<DateTime-Cancelled value="N/A" />
<Streaming-Recording-Activated/>	Indicates whether streaming recording is enabled or not.	value	Boolean	<Streaming-Record ing-Activated value="false"/>

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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 name of the recorded file, 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"/>
<Conference-Lifecycle-Summary><Conference-Life Cycle-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-ddTh h-m m-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></Resources>	Contains a list of resources committed or required for a meeting.			
<Conference-Service></Conference-Service>	Contains a list of meeting types scheduled for use.			

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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"/>
<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" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Max-T120-Ports-Reserved />	Contains the total number of T120 ports reserved for the meeting.	value	Integer	<Max-T120-Ports-Reserved value="0"/>
<Max-Subconferences/>	Contains the number of breakout meetings (or sub-meetings) that are a part of the selected meeting type.	value	Integer	<Max-Subconferences value="0" />
<Resources-Scheduled-At-Time-Of-Conference></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></Attendees-Terminals>	Contains lists of attendees and terminals scheduled for a conference.			
<Host></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 19-9 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></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 19-9 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></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 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<External-Attendees> </External-Attendees>	Contains a list of external meeting attendees (attendees not registered to Resource Manager).			
<External-Attendee> </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> </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-PART Y-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 19-9 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> </External-Terminals>	Contains a list of external terminals (terminals not registered to Resource Manager) scheduled for the meeting.			
<External-Terminal> </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" />
<MCU />	Contains MCU information of the external terminal.	value	String	<MCU value="0001-MCU-10001" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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></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@testco.com" LoginId = "Mjones"/>
<Network-Devices> </Network-Devices>	Contains information about network devices scheduled for use in a meeting during resource allocation.			
<GKs></GKs>	Contains a list of all gatekeepers reserved for use during a meeting.			
<GK-Proxy-Information> </GK-Proxy-Information />	Contains information about an individual gatekeeper that is reserved for use during the meeting.			

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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> </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="Term inal" />
<MCUs></MCUs>	Contains a list of all MCUs reserved for use during the meeting.			
<MCU-Information></MCU-In formation>	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" />
<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+" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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-1 0001" />
<Service-Prefix />	Specifies the service prefix of an MCU.	value	String	<Service-Prefix value="80" />
<List-of-Assigned-Terminals>< /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="8125 18" IP-ISDN-SIP="IP"/ >
<Gateways></Gateways>	Contains a list of all gateways reserved for use during the meeting.			
<Gateway-Information></Gate way-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" />
<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" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<Zone-Prefix />	Specifies the zone prefix of a gateway.	value	String	<Zone-Prefix value="58" />
<Terminal-Gateway-Association></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></Rooms>	Contains a list of all rooms reserved for use during the meeting.			
<Room-Information></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/> </Terminal-Room- Association>	Contains a list of terminals and rooms to which they are assigned for the meeting.			
<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/> </Completed-Conference-Data>	Contains actual conference data collected during the course of the meeting and at the conclusion of the meeting.			

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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-ddTh h-m m-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-ddTh h-m m-ssZ	<Actual-End-Time value="2003-03-29 T11:47:43Z" />
<Actual-Predefined-Terminals> </Actual-Predefined-Terminals>	Contains a list of terminals registered to Resource Manager that actually participated in the meeting.			
<Actual-Predefined-Terminal>< /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" />
<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="192.168.22 3.23" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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></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-ddTh h-m m-ssZ; Dial-in/Dial-out; yyyy-mm-ddTh h-m m-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dial-out" Disconnection-Time="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Disconnect"/>
<Actual-External-Terminals></Actual-External-Terminals />	Contains a list of external terminals that actually participate in the meeting.			
<Actual-External-Terminal></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"/>

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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" />
<List-of-Connection-Records></List-of-Connection-Records>	Contains a list of records for each time the participating terminal connected to and disconnected from the meeting.			

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<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-ddTh h-m m-ssZ; Dial-in/Dial-out; yyyy-mm-ddTh h-m m-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dial-out" Disconnection-Time="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Discon nect" />
<Connected-MCUs></Connected-MCUs>	Contains a list of all MCUs actually used during the meeting.			
<MCU-Information></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" />
<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" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
<List-of-Assigned-Terminals></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></ConnectedGWs>	Contains a list of all gateways that actually participated in the meeting.			
<Gateway-Information></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" />
<Terminal-Gateway-Association></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" />

Table 19-9 CDR XML Tag Details (continued)

Tag	Description	Attribute	Type	Example
Actual bandwidth usage				
<Call-Rate>	Refers the call rate of a call or a gateway call.	value	String	<Call-Rate value="[64/128/..... ./]" />
<Scheduling-Data>	Refers to the bandwidth allocated for the call.	value	String	
<Completed-Conference- Data>	Refers to the actual bandwidth of the call. This parameter is relevant for both point-to-point calls and multipoint.	value	String	
Distinction between an audio-only call and a video call				
<Call-Type>	Specifies the call type of each call participant.	value	String	<Call-Type value="[Audio/ Video/Data only]">
<Scheduling-Data>	Specifies the call type for scheduled calls.	value	String	
<Completed-Conference- Data>	Specifies the actual call type during the call. This parameter is relevant for both point-to-point calls and multipoint.	value	String	
Video resolution indication				
<Video-Resolution>	Specifies whether the video resolution is full high definition (HD), high definition or standard (SD). If the call type is Audio, this parameter is not displayed.	value	String	<Video-Resolu tion value= "[Full HD/HD/SD]">
<Completed-Conference- Data>	Specifies the actual video resolution during the call. This parameter is relevant for both point-to-point calls and multipoint.	value	String	
Call Encryption Level				
<Encryption-Level>	Specifies the encryption level for each call participant.	value	String	<Encryption- Level value="Off /ON" />
<Completed-Conference- Data>	Refers to the actual encryption level during the call. This parameter is relevant for both point-to-point calls and multipoint.	value	String	

CHAPTER 20

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

Revised: January 27, 2010/OL-21622-01

- Component Identity via SSL, page 20-1
- How to Generate Certificates, page 20-1

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 identity of the owner.

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 20-1
- Prerequisites, page 20-2
- Using Keytool to Generate a Certificate, page 20-2
- Configuring JBoss to use SSL, page 20-4
- Accessing Resource Manager Using HTTPS, page 20-5

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 options 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 to be configured by the administrator as a trusted 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 that gives the user the option to trust the connection and add it to the trust file.

Prerequisites

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

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=yourcompanyname,DC=com"
-alias scheduler
-keypass yourpassword
-keystore filename.keystore
-storepass keystorepassword
```

Step 3 Specify RSA as the private key in the `-keyalg` command 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 in the `-keypass` command.

Step 5 Specify the name of the file containing the certificate in the `-keystore` command.

Step 6 Set a password to open the file containing the certificate in the `-storepass` command.

Step 7 If you do not want to send a certificate signing request, skip to the "Configuring JBoss to use SSL" section on page 20-4.

Step 8 Generate the certificate signing request. For example

```
D:\>keytool -certreq -v -alias scheduler
-file scheduler.csr
-keypass yourpassword
-keystore filename.keystore
-storepass keystorepassword
```

This request generates the following output:

```
Certification request stored in file <filename.csr>
```

Step 9 Send the filename.csr file to your selected CA for signing.

Step 10 Save the content of the signed certificate to a file. For example, filename.cer.

Step 11 Import the CA trusted root certificate into the keystore. For example

```
D:\>keytool -import -alias "rootbindir" -file "rootbin.cer"
-keystore filename.keystore
-storepass keystorepassword
```

where

- rootbindir is the directory containing the test CA root binary and text files.
- rootbin.cer is the test CA root binary file.

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

```
Certificate was added to keystore
```

Step 12 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 filename.cer
-keystore filename.keystore
-storepass keystorepassword
```

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 filename.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
```

and add the indicators shown in bold.

```
<!-- 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="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>

<!-- A AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="${jboss.bind.address}"
enableLookups="false" redirectPort="8443" debug="0"
protocol="AJP/1.3"/>

<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
```

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/
chap8.keystore"
keystorePass="rmi+ssi" sslProtocol = "TLS" />
<!-- -->
```

Step 4 Change the keystore file from `chap8.keystore` to `filename.keystore`.

Step 5 Change the keystorePass from `rmi+ssi` to `keystorepassword`.

Step 6 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.

Step 7 Restart JBoss.

Accessing Resource Manager Using 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 Select **Yes** to access Resource Manager.

Step 3 Select **View Certificate** to avoid this message in future logins.

Step 4 Select **Install Certificate**.

After the certificate is installed, the user will not see the security alert on subsequent sign ins.

PART 2

Network Manager

CHAPTER 21

Network Manager Overview

Revised: January 27, 2010/OL-21622-01

- About the Network Manager, page 21-1
- What the Network Manager Provides, page 21-1

About the Network Manager

The Network Manager is a simple-to-use network management system for Cisco Unified Videoconferencing deployments.

Designed with the network administrator in mind, the Network Manager provides a unified interface for managing all the devices (elements) in your video conferencing network, including:

- Cisco Unified Videoconferencing MCUs
- Cisco IOS H.323 Gatekeeper
- Cisco Unified Videoconferencing Gateways
- Third-party elements and endpoints: Polycom, Sony, Tandberg

System Requirements

The Network Manager communicates with Cisco elements using a variety of industry-standard protocols, such as SNMP, XML, Telnet and FTP.

Note Ports supporting these protocols must be available in each element in order to be managed by the Network Manager.

What the Network Manager Provides

The Network Manager is a fully compliant network management system that provides network-wide functionality for Cisco elements.

- Viewing Network Status, page 21-2
- Viewing Calls and Conferences, page 21-2

- Using Auto-Detect, page 21-3
- Configuring Basic Elements, page 21-3
- Viewing Alarms and Events, page 21-4
- Connecting to Element Managers, page 21-4
- Connecting to Terminal Managers, page 21-4
- Managing a Centralized Log, page 21-4
- Viewing Multiple Networks, page 21-5
- Configuring Offline Elements, page 21-5
- Defining Network Subsets, page 21-5
- Supporting Cisco IOS H.323 Gatekeeper, page 21-5
- Dragging and Dropping, page 21-5
- Monitoring Calls, page 21-5

Viewing Network Status

The Network Manager provides network administrators with the most critical network status information at a glance, including:

- Element information—Total number of elements, the number of faulty elements and the number of elements that are offline.
- Call information—Total number of calls in the network, the number of point-to-point calls and the number of conferences.
- Endpoint information.
- Bandwidth information—Inter-zone bandwidth usage.
- B-channel usage information.

All network status information is updated in real time by the Network Manager database.

Viewing Calls and Conferences

The Network Manager provides network administrators with a view of all calls and conferences currently taking place over the network.

One-click control allows the network administrator to view call details or to access the source or destination gatekeeper element manager per call, and to link to the MCU Conference Control interface to assume full control of any conference in the list.

With these views, administrators can quickly determine:

- Call source and destination alias
- Call source and destination gatekeeper
- Call allocated resources
- The MCU controlling the conference
- Conference type.

- Conference video and bandwidth settings.
- Number of participants—including the current number, the number reserved and the number of local participants.

Using Auto-Detect

The Network Manager uses an automatic detection mechanism for discovering the Cisco elements present on the network. This information is saved to the Network Manager database and is used to create the various network views available via the Network Manager interface. Auto-detect can be run at regular intervals and whenever the server is restarted. Auto-detect can also be manually initiated at any time.

Note The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

Configuring Basic Elements

The Network Manager provides network administrators with the ability to view and edit the most commonly used configuration parameters of various elements in the network, such as MCUs, gatekeepers, gateways, and TANDBERG and Polycom endpoints.

Configuring an MCU

Network administrators can configure the following MCU parameters, using the Network Manager:

- Gatekeeper IP address
- MCU type (such as MCU or MP Only)

Configuring a Gatekeeper

Using the Network Manager, network administrators can configure the following Gatekeeper parameters:

- GKTMP port
- LRQ hop count

Configuring a Gateway

Using the Network Manager, network administrators can configure the following gateway parameters:

- Gatekeeper IP address
- Location

Configuring Endpoints

For Polycom and Sony endpoints network administrators can configure the following endpoint parameters:

- Gatekeeper IP address
- Endpoint alias name and E.164 number

For TANDBERG endpoints network administrators can configure the following endpoint parameters:

- Endpoint alias name and E.164 number
- Auto answer
- Trap server address
- SNMP community

Viewing Alarms and Events

The Network Manager provides network administrators with a list of the alarms currently active in any of the elements in the network. The list is constantly updated by the system, ensuring that any problems are located without delay. One-click access from any alarm directly to the administration interface of the device ensures that problems can be investigated and dealt with immediately.

In addition, the Network Manager provides a list of all events that have taken place in the network. This list can be filtered by the network administrator, as required.

Connecting to Element Managers

The Network Manager provides one-click access to the administration interfaces (element managers) of all the elements in the network, regardless of type, without the need to log in individually to each element. This gives network administrators the ability to perform a full range of management and configuration procedures on individual elements. Links to element managers can be found throughout the Network Manager interface, including the Alarm and Event views, the Conferences view and the various network views.

Connecting to Terminal Managers

In addition to providing one-click access to element managers, the Network Tree view of the Network Manager also provides one-click access to the Web-based management systems of some common endpoints registered to the network.

Managing a Centralized Log

The Network Manager provides centralized log management at both the network and element type levels. Using the Settings View, network administrators can define the size of the network log file, as well as the number of backups to maintain and the level of activity detail to include in the log. In addition, the Network Manager can be used to keep logs for those elements types, such as MCU elements and gateways, that do not maintain log files of their own.

Viewing Multiple Networks

The Network Manager provides network administrators with multiple options for viewing the elements in the network, including a Network Tree view with elements arranged in a tree structure according to zone, a Network Table view that displays a single, unified list of all network elements, as well as a Network Map view that displays elements and network status information in a graphic, multi-layered format.

The Network Tree view features a default view based on the zones in the IP conferencing network. However, the Network Manager also enables network administrators to create custom views. By creating folders and placing elements into them, administrators can view the network in whatever arrangement works best, such as dividing the network according to location. The views created in the Network Tree view can also be displayed in graphic format in the Network Map view.

Configuring Offline Elements

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.

Defining Network Subsets

The Network Manager enables administrators to define subsets of the network and restrict users with specific profiles to control certain network areas. Administrators can configure the network subsets using criteria to include or exclude certain zones and element types.

Supporting Cisco IOS H.323 Gatekeeper

The Network Manager provides extensive monitoring, configuration and management capabilities of the Cisco IOS H.323 Gatekeeper including local and remote zone setup, bandwidth policies, prefixes, logs, debugging and Telnet commands.

Dragging and Dropping

The Network Manager provides Network Tree drag and drop functionality for convenient element hierarchy management. Element addressing details are automatically updated in the tables of related elements. This feature can be used during offline configuration.

This feature is not available for Polycom endpoints.

Monitoring Calls

The Network Manager supports a comprehensive calls view detailing endpoint information, source and destination gatekeepers, bandwidth settings and call disconnection capabilities.

CHAPTER 22

Viewing Your Network in Network Manager

Revised: January 27, 2010/OL-21622-01

- How to View the Network as a Tree, page 22-1
- Viewing the Network as a Table, page 22-2
- Viewing the Network as a Map, page 22-3

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 22-1
- Creating a Custom Network Tree View, page 22-2

Configuring Network Hierarchy

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

The following element relationships can be configured using the drag and drop feature:

- Gatekeeper Parent - Child
- Gatekeeper - MCU/Gateway

Network Manager automatically updates element tables for Gatekeeper parent and child elements in the relationship. Network Manager updates MCU, gateway and endpoint elements with the appropriate gatekeeper IP address.

Procedure

Step 1 Select **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 Select **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 select **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 Select **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
- Resource usage versus capacity

Step 2 Select 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 Select **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 23

Managing Elements in Network Manager

Revised: January 27, 2010/OL-21622-01

- Displaying General Element Information, page 23-1
- Management Status of Elements, page 23-2
- Viewing all Network Elements, page 23-2
- Creating or Modifying an Element Profile, page 23-3
- Removing an Element Profile, page 23-4
- Searching for an Element Profile, page 23-4
- Defining Default Element Access Settings, page 23-5
- Overriding Default Element Access Settings, page 23-5
- How to Upgrade Element Software, page 23-6
- Cancelling Pending Offline Configuration Settings, page 23-8
- How to Manage the Element Software Upgrade Upload Log, page 23-8
- How to Automatically Detect New Elements on the Network, page 23-9
- Accessing an Element Web User Interface, page 23-12
- Accessing the Monitor Tab for a Specified Element, page 23-12

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 Select **Network Tree** in the sidebar menu.

Step 2 Select the element you require in the tree.

Step 3 Select **Monitor**.

Step 4 (Optional) Select the link to display the element manager for the selected element.

Management Status of Elements

Table 23-1 describes the different types of element management status.

Table 23-1 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. 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. 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 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 Select **Network Tree** in the sidebar menu.

Step 2 Select Network root element.

Step 3 Select **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)

  Traffic usage versus capacity

Creating or Modifying an Element Profile

Procedure

Step 1 Select 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 select **Edit element**  .

Step 3 Select the location in the network view at which you want to add the new element, and do one of the following to create a new element profile:

- Select **Add > New > New element**.
- Select **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 (Optional) Select **Managed element** to enable Network Manager to manage the element.

This option is not available for endpoint elements.

Step 7 (Optional) Select **Allow offline configuration** to allow offline configuration of the element.

This option is not available for MCU or endpoint elements.

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 Select an option from the Gatekeeper IP field.

You can select the IP address of a gatekeeper already configured in the system, or you can select **No Gatekeeper** or **Upon endpoint configuration**.

Step 9 (Optional) Select **Set** Resource Manager **as the default trap server** to use Network Manager as the SNMP trap server for endpoint elements.

Step 10 Select **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 Select 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 select **Delete element**  .

Step 3 Select **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 Select 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**.
- Select **Find element**  .

Step 3 Enter the IP address of the element or select the element type.

Step 4 Select **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 Select **Settings** in the sidebar menu.

Step 2 Select **Element Management**.

Step 3 Select **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.

The SNMP option is not available for endpoint elements.

The HTTP option is not available for endpoint elements.

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 Select **Upload** to save the information to the Network Manager database.

Overriding Default Element Access Settings

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the required network element.

Step 3 Select **Access**.

Step 4 Select **Use default** to use the default access settings for the element type.

When deselected, all other tab options are enabled.

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 Select **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 (Gateway, 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 MCUs, gateways, as well as for Polycom, TANDBERG and Sony endpoints on your network.

- Adding a Software Upgrade File, page 23-6
- Modifying a Software Upgrade File, page 23-7
- Removing a Software Upgrade File, page 23-7

Adding a Software Upgrade File

Procedure

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

Step 2 Select **Element Management**.

Step 3 Select **Software Upgrade Files**.

Step 4 Select the type of element you require in the Show field.

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

Modifying a Software Upgrade File

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

Procedure

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

Step 2 Select **Element Management**.

Step 3 Select **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 select **Edit**.
- Right-click the software upgrade file you require and select **Edit**.

Step 6 Enter a new description for the upgrade file in the relevant fields.

Step 7 Select **OK** to save your changes.

Removing a Software Upgrade File

Procedure

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

Step 2 Select **Element Management**.

Step 3 Select **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 select **Delete**.
- Right-click the software upgrade file you require and select **Delete**.

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

The software upgrade file is removed from the database.

Cancelling Pending Offline Configuration Settings

Procedure

Step 1 Select **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 cleared.

How to Manage the Element Software Upgrade Upload Log

- Viewing Your Software Upgrade Upload History, page 23-8
- Uploading a File After a Failed Attempt, page 23-8
- Removing Entries from the Upload Log, page 23-9

Viewing Your Software Upgrade Upload History

Procedure

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

Step 2 Select **Element Management**.

Step 3 Select **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 Select **Settings** in the sidebar menu.

Step 2 Select **Element Management**.

Step 3 Select **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 select **Retry**.
- Right-click the log entry you require and select **Retry**.

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

Removing Entries from the Upload Log

Procedure

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

Step 2 Select **Element Management**.

Step 3 Select **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 select **Delete**.
- Right-click the log entry you require and select **Delete**.

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

Step 7 Select **Delete All** to remove all entries from the log.

Step 8 Select **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 for 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 23-3.

- Running the Auto-detect Mechanism Manually, page 23-10
- Running the Auto-detect Mechanism Automatically, page 23-10
- Adding or Modifying Auto-detect Element Access Information, page 23-11
- Removing an Element Type from the Auto-detect Mechanism, page 23-11

Running the Auto-detect Mechanism Manually

Procedure

Step 1 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 2 Select **Tools** > **Auto-detect elements**.

Step 3 Select **Yes**.

The Network Manager interface is updated accordingly.

The auto-detect procedure may take some time, depending on the size of the network.

Running the Auto-detect Mechanism Automatically

Procedure

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

Step 2 Select **Auto-detect**.

Step 3 (Optional) Select **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) Select **Run auto-detect every (hrs)** and set an hourly interval to instruct Network Manager to look for new elements periodically.

Step 5 (Optional) Select **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 Select **Upload** to save your changes.

Adding or Modifying Auto-detect Element Access Information

Procedure

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

Step 2 Select **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 select **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:

- Select **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 Define a description, SNMP write community, and user name and password in the relevant fields.

Step 8 Select **Enabled** to activate the new access settings.

Step 9 Select **OK** to save the information to the Network Manager database.

Removing an Element Type from the Auto-detect Mechanism

Procedure

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

Step 2 Select **Auto-detect**.

Step 3 Do one of the following:

- Select the element type you require and select **Delete**.
- Right-click the element type you require and select **Delete**.

Step 4 Select **OK** to save your changes.

Accessing an Element Web User Interface

Procedure

Step 1 Select 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–

Select the link to the name or IP address of the element.

Accessing the Monitor Tab for a Specified Element

Procedure

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

Step 2 Double-click the element you require in the table.

CHAPTER 24

Managing Endpoints in Network Manager

Revised: January 27, 2010/OL-21622-01

- Defining Default Endpoint Access Settings, page 24-1
- How to Override Default Endpoint Settings, page 24-2
- Retrieving Configuration Parameters, page 24-3
- How to Manage Endpoint Software Upgrade Files, page 24-4
- How to Manage Endpoint Configuration Files, page 24-6
- How to Upgrade Software for Selected Endpoints, page 24-7
- How to Update Configuration for Selected Endpoints, page 24-8
- Setting the Managed Status of TANDBERG and Polycom Endpoints, page 24-9
- Manually Adding a New Managed Endpoint, page 24-10
- How to Manage the Endpoint Upload Log, page 24-10

Defining Default Endpoint Access Settings

This section applies to TANDBERG, Polycom and Sony endpoints only.

Default access settings for common endpoint types recognized by the Network Manager allow the Network Manager to access these elements.

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

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **Access**.

Step 4 Select an element type.

Step 5 Define a user name and password in the relevant fields.

Step 6 Select **Upload** to save the information to the Network Manager database.

How to Override Default Endpoint Settings

- Overriding Default Endpoint Addressing, page 24-2
- Overriding Default Access Settings for a Selected Endpoint, page 24-2
- Configuring Endpoint Dialing, page 24-3

Overriding Default Endpoint Addressing

This section applies to TANDBERG and Polycom endpoints only.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the endpoint you require in the tree.

Step 3 Select the **Configure** tab.

Step 4 Select a gatekeeper IP address from the list of gatekeepers available on the network.

Step 5 Enter an E.164 number for the endpoint.

Step 6 Enter an H.323 alias for the endpoint.

Step 7 Select **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 TANDBERG, and Polycom endpoints only.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the endpoint you require in the tree.

Step 3 Select the **Access** tab.

Step 4 Select **Use default** to use default access settings defined by the endpoint.

When unchecked, Remote API port and Telnet prompt for Polycom endpoints only can be modified.

Step 5 Enter the user name required for communicating with the endpoint.

Step 6 Enter the password required for communicating with the endpoint.

Step 7 Select **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

Configuring Endpoint Dialing

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints**.

Step 3 Do one of the following:

- Select the endpoint you require in the Endpoints tab and select **Configure**, then select the **Dial** tab in the Endpoint control screen.
- Double-click the endpoint you require in the Endpoints tab and select the **Dial** tab in the Endpoint control screen.
- Right-click the endpoint you require in the Endpoints tab and select **Dial**.

Step 4 Enter the address that you want this endpoint to call in the Dial to address field.

Step 5 Enter the network endpoint that you want this endpoint to call in the Dial to network endpoint field.

Step 6 Select **Connect** to connect the endpoint to a call at the specified address or with the selected endpoint.

Step 7 Select **Dial Parameters to** specify the call type and whether the call is restricted to other incoming callers.

Step 8 Select **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

Retrieving Configuration Parameters

This section applies to TANDBERG, Polycom, and Sony endpoints only.

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 Select **Network Tree** in the sidebar menu.

Step 2 Select the endpoint you require in the tree.

Step 3 Do one of the following:

- Select **Endpoints**, select the endpoint you require in the Endpoints tab, and then select **Retrieve configuration file**.
- Right-click the endpoint you require and select **Update > Retrieve configuration file**.

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 Select **OK** to save the file in the Network Manager database.

How to Manage Endpoint Software Upgrade Files

Network Manager enables you to manage software upgrade files for TANDBERG, Polycom and Sony endpoints on your network.

- Adding a Software Upgrade File, page 24-4
- Modifying a Software Upgrade File, page 24-5
- Removing a Software Upgrade File, page 24-5

Adding a Software Upgrade File

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select the type of endpoint you require in the **Endpoint type** field.

Step 4 Select **Software Upgrade Files**.

Step 5 Select **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.

If the validation process fails, select another package file to upload.

Step 7 Enter a name and description for the upgrade file in the relevant fields.

Step 8 (TANDBERG and Polycom endpoints only) Enter a related version number for the upgrade file.

Step 9 Select **OK** to save your changes.

Modifying a Software Upgrade File

This section applies to TANDBERG, Polycom and Sony endpoints only.

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

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **Edit**.
- Right-click the software upgrade file you require and select **Edit**.

Step 6 Enter a description for the upgrade file in the relevant fields.

Step 7 Select **OK** to save your changes.

Removing a Software Upgrade File

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **Delete**.
- Right-click the software upgrade file you require and select **Delete**.

Step 6 Select **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 TANDBERG, Polycom, and Sony endpoints on your network.

- Viewing Saved Endpoint Configuration Files, page 24-6
- Modifying an Endpoint Configuration File, page 24-6
- Removing an Endpoint Configuration File, page 24-7

Viewing Saved Endpoint Configuration Files

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 TANDBERG, Polycom and Sony endpoints only.

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

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **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 Select **OK** to save your changes.

Removing an Endpoint Configuration File

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **Delete**.
- Right-click the log entry you require and select **Delete**.

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

The endpoint configuration file is removed from the database.

How to Upgrade Software for Selected Endpoints

This section applies to TANDBERG, Polycom and Sony endpoints only.

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.

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

- Upgrading Software for Sony Endpoints, page 24-7
- Upgrading Software for TANDBERG and Polycom Endpoints, page 24-8

Upgrading Software for Sony Endpoints

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints** in the required zone.

Step 3 Locate the endpoint you require from the list in the panel on the right.

Step 4 Do one of the following:

- Right-click the endpoint and select **Update > Upgrade Software**.
- Select the endpoint and select the **Update software** button.

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 5 Select the file with which to update the selected endpoints.

Step 6 Select **OK** to start upgrading endpoint software.

Upgrading Software for TANDBERG and Polycom Endpoints

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints** in the required zone.

Step 3 Right-click the endpoint you require from below the Endpoints node in the network tree.

Step 4 Select **Update > Upgrade Software**.

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 5 Select the file with which to update the selected endpoints.

Step 6 Select **OK** to start upgrading endpoint software.

How to Update Configuration for Selected Endpoints

This section applies to TANDBERG, Polycom and Sony endpoints only.

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.

- Updating Configuration for Sony Endpoints, page 24-8
- Updating Configuration for TANDBERG and Polycom Endpoints, page 24-9

Updating Configuration for Sony Endpoints

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints** in the required zone.

Step 3 Locate the endpoint you require from the list in the panel on the right.

Step 4 Do one of the following:

- Right-click the endpoint and select **Update > Update configuration**.
- Select the endpoint and select the **Update configuration** button.

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 5 Select the file with which to update the selected endpoints.

Step 6 Select **OK** to start updating endpoint configuration.

Updating Configuration for TANDBERG and Polycom Endpoints

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints** in the required zone.

Step 3 Right-click the endpoint you require from below the Endpoints node in the network tree.

Step 4 Select **Update > Update configuration**.

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 5 Select the file with which to update the selected endpoints.

Step 6 Select **OK** to start updating endpoint configuration.

Setting the Managed Status of TANDBERG and Polycom Endpoints

Managed endpoints are displayed below the Endpoints entry for each zone in the network.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Endpoints**.

Step 3 Right-click the endpoint you require in the Endpoints tab.

Step 4 Select **Manage**.

Step 5 (Optional) Modify the endpoint display name.

Step 6 (Optional) Select **Set** Resource Manager **as the default trap server** to use Network Manager as the SNMP trap server for the endpoint.

Step 7 Select **OK**.

Step 8 Select **Refresh** to update the new settings.

Manually Adding a New Managed Endpoint

This section applies to the TANDBERG and Polycom endpoints only.

Procedure

Step 1 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 2 Select the location in the network view at which you want to add the new endpoint and select **Add element**  .

Step 3 Enter the endpoint display name and IP address in the relevant fields.

Step 4 Select **Endpoint** in the Element type field.

Step 5 Select **TANDBERG** or **Polycom** in the Endpoint type field.

Step 6 Select an option from the Gatekeeper IP field.

You can select the IP address of a gatekeeper already configured in the system, or you can select **No Gatekeeper** or **Upon endpoint configuration**.

Step 7 (Optional) Select **Set** Resource Manager **as the default trap server** to use Network Manager as the SNMP trap server for these endpoints.

Step 8 Select **OK** to save your changes.

How to Manage the Endpoint Upload Log

Network Manager enables you to manage the upload log for TANDBERG, Polycom and Sony endpoints that support a software upgrade or an update configuration.

- Viewing Your Endpoint Configuration Upload History, page 24-11
- Uploading a File After a Failed Attempt, page 24-11
- Removing Entries from the Upload Log, page 24-11

Viewing Your Endpoint Configuration Upload History

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **Retry**.
- Right-click the log entry you require and select **Retry**.

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

Removing Entries from the Upload Log

This section applies to TANDBERG, Polycom and Sony endpoints only.

Procedure

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

Step 2 Select **Endpoint Management**.

Step 3 Select **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 select **Delete**.
- Right-click the log entry you require and select **Delete**.

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

Step 7 Select **Delete All** to remove all entries from the log.

Step 8 Select **OK** to save your changes.

CHAPTER 25

Managing an MCU in Network Manager

Revised: January 27, 2010/OL-21622-01

MCU configuration options vary according to MCU version.

- Setting Call Routing Devices, page 25-1
- Viewing Registered Multipoint Processors, page 25-1
- Viewing MCU Supported Services, page 25-2
- How to Back Up and Restore MCU Configuration Settings, page 25-2
- Configuring MCU Location, page 25-4

Setting Call Routing Devices

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Protocols**.

Step 4 Select **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 Select **Upload** to save your changes.

Viewing Registered Multipoint Processors

The term Multipoint Processors (MPs) refers to MCUs and EMPs.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Registered MPs** to view the list of MPs currently registered with the MCU.

Table 25-1 describes the information displayed on the Registered MPs tab.

Table 25-1 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 MCU operating in MP Only 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 may be the same as the current MCU if the MP is the media processing component of the current unit.
Description	Version number and type.

Viewing MCU Supported Services

The Services tab displays the list of services supported by the selected MCU Services can be edited by selecting the link to the MCU element manager above the Services table.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Services**.

How to Back Up and Restore MCU Configuration Settings

This feature is available for Cisco Unified Videoconferencing 5000 Series MCUs, but not for Cisco Unified Videoconferencing 3500 Series MCUs.

- Backing Up MCU Configuration Settings, page 25-3
- Restoring MCU Configuration Settings, page 25-3
- Modifying MCU Configuration File Information, page 25-3
- Deleting a Configuration File, page 25-4

Backing Up MCU Configuration Settings

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Backup & Restore**.

Step 4 Select **Backup**.

Step 5 Enter a description of the MCU configuration file in the Retrieve Configuration File window and select **OK**.

Step 6 Select **OK** in the "Configuration file backup successful" message window to complete the backup procedure.

Restoring MCU Configuration Settings

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Backup & Restore**.

Step 4 Select a configuration file from the list.

Step 5 Select **Restore**.

Step 6 Select **Yes** when prompted by the "Are you sure you want to restore ...?" message.

Modifying MCU Configuration File Information

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Backup & Restore**.

Step 4 Select a configuration file from the list.

Step 5 Select **Edit**.

Step 6 Modify the name and description of the configuration file, as required.

Step 7 Select **OK**.

Deleting a Configuration File

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Backup & Restore**.

Step 4 Select a configuration file from the list.

Step 5 Select **Delete**.

Step 6 Select **OK**.

Configuring MCU Location

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the MCU you require in the tree.

Step 3 Select **Configure**.

Step 4 Enter a string identifying the physical location of the MCU device in the Location field.

Step 5 Select **Upload**.

CHAPTER 26

Managing the Internal Gatekeeper in Network Manager

Revised: January 27, 2010/OL-21622-01

- How to Manage Services, page 26-1
- How to Manage Prefixes, page 26-4
- How to Configure a Parent Gatekeeper, page 26-5
- How to Manage Parent Filters, page 26-6
- How to Configure a Child Gatekeeper, page 26-7
- How to Manage Child Prefixes, page 26-9
- How to Configure a Neighbor Gatekeeper, page 26-10
- How to Manage Zones, page 26-12
- How to Manage Bandwidth Rules, page 26-13
- How to Manage Debug Flags, page 26-14

How to Manage Services

- Viewing Internal Gatekeeper Supported Services, page 26-2
- Creating or Modifying a Service, page 26-2
- Viewing Global Services, page 26-3
- Creating or Modifying a Global Service, page 26-3
- Removing a Service, page 26-4

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 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Services**.

Table 26-1 describes the information displayed on the Services tab.

Table 26-1 Services Tab Parameters

Parameter	Description
Prefix	Prefix used to access the service
Description	Service description
Status	Indicates whether the service is predefined or online
Conference Hunting	Indicates whether conference hunting is enabled for the service
In-Zone Default	Default policy for in-zone endpoints
Out of Zone	Service policy for out-of-zone endpoints

Creating or Modifying a Service

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **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 select **Edit**.
- Right-click the service you require and select **Edit**

Step 5 Do one of the following to create a new service:

- Select **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 Select **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 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Global Services**.

Table 26-2 describes the information displayed on the Global Services tab.

Table 26-2 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 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **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 select **Edit**.
- Right-click the service you require and select **Edit**.

Step 5 Do one of the following to create a new global service:

- Select **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 Select **OK** to save your changes.

Removing a Service

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Services** or **Global Services**.

Step 4 Do one of the following:

- Select the service you require and select **Delete**.
- Right-click the service you require and select **Delete**.

Step 5 Select **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 26-4
- Removing a Prefix, page 26-5

Creating or Modifying a Prefix

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Prefixes**.

Step 4 Select the prefix you require and select **Edit** to modify an existing prefix.

Step 5 Select **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 Select **Upload** to save your changes to the internal gatekeeper database.

Removing a Prefix

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Prefixes**.

Step 4 Select the prefix you require and select **Delete**.

Step 5 Select **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 26-5
- Adding a Parent Manually, page 26-6
- Adding a Parent Automatically, page 26-6

Enabling the Parent Tab

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Configure**.

Step 4 Select **Version 2** in the Dial plan version field.

Step 5 Ensure that Use Central Database is deselected.

Step 6 Select **Upload** to save your changes.

Adding a Parent Manually

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Parent**.

Step 4 Select **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 Select **Upload** to save your changes.

Adding a Parent Automatically

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Drag and drop the internal gatekeeper element into the zone of the gatekeeper you want 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 26-7
- Removing a Parent Filter, page 26-7

Creating or Modifying a Parent Filter

Procedure

Step 1 Select **Network Tree** in the sidebar menu.
Step 2 Select the internal gatekeeper you require in the tree.
Step 3 Select **Parent**.
Step 4 Locate the Parent Filters section.
Step 5 Select the parent filter you require and select **Edit** to modify an existing parent filter.
Step 6 Select **Add** to create a new parent filter.
Step 7 Enter a name for the parent filter and select **OK**.
Step 8 Select **Upload** to save the filter to the internal gatekeeper database.

Removing a Parent Filter

Procedure

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

How to Configure a Child Gatekeeper

- Enabling the Children Tab, page 26-8
- Viewing Child Gatekeepers, page 26-8
- Adding a Child Manually, page 26-9
- Adding a Child Automatically, page 26-9

Enabling the Children Tab

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Configure**.

Step 4 Select **Version 2** in the Dial plan version field.

Step 5 Ensure that Use Central Database is deselected.

Step 6 Select **Upload** to save your changes.

Viewing Child Gatekeepers

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Children**.

Table 26-3 describes the information displayed on the Children tab.

Table 26-3 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 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Children**.

Step 4 Select **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 Select **Upload** to save your changes to the internal gatekeeper database.

Adding a Child Automatically

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Drag and drop the internal gatekeeper element you want 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 26-10
- Removing a Child Prefix, page 26-10

Creating or Modifying a Child Prefix

Procedure

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

Removing a Child Prefix

Procedure

Step 1 Select **Network Tree** in the sidebar menu.
Step 2 Select the internal gatekeeper you require in the tree.
Step 3 Select **Children**.
Step 4 Open the required child gatekeeper profile.
Step 5 Select the prefix you require and select **Delete**.
Step 6 Select **Yes** to remove the prefix from the internal gatekeeper database.

How to Configure a Neighbor Gatekeeper

- Viewing Neighbor Gatekeepers, page 26-10
- Adding or Modifying a Neighbor Gatekeeper, page 26-11

Viewing Neighbor Gatekeepers

Procedure

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

Step 3 Select **Neighbors**.

Table 26-4 describes the information displayed on the Neighbors tab.

Table 26-4 Neighbors Tab Parameters

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

Adding or Modifying a Neighbor Gatekeeper

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **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 select **Edit**.
- Right-click the internal gatekeeper you require and select **Edit**.

Step 5 Do one of the following to create a new service:

- Select **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 Select **Upload** to save your changes to the internal gatekeeper database.

How to Manage Zones

- Creating or Modifying a Local Zone, page 26-12
- Creating or Modifying a Remote Zone, page 26-12
- Removing a Zone, page 26-13

Creating or Modifying a Local Zone

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Local Zones**.

Step 4 Select the zone you require and select **Edit** to modify an existing local zone.

Step 5 Select **Add** to create a new local zone.

Step 6 Enter a zone name and the zone domain.

Step 7 Select **Upload** to save your changes to the internal gatekeeper database.

Creating or Modifying a Remote Zone

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Remote Zones**.

Step 4 Select the zone you require and select **Edit** to modify an existing remote zone.

Step 5 Select **Add** to create a new remote zone.

Step 6 Enter a zone name, zone domain, IP address and port.

Step 7 Select **Upload** to save your changes to the internal gatekeeper database.

Removing a Zone

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Local Zones** or **Remote Zones**.

Step 4 Select the zone you require and select **Delete**.

Step 5 Select **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 26-13
- Creating or Modifying a Bandwidth Rule, page 26-14
- Removing a Bandwidth Rule, page 26-14

Viewing Bandwidth Rules

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **BW Rules**.

Table 26-5 describes the information displayed on the BW Rules tab.

Table 26-5 BW Rules Tab Parameters

Parameter	Description
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.

Table 26-5 BW Rules Tab Parameters (continued)

Parameter	Description
Session	Indicates the maximum bandwidth allowed for a session in the zone.
Default	Indicates whether or not the default value for all zones is configured in this rule.

Creating or Modifying a Bandwidth Rule

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **BW Rules**.

Step 4 Select the rule you require and select **Edit** to modify an existing bandwidth rule.

Step 5 Select **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 Select **Upload** to save your changes to the internal gatekeeper database.

Removing a Bandwidth Rule

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **BW Rules**.

Step 4 Select the bandwidth rule you require and select **Delete**.

Step 5 Select **Yes** to remove the bandwidth rule from the internal gatekeeper database.

How to Manage Debug Flags

- Creating or Modifying a Debug Flag, page 26-15
- Removing a Debug Flag, page 26-15

Creating or Modifying a Debug Flag

Restrictions

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

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Debug Flags**.

Step 4 Select the flag you require and select **Edit** to modify an existing debug flag rule.

Step 5 Select **Add** to create a new debug flag.

Step 6 Enter the debug command name, a description and enable the flag.

Step 7 Select **Upload** to save your changes to the internal gatekeeper database.

Removing a Debug Flag

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the internal gatekeeper you require in the tree.

Step 3 Select **Debug Flags**.

Step 4 Select the debug flag you require and select **Delete**.

Step 5 Select **Yes** to remove the debug flag from the internal gatekeeper database.

CHAPTER 27

Managing a Gateway in Network Manager

Revised: January 27, 2010/OL-21622-01

- How to Manage Services, page 27-1
- Configuring Gateway Addressing, page 27-2

How to Manage Services

- Viewing Gateway Supported Services, page 27-1
- Creating or Modifying a Service, page 27-1
- Removing a Service, page 27-2

Viewing Gateway Supported Services

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the gateway you require in the tree.

Step 3 Select **Services**.

Creating or Modifying a Service

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the gateway you require in the tree.

Step 3 Select **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 select **Edit**.
- Right-click the service you require and select **Edit**.

Step 5 Do one of the following to create a new service:

- Select **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 Select **OK**.

Removing a Service

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the gateway you require in the tree.

Step 3 Select **Services**.

Step 4 Do one of the following:

- Select the service you require and select **Delete**.
- Right-click the service you require and select **Delete**.

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

The service is removed from the database.

Configuring Gateway Addressing

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the gateway you require in the tree.

Step 3 Select **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 28

Configuring a User Profile in Network Manager

Revised: January 27, 2010/OL-21622-01

- Creating or Modifying a User Profile, page 28-1
- Removing a User Profile, page 28-2
- How to Define Network Subsets, page 28-2

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 Select **Settings** in the sidebar menu.

Step 2 Select **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 select **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:

- Select **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 Select **OK** to save your changes.

Removing a User Profile

Procedure

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

Step 2 Select **Users**.

Step 3 Do one of the following:

- Select the user you require and select **Delete**.
- Right-click the link in the User Name column for the user you require and select **Delete**.

Step 4 Select **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 28-2
- Removing a Network Subset, page 28-3
- Removing an Include or Exclude Criterion, page 28-3

Creating or Modifying a Network Subset

Procedure

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

Step 2 Select **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 select **Edit**.
- Right-click the network subset you require and select **Edit**.

Step 4 Do one of the following to create a new network subset:

- Select **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 select **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:

- Select **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 Select **OK** to add the criterion to the relevant list in the Add Network Subset window.

Step 10 Select **OK** to save your changes.

Removing a Network Subset

Procedure

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

Step 2 Select **Network Subsets**.

Step 3 Do one of the following:

- Select the network subset you require and select **Delete**.
- Right-click the network subset you require and select **Delete**.

Step 4 Select **OK** to save your changes.

Removing an Include or Exclude Criterion

Procedure

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

Step 2 Select **Network Subsets**.

Step 3 Do one of the following:

- Double-click the network subset you require.
- Select the network subset you require and select **Edit**.
- Right-click the network subset you require and select **Edit**.

Step 4 Do one of the following:

- Select the criterion you require and select **Delete**.
- Right-click the criterion you require and select **Delete**.

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

CHAPTER 29

Managing Traps and Alarms in Network Manager

Revised: January 27, 2010/OL-21622-01

- Sending Traps to Network Manager, page 29-1
- Creating or Modifying a Trap Forwarding Rule, page 29-2
- Disabling a Trap Forwarding Rule, page 29-3
- Removing a Trap Forwarding Rule, page 29-3
- Creating or Modifying an Alert Recipient Profile, page 29-3
- Removing an Alert Recipient Profile, page 29-4
- Viewing Generated Events, page 29-5
- Filtering Generated Events, page 29-5
- Viewing Events per Network Item, page 29-6
- Viewing and Sorting Supported Alarms, page 29-6
- Modifying Alarms, page 29-6
- Viewing and Sorting Generated Alarms, page 29-7
- Viewing Generated Alarms per Network Item, page 29-7

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 Select **Settings** in the sidebar menu.

Step 2 Select **Traps**.

Step 3 Select **Receive traps from elements**.

Step 4 Select **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.

You can also enable SNMP version 3 support to add privacy, authentication and access control to SNMP traps before forwarding them to the trap server.

Procedure

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

Step 2 Select **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 select **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:

- Select **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 (Optional) Select **Enable SNMP v3** to add security attributes to SNMP traps, and select a security level.

Note You can select this option only after selecting the **Enable trap forwarding** option.

- Low—No Authentication or Privacy
- Medium—Authentication without Privacy
- High—Authentication with Privacy

Step 9 (For Medium or High security only) Enter a user name and password for authentication of SNMP trap messages.

Step 10 (For Medium or High security only) Select a protocol for authentication of SNMP trap messages.

The default protocol is MD5.

Step 11 (For High security only) Enter a privacy password for encryption of SNMP trap messages.

Step 12 (For High security only) Select a privacy protocol for encryption of SNMP trap messages.

The default protocol is DES (56-bit).

Step 13 Select **OK** to save your changes.

Disabling a Trap Forwarding Rule

Procedure

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

Step 2 Select **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 select **Edit**.
- Right-click the trap rule you require and select **Edit**.

Step 4 Deselect **Enable trap forwarding**.

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

The trap forwarding rule is disabled but remains in the database.

Removing a Trap Forwarding Rule

Procedure

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

Step 2 Select **Traps**.

Step 3 Do one of the following:

- Select the trap rule you require and select **Delete**.
- Right-click the trap rule you require and select **Delete**.

Step 4 Select **OK** to save your changes.

The trap forwarding rule is removed from the database.

Creating or Modifying an Alert Recipient Profile

Procedure

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

Step 2 Select **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 select **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:

- Select **Add**.
- Right-click any link in the Recipient Name column and select **Add**.

Step 5 Enter the name and email 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 using email when the alarms have been cleared.

Step 9 (Optional) Select **Use custom subject line** to include a custom subject line in the email 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 Select **OK** to save your changes.

Removing an Alert Recipient Profile

Procedure

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

Step 2 Select **Alert Recipients**.

Step 3 Do one of the following:

- Select the alert recipient you require and select **Delete**.
- Right-click the alert recipient you require in the Recipient Name column and select **Delete**.

Step 4 Select **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 Select **Alarms** in the sidebar menu.

Step 2 Select **Events**.

The Events tab displays the following information:

- Event severity level (Minor, Cleared, Information, Warning, Minor, Major, Critical).
- Date and time of the event.
- Text message describing the event.

Step 3 Select 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 Select **Alarms** in the sidebar menu.

Step 2 Select **Events**.

Step 3 Do one of the following:

- Select **View > Filter events**.
- Select 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 select **OK**.

The events that correspond to your selection are displayed in the table.

Viewing Events per Network Item

You an view a table of the events that have occurred in the system related to a specific item in your network.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Network** or a relevant custom view.

Step 3 Select the network item you require.

Step 4 Select **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**.
- Select the **Current filter** link above the table.

Viewing and Sorting Supported Alarms

Procedure

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

Step 2 Select **Alarms**.

Step 3 Select the **Alarm** heading in the alarms table to view alarms generated by the managed elements in the network in alphabetical order.

Step 4 Select the **Severity** heading in the alarms table to sort the alarms by increasing or decreasing order of severity.

Modifying Alarms

Procedure

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

Step 2 Select **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 select **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 Select **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 Select **Alarms** in the sidebar menu.

Step 2 Select **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 Select **Network Tree** in the sidebar menu.

Step 2 Select **Network** or a relevant custom view.

Step 3 Select the network item you require.

Step 4 Select **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 30

Managing Calls and Conferences in Network Manager

Revised: January 27, 2010/OL-21622-01

- Viewing Current Call Details, page 30-1
- Viewing Current Call Details per Network Item, page 30-2
- Disconnecting Calls, page 30-2
- Searching for a Call, page 30-2
- Viewing Current Conferences, page 30-3
- Viewing Current Conferences per Network Item, page 30-4
- Searching for a Conference, page 30-4
- Accessing the Conference MCU, page 30-5

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 Select **Calls** in the sidebar menu.

Step 2 Select **Calls**.

Step 3 To display extended details per call, select on the table row and select **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.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Network** or a relevant custom view.

Step 3 Select the network item you require.

Step 4 Select **Calls**.

Step 5 To display extended details per call, select on the table row and select **Show call details**.

Disconnecting Calls

Procedure

Step 1 Select **Calls** in the sidebar menu and then select **Calls**

–or–

Select **Network Tree** in the sidebar menu, select the network item you require, and then select **Calls**.

Step 2 Do one of the following:

- Select the call(s) you want to disconnect and select **Disconnect selected call**.
- Select **Disconnect all calls**.

Searching for a Call

Procedure

Step 1 Select **Calls** in the sidebar menu and then select **Calls**

–or–

Select **Network Tree** in the sidebar menu, select the network item you require, and then select **Calls**.

Step 2 Select **Find**.

Step 3 Enter the call alias, IP address of the endpoint, or service ID.

Step 4 Select **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 Select **Calls** in the sidebar menu.

Step 2 Select **Conferences**.

Table 30-1 describes the information displayed on the Conferences tab.

Table 30-1 Conferences Tab Parameters

Parameter	Description
MCU	IP address of the MCU on the which the conference is being hosted. Select on the link to view the element manager of the MCU (Administrator).
Conference ID	Conference ID number. Select 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.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select **Network** or a relevant custom view.

Step 3 Select the network item you require.

Step 4 Select **Conferences**.

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 Select **Calls** in the sidebar menu and then select **Conferences**

–or–

Select **Network Tree** in the sidebar menu, select the network item you require, and then select **Conferences**.

Step 2 Select **Find**  .

Step 3 Enter the conference ID or the zone prefix.

Step 4 (Optional) Use the [*] wildcard to search for conferences.

Step 5 Select **Find**.

The row in the table matching your search criteria is highlighted.

Accessing the Conference MCU

Procedure

Step 1 Select **Calls** in the sidebar menu and then select **Conferences**

–or–

Select **Network Tree** in the sidebar menu, select the network item you require, and then select **Conferences**.

Step 2 To access the element manager of the MCU (Administrator), select the MCU link in the left-hand column of each table row.

Step 3 To access the MCU Conference Control interface, select the link in the Conference ID column.

This enables you to manage and take control of the conference.

CHAPTER 31

Configuring Logging for Network Manager

Revised: January 27, 2010/OL-21622-01

- Viewing Logs for a Selected Element, page 31-1
- Defining Network Manager Logging Activity, page 31-1
- Saving Element Logs, page 31-2
- Collecting Logs from a Cisco IOS H.323 Gatekeeper Element, page 31-2

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 Select **Network Tree** in the sidebar menu.

Step 2 Select the required network element.

Step 3 Select **Logs**.

Step 4 Define the log details for the selected network element.

Step 5 Select **Open log view** to view the logs directory for the selected network element.

Defining Network Manager Logging Activity

Procedure

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

Step 2 Select **Logging**.

Step 3 Select **Network Manager Logs**.

Step 4 Select Save Network 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.

The maximum log file size is 327,200 KB.

The maximum number of log files is 200.

Network Manager overwrites the oldest file with the next new file when disk space is full.

Step 6 Select the **View log directory** link to view a list of links to log files for Network Manager and managed network elements.

Step 7 Select **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 Select **Settings** in the sidebar menu.

Step 2 Select **Logging**.

Step 3 Select **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 Select **Upload** to save your changes.

Collecting Logs from a Cisco IOS H.323 Gatekeeper Element

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 2 Select the Cisco IOS H.323 Gatekeeper you require in the tree.

Step 3 Select **Debug Flags**.

Step 4 Select **Add**.

Step 5 Enter **debug ip icmp** in the Debug Command field to generate traffic and confirm logging is configured properly.

Step 6 Enter **Enable ip icmp debugging** in the Description field.

Step 7 Select **Enable**.

Step 8 Select **OK**.

A new alarm appears in the Alarms tab.

Step 9 Select **Logs**.

Step 10 Select **Save logs**.

Step 11 Enter a file name and set the log level to **Debugging**.

Step 12 Ping the Cisco IOS H.323 Gatekeeper to generate traffic to capture logs.

Step 13 Select **Open log view** to verify the result.

PART 3

Desktop

CHAPTER 32

How to Configure Cisco Unified Videoconferencing Desktop Server

Revised: January 27, 2010/OL-21622-01

- Accessing the Administration Interface, page 32-1
- How to View Status of Servers and Directory, page 32-2
- How to Configure Deployments, page 32-5
- How to Configure Client-Related Settings, page 32-8
- How to Configure Recording Server, page 32-11
- How to Manage Recordings, page 32-16
- How to Configure Streaming Server Settings, page 32-21
- How to Configure Messages and Invitations, page 32-24
- Configuring Sametime Settings, page 32-33
- Configuring a Local Administrator Account, page 32-33
- Configuring Local Directory of Terminals, page 32-34
- Increasing Cisco Unified Videoconferencing Desktop Server Memory, page 32-34
- Generating a PKCS12 Certificate Using Microsoft Certificate Service, page 32-35

Accessing the Administration Interface

Procedure

Step 1 Open the Internet browser.

Step 2 Enter the following URL:

http://<host>[:<port>]/cuvm/admin

where <host> is the location of your corporate Desktop Server.

Step 3 On the Administration page, enter your user name and password.

Step 4 Select **Sign In**.

The default user name and password are both “admin”

How to View Status of Servers and Directory

- Viewing Server Status and Port Resource Usage, page 32-2
- Viewing Directory Status, page 32-3
- Viewing Recording Server Status, page 32-4

Viewing Server Status and Port Resource Usage

The Status tab displays status information about the Cisco Unified Videoconferencing Desktop Server and other servers with which it interacts:

- Gatekeeper—Internal Gatekeeper.
- Streaming—Cisco Unified Videoconferencing Desktop Server. This information appears only if the Desktop Server is configured to manage streaming.
- Cisco Unified Videoconferencing 3500 MCU—MCU. This information is displayed only for basic deployments.
- Cisco Unified Videoconferencing Manager—Cisco Unified Videoconferencing Manager. This information is displayed only for advanced deployments.
- Sametime Server—Sametime Community Server. This information appears if the Cisco Unified Videoconferencing Desktop Server is configured to work with IBM Lotus Sametime Web.

Note In the Desktop Server GUI, Cisco Unified Videoconferencing 3500 MCU is referred to as ‘CUV MCU’.

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. Select the red indicator to view further error information.

The Status tab also shows port usage statistics and presents port usage graphically. Depending on your needs you may choose one of the graph reports described in Table 32-1.

Note We recommend that you wait five minutes after you run the Cisco Unified Videoconferencing Desktop Server before you refresh the Status tab to acquire the updated port information.

Table 32-1 Graph Views

Graph Report	Data is Collected Every...	This Number of Data Points is Collected...	Source
one hour	one minute	60	Desktop
6 hours	four minutes	90	Four data points from one hour report
24 hours	20 minutes	72	Five data points from 6 hour report
7 days	120 minutes	84	Six data points from 24 hour report
30 days	12 hours	60	Six data points from 7 day report

Depending on the deployment the Status tab also displays the following statistics:

- Number of participants in group calls
- Number of streaming ports

Sometimes group calls may exceed the allowed port limit because the limit is enforced at connecting time. If this happens, number of connected ports appears in red and the "Usage has exceeded the maximum allocated resources" warning is displayed.

If you set the call limit to a number lower than defined by the license, an error message is displayed next to the number of participants in group calls.

Viewing Directory Status

Select Status > Directory Status to display directory information. In deployments where Desktop is configured to work with Cisco Unified Videoconferencing Manager, Cisco Unified Videoconferencing Desktop Server must synchronize with Cisco Unified Videoconferencing Manager to download information about users and global policy. Cisco Unified Videoconferencing Desktop Server synchronizes with Cisco Unified Videoconferencing Manager when it connects to it for the first time; then Cisco Unified Videoconferencing Manager updates Cisco Unified Videoconferencing Desktop Servereach time there is new or modified information. There are the following synchronization states:

- Synchronized—Cisco Unified Videoconferencing Desktop Server is synchronized with Cisco Unified Videoconferencing Manager
- Synchronizing—Cisco Unified Videoconferencing Desktop Server is caching information from Cisco Unified Videoconferencing Manager. Users cannot search for users and terminals in the contact list or in the Invite dialog box.

- Not Synchronized—Cisco Unified Videoconferencing Desktop Server functions using locally cached information.The Desktop functionality is not influenced except one feature: standard sign in is not available.
- Synchronization error—Cisco Unified Videoconferencing Desktop Server is not synchronized with Cisco Unified Videoconferencing Manager, no information is cached. The Desktop functionality is reduced.

Related Topics

- How to Configure Streaming Server Settings, page 32-21

Viewing Recording Server Status

Select Status > Recording Status to access Recording Server information.

You can view the Recording Server Status information only if recording is enabled in your deployment.

The Recording Status tab displays this information:

- Recording Components:
  - 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 MCU.
- Recording Server Information:
  - 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. Select the icon for details.
- Storage Capacity—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.
- Recording Ports:
  - In Use—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.
  - Licensed—Shows the number of recording ports defined by the license.

- Available Recordings:
  - Completed—Shows the total number of completed recordings available for watching.
  - Reconstructed—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. Select the icon for more information.

How to Configure Deployments

- Deployment Types, page 32-5
- Configuring Settings for Single/Multiple-NIC Deployments, page 32-5
- Configuring Basic Deployment, page 32-6
- Configuring Advanced Deployment, page 32-7

Deployment Types

We strongly recommend to read the “Planning a Deployment Topology” chapter of the Cisco Unified Videoconferencing Solution Deployment Guide for detailed explanation of different topologies.

After you set the deployment type, the Administration web user interface changes to display only relevant configuration information.

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 may 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, it is recommended 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 Basic Deployment

This section describes how to configure a basic deployment where Desktop is configured to work with one specific MCU.

When you set the deployment type to Basic, these changes take place in the Administration web user interface:

- The local directory is displayed on the Directory tab under Directory and Authentication.
- The Allow meeting participants to record check box is enabled on the Settings tab under Recording.

MCUs can support dual NIC with IP separation which allows separating the media and signaling traffic from the management traffic. When this feature is enabled on an MCU, the XML control is sent on one NIC, and the XML cascade as well as all signaling and media are sent on a different NIC. If you configure the Cisco Unified Videoconferencing Desktop Server to work with an MCU on which this feature is enabled, you need to configure two MCU IP addresses: for media traffic and for management traffic.

Before You Begin

- Navigate to the Desktop Administration web user interface.
- If the dual NIC support feature is enabled on the MCU, determine the IP addresses used for the MCU Management Interface and Media and Signaling Interface.

Procedure

Step 1 Select **Deployment** in the sidebar.

Step 2 Select **Basic** from the deployment list.

Step 3 Enter the MCU IP address in the Management Address field.

If the dual NIC support feature is enabled on the MCU, select Use a different interface for media and signaling, and then enter IP addresses in the Management Address field and in the Media and Signaling Address field.

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”. There is no default password for Cisco Unified Videoconferencing 3500 Series MCU; for Cisco Unified Videoconferencing 5000 Series MCU the default password is “password”.

Step 6 If Cisco Unified Videoconferencing Desktop Server is configured with multiple IP addresses, select the relevant address from the Desktop Network Interface list.

Step 7 To enable recording:

a. Select the **Recording** check box.

b. Enter the Recording Server address.

Step 8 To enable streaming:

a. Select the **Streaming** check box.

b. Enter the Darwin Streaming Server address.

Step 9 Select **OK** or **Apply**.

The indicators next to the Cisco Unified Videoconferencing 3545 MCU Address and the Cisco Unified Videoconferencing Desktop Server fields show whether or not the connection to the target servers is successful. When the indicators are red, tooltips containing error details are displayed.

Related Topics

- *Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component*

Configuring Advanced Deployment

The source H.323 ID is used to allow Cisco Unified Videoconferencing Manager to identify Desktop. Cisco Unified Videoconferencing Manager contains a corresponding field and uses the source H.323 ID to identify clients from a particular Cisco Unified Videoconferencing Desktop Server, and then route clients to the appropriate MCU.

Before You Begin

Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Deployment** in the sidebar.

Step 2 Select **Advanced** from the deployment list.

Step 3 Enter the address of Cisco Unified Videoconferencing Manager.

Step 4 To use secure connection between Cisco Unified Videoconferencing Manager and Cisco Unified Videoconferencing Desktop Server, select the **Secure connection using TLS** check box.

Ensure the check box is also selected on Cisco Unified Videoconferencing Manager.

Step 5 If the Cisco Unified Videoconferencing Desktop Server is configured with multiple IP addresses, select the relevant address from the Desktop Network Interface list.

Step 6 Enter IP address of the gatekeeper.

Step 7 Enter the source H.323 ID of the Desktop.

The H.323 ID must match the Desktop H.323 ID configured on Cisco Unified Videoconferencing Manager.

Step 8 To enable recording, select the **Recording** check box, and then enter the Recording Server address.

Step 9 To enable streaming, select the **Streaming** check box, and then enter the Streaming Server address.

Step 10 Select **OK** or **Apply**.

The indicators next to the Address fields show whether connection to the target servers is successful or not. When the indicators are red, tooltips containing error details are displayed.

How to Configure Client-Related Settings

- Configuring Client Connection and Video Quality, page 32-8
- Configuring Meeting Features, page 32-10

Configuring Client Connection and Video Quality

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 MCU that enables H.323 endpoints to use a higher bandwidth rate or high definition without enabling high definition on Desktop, 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 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. The default value is 384K.

- High Definition

  This option allows Desktop Clients to connect to a conference in high definition mode. If you select this option, select a maximum call rate of at least 1024 Kbps or greater to enable the conference to continue in 720p high definition video resolution for all clients. For deployments using Cisco Unified Videoconferencing 3500 Series MCU, you may want to allow Desktop to reduce the video resolution from 720p to 480p if you set the call rate to 1024 Kbps and there is a bandwidth congestion during a conference.

  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.

  When Desktop is set to high definition mode and connected to a high definition service in deployments using MCU, Desktop limits fast update requests to avoid degradation of the video quality or frame rate to all the connected endpoints.

  If Desktop connects to a standard definition service or if there are no high definition ports left for the high definition service, then the standard definition maximum call rate 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 MCU and your network setting to avoid fragmentation.

If you need to limit UDP ports that are opened on the firewall to allow Desktop Conference Clients to send RTP to Desktop, you must define a multimedia port range. We recommend that you use a limited range between 10000 and 65535. If this option is used, each client connection uses 11 ports; therefore to define the range, multiply the number of connections allowed by your license by 11.

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.

If a server on which the Cisco Unified Videoconferencing Desktop Server is installed is not powerful enough to support 250 calls, you can use the call limit setting to reduce the number of allowed calls to limit the resources used by the system.

During this procedure you also configure Desktop public address which Desktop Clients use to connect to Cisco Unified Videoconferencing Desktop Server. To allow Clients from the public network to connect, use a FQDN they can resolve.

Before You Begin

Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Client** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 To configure settings for standard definition, select a bandwidth rate from the Maximum Call Rate list.

Step 4 To configure settings for high definition:

a. Select the **High Definition** check box.

b. Select a bandwidth rate from the Maximum Call Rate list.

c. If necessary, select the Allow CUV MCU version 5.x to negotiate high definition calls down to 480p check box.

Step 5 Enter a value in the MTU Size field.

Step 6 If necessary, configure a multimedia port range by entering the lowest multimedia port and the highest multimedia port values.

Step 7 Configure the public address.

Step 8 Enter a value in the Call Limit field.

Step 9 Select **OK** or **Apply**.

Related Topics

- Configuring Settings for Single/Multiple-NIC Deployments, page 32-5

Configuring Meeting Features

This section describes how to configure meeting features such as the meeting room, push to talk and security features.

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 Present button does not appear, but the various layouts are still available.

The Raise Hand feature allows a muted user to request the permission to speak. For deployments with multiple Cisco Unified Videoconferencing Desktop Servers, we recommend that you clear this check box. A moderator using one Cisco Unified Videoconferencing Desktop Server cannot see a request made by a participant using another Cisco Unified Videoconferencing Desktop Server.

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.

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".

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 select 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 select the microphone button to unmute themselves.
- Force users to hold down their microphone button while speaking—Participants must select and hold down the microphone button to activate their microphones and to send their audio output.

You can also configure these security features:

- sRTP media encryption between Desktop Clients and the Desktop Server— Encrypting media (audio, video, presentation) between Desktop Server and the Desktop Client may 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 web portal.
- Desktop callback—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 “data only” mode to a meeting from their computers and automatically connect their H.323 devices at the same time.

Note In “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 Administration web user interface.

Procedure

Step 1 Select **Client** in the sidebar.

Step 2 Select the **Meeting Features** tab.

Step 3 Configure the Desktop Sharing option as desired.

Step 4 Configure the Chat option as required.

For deployments with multiple Desktop Servers, it is recommended 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 5 Configure the Raise Hand option as desired.

For deployments with multiple Desktop Servers, it is recommended that you do not enable the Raise Hand option. A moderator using one Desktop Server cannot see the request of a participant using another Desktop Server.

Step 6 Define the additional custom panel option as desired:

a. Select the **Display an additional panel in the conference room** check box to enable the option.

b. Enter the URL in the field.

Step 7 Define the Push to Talk option as desired.

Step 8 Define security options as desired.

Step 9 Select **OK** or **Apply**.

Related Topics

- *Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component*

How to Configure Recording Server

After you enable recording for a basic or advanced deployment, 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. Desktop supports up to 10 simultaneous recordings.

Note Recordings made using Desktop release 5.x appear as public in Desktop version 7.0.

If you did not provide the Recording Server license key during Cisco Unified Videoconferencing Desktop Server installation, you still have a default evaluation license allowing to record one meeting at a time; each recording duration is limited to five minutes.

- About Configuring the Desktop Recording Server Connection, page 32-12
- Adding Recording Server to Deployment, page 32-12
- Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording, page 32-13
- Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording, page 32-15
- Modifying the Disk Space and Storage Location for Recordings, page 32-15

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 other Cisco Unified Videoconferencing Desktop Servers in the deployment can be configured 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.

Adding Recording Server to Deployment

If during the Cisco Unified Videoconferencing Desktop Server installation the Recording Server was not installed and users recorded meetings using the evaluation license, you can add the Recording Server to the deployment.

Before You Begin

Prior to modifying the Desktop installation, acquire the recording license and make sure you have the license key for the Recording Server.

Procedure

Step 1 Open the Control Panel.

Step 2 Select the Cisco Unified Videoconferencing Desktop Server and select **Change**.

The Cisco Unified Videoconferencing Desktop Server Installation Wizard opens.

Step 3 Select a language and select **OK**.

The Welcome screen is displayed.

Step 4 Select **Next**.

Step 5 Select **Modify**, and then select **Next**.

The Custom Setup screen opens.

Step 6 Select the **Recording Server** icon and select the **This feature will be installed on local hard drive** option.

Step 7 Select **Next**.

The Desktop License Key screen opens.

Step 8 Enter the license key for the Recording Server, and then select **Next**.

The Network Configuration screen opens.

Step 9 Select **Next** in the rest of the configuration screens.

Step 10 In the Ready to Modify the Program screen, select **Install**.

Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording

You can configure recording settings as well as manage recordings if you select this 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 may not resolve the Desktop Recording Server IP address. In this case the clients use the public address to connect to the Desktop Recording Server.

If Cisco Unified Videoconferencing Manager is configured to work with the Desktop Server in advanced deployments, recording policies configured on Cisco Unified Videoconferencing Manager determine whether users are allowed to record meetings or not. However, for basic deployments you need to define the recording policy on Cisco Unified Videoconferencing Desktop Server by enabling the recording option for Desktop users.

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.
- 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 sound signal played during a recording which serves to remind users that their meeting is being recorded.

In deployments where the Recording Server is installed on the same server as the Cisco Unified Videoconferencing Desktop Server, users watching recorded meetings take up Desktop bandwidth which can be used for other purposes, such as meetings. Use the Playback Bandwidth area to configure bandwidth usage for such deployments. Set the Total Bandwidth Allowed value to define a total amount of bandwidth Desktop uses for playing back recorded meetings. For example, if you set the Total

Bandwidth Allowed value to 100 Mb/s, then Desktop allows 100 Mb/s bandwidth if one user watches a recording and 50 Mb/s bandwidth for each user if two users watch recordings. You need to set the Minimum Bandwidth required for download value to prevent too many users watching recordings at the same time.

You can use the Cisco Unified Videoconferencing Manager to automatically record a scheduled meeting when the meeting begins.

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 Cisco Unified Videoconferencing 3500 Series MCU 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.

When you enable high definition recording in deployments using Cisco Unified Videoconferencing 3545 MCU, Cisco Unified Videoconferencing Desktop Server starts recording in high definition. If the attempt to record in high definition fails, the Cisco Unified Videoconferencing Desktop Server automatically switches to standard definition and continues recording.

Before You Begin

- Navigate to the Desktop Administration web user interface.
- Select **Deployment** in the sidebar, and verify that the **Recording** check box is selected.

Procedure

Step 1 Verify that the Recording Server address is configured correctly:

a. Select **Status** in the sidebar.

b. Select the **Recording Status** tab.

c. Verify that the IP address in the Recording Server Address field is correct.

Step 2 Select **Recording** in the sidebar.

The Settings tab is displayed.

Step 3 To configure standard definition recording, select a value from the Maximum Bit Rate list under Standard Definition.

Step 4 To configure high definition recording, perform the following:

a. Select the **High Definition** check box.

b. Select a value from the Maximum Bit Rate list under High Definition.

Step 5 Enter a value in the Maximum Recording Duration field.

Step 6 Enter a value in the Total Bandwidth Allowed field.

Step 7 Enter a value in the Minimum Bandwidth required for download field.

Step 8 From the Send tone periodically during recording list, choose an option.

Step 9 For advanced deployments, select the **Allow virtual rooms and scheduled meetings to be recorded automatically** check box to enable automatic recording when a meeting starts.

Step 10 In the Public Address field, enter a FQDN.

We recommend that you use a FQDN that clients can resolve.

Step 11 Enter the HTTP port.

This port is used by clients to access the recording.

You must configure the HTTP port on the Recording Server and open this port on the firewall.

Step 12 Select **OK** or **Apply**.

Related Topics

- *Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component*

Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording

If recording is disabled for your deployment, you can still select an alternate server to manage recordings.

Before You Begin

Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 Select the Allow playback of recordings from an alternate Desktop server check box.

Step 4 In the Server URL field, enter the URL of the alternate Desktop Server.

Step 5 Select **OK** or **Apply**.

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 Select **Start > Settings > Control Panel**.

Step 2 Double-click **Add or Remove Programs**.

Step 3 From the list of programs, choose Desktop, and then **Change**.

The Setup Wizard opens.

Step 4 In the Welcome screen select **Next**.

Step 5 In the Program Maintenance screen, choose **Modify**, and select **Next**.

Step 6 In the Custom Setup screen, select **Next**.

Step 7 In the Desktop Serial Key screen, select **Next**.

Step 8 In the Desktop Network Configuration screen, select **Next**.

Step 9 In the Desktop Hostname Configuration screen, select **Next**.

Step 10 In the Desktop Recording Configuration screen, modify the storage location:

a. Select **Change**.

b. Navigate to a new location.

c. Select **OK**.

Step 11 To modify the maximum amount of disk space, enter new value in the field.

Step 12 Select **Next**.

Step 13 Select **Install**.

How to Manage Recordings

- Viewing Recording Information, page 32-16
- Editing Recording Attributes, page 32-17
- Managing Categories, page 32-18
- Setting Categories for Multiple Recordings, page 32-19
- Recording Meetings, page 32-20
- Stopping Recordings in Progress, page 32-20
- Deleting Recordings, page 32-21

Viewing Recording Information

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

Note 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 Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select 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, select the column according to which you want to sort.

Step 5 To search for a specific recording by an attribute:

- Meeting ID—Select the **Meeting ID** column, enter the meeting ID in the Search field, and then select the **Search** button.
- Meeting Name—Select any column except the Meeting ID and Owner columns, enter the meeting name in the Search field, and then select the **Search** button.

Step 6 To display additional information for a specific recording, select the **Information** icon. The Meeting Information window opens.

Editing Recording Attributes

You can assign either an owner or an access PIN for recording protection. The access PIN is optional and is used for watching a recording. In the list of recorded meetings, those protected by an access PIN are marked by a key icon.

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 Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Recordings** tab.

Step 3 Select the **Manage Recording** button for the required recording in the list.

The Edit Recording window is displayed.

Step 4 To modify the recording name and description, enter new text in relevant fields.

Step 5 If necessary, select the check box to make the recording public.

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 select 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 Select **OK**.

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 Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Categories** tab.

Step 3 To create a new category:

a. In the Create a new category field, enter the name.

b. Select **Create**.

The new category appears in the list.

Step 4 To edit an existing category:

a. Select the **Edit** icon.

b. Enter the new name for the category.

c. Select **OK**.

Step 5 To delete an existing category:

a. Select the **Delete** icon.

b. Select **Yes**.

Setting Categories for Multiple Recordings

You can set categories for multiple recordings at one time.

Before You Begin

Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Recordings** tab.

Step 3 In the recording list, select check boxes for required recordings.

Step 4 Select **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, select the check box for this category.

b. Select **Assign**.

Step 6 To remove a category, which is currently assigned to selected recordings:

a. In the right pane, select the check box for this category.

b. Select **Remove**.

Recording Meetings

You can record meetings using the Desktop Administration web user interface.

Before You Begin

- Verify that you have the ID of a meeting you wish to record.
- Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Recordings** tab.

Step 3 In the Start recording meeting ID field, enter ID.

Step 4 Select **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. Enter the owner PIN.

b. Enter the owner PIN in the Confirm field.

Step 8 To set the meeting PIN:

a. Enter the access PIN.

b. Enter the access PIN in the Confirm field.

Step 9 Select **Start Recording**.

The meeting appears in the list, and its duration is indicated as “In Progress”.

Stopping Recordings in Progress

You can stop any recording which 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 Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar

Step 2 Select the **Recordings** tab.

Step 3 In the recording list, select the check box for recordings you wish to stop.

Step 4 Select **Stop**.

Step 5 Select **Yes** in the confirmation message.

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 Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Recordings** tab.

Step 3 In the recording list, select the check box for recordings you wish to delete.

Step 4 Select **Delete**.

Step 5 Select **Yes** in the confirmation message.

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 servers 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, 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 32-2 compares using single Desktop Server to using multiple Cisco Unified Videoconferencing Desktop Servers for streaming.

Table 32-2 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 Cisco Unified Videoconferencing Desktop Server to Manage Streaming, page 32-22
- Configuring an Alternate Desktop Server for Watching Webcasts, page 32-24

Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Streaming

You need to perform the procedure described in this section only if you enabled streaming during deployment configuration.

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.

You can enable and configure multicast streaming to allow unlimited number of simultaneous streaming connections. Multicast streaming in Desktop is performed without Streaming Server support. If the IP address of a client computer is not within the multicast IP address range you configure, this client will use a unicast streaming connection. During multicast configuration you also need to define the Time to Live value—the number of transmissions of a multicast packet that Desktop performs. Setting this value to 1 means that a multicast packet stays within a local network. The change in the multicast streaming configuration applies only to meetings created after the change takes place; the change does not effect meetings in progress.

By default the maximum number of ports used for streaming is 600. However, we recommend that you adjust the number of ports value to match the supported number of streaming ports based on the CPU and Memory system requirements.

Before You Begin

- Navigate to the Desktop Administration web user interface.
- Select Deployment in the sidebar and verify that streaming is enabled on the Servers page.

Procedure

Step 1 Select **Streaming** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 To configure standard definition recording, select a value from the Maximum Bit Rate list under Standard Definition.

Step 4 To configure high definition recording, perform the following:

a. Select the **High Definition** check box.

b. Select a value from the Maximum Bit Rate list under High Definition.

Step 5 If necessary, configure multicast settings:

a. Check the **Enable Multicast** option.

b. Enter the multicast IP address.

The valid multicast IP address is in the range of 224.0.0.1 and 239.255.255.255.

c. Enter the Time to Live value.

d. Define clients that will be able to watch multicasts by entering IP range in the fields and selecting the Arrow button.

Step 6 Enter a public address.

We recommend to use a public address that clients can resolve.

Step 7 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. at http://www.cisco.com/en/US/products/hw/video/ps1870/products_implementation_design_guides_list.html.

Step 8 Enter a value for the maximum number of ports you want to use for unicast streaming clients.

Step 9 Select **OK** or **Apply**.

Related Topics

- Configuring Settings for Single/Multiple-NIC Deployments, page 32-5

Configuring an Alternate Desktop Server for Watching Webcasts

For basic and advanced deployments where streaming is disabled, you can 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 Administration web user interface.
- Select Deployment in the sidebar and verify that streaming is disabled on the Servers page.

Procedure

Step 1 Select **Streaming** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 Select the Allow watching of webcasts from an alternate Desktop server check box.

Step 4 In the Server URL field, enter the URL of the alternate Desktop Server.

Step 5 Select **OK** or **Apply**.

How to Configure Messages and Invitations

- Configuring Meeting Access Messages, page 32-24
- Configuring Meeting Access Instructions, page 32-26
- How to Configure Dial String Rules, page 32-26

Configuring Meeting Access Messages

This section describes how to edit the Administrator and Dial Plan messages.

You can use the Administrative message appearing on the Cisco Unified Videoconferencing Desktop Server portal entry page to post important information such as: system status, scheduled shutdown, or configuration tips.

The Dial Plan message appears in the Invitation dialog box. You can use this message to provide users with dialing tips, for example, explain what prefixes they should use for gateways of different types.

These tags and attributes are supported in the administrator messages text editor:

-
- <img src=”http*”>
- <iframe src=”http*”></iframe>
-
- <u></u>
-
-

-
</br>
-
-
-
-
-

You must fix a width and height of the <iframe> tag according to the style sheet of the corresponding page. For example, for the portal entry page the style sheet looks like this:

```
<style>
        .motd iframe
        {
                width: 100%;
                height: 150px;
        }
</style>
```

The administrator message text editor replaces single '&' characters with '&amp'; it also replaces '<' and '>' of invalid tags with '&It' and '&gt' respectively.

Before You Begin

Navigate to the Desktop Administration web user interface.

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Messages** tab.

Step 3 Select the **Administrative Message** check box.

Step 4 Modify the text of the entry page message as required.

Step 5 Select the **Invitation Dial Plan Assistance** check box.

Step 6 Modify the text of the invitation message as required.

Step 7 Select **OK** or **Apply**.

Configuring Meeting Access Instructions

While modifying the contents of e-mail invitations, you can define these links:

- Meeting URL—For connecting to a Desktop meeting.
- Portal URL—For watching a webcast or a recorded meeting.

If you have multiple Desktop Servers and want participants to know about them, insert link information for each of them into each Desktop e-mail configuration.

For example, if you have one Desktop in Europe, one in Asia, and another in the US, you could place the following information in your e-mail:

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Invitations** tab.

The default instructions for accessing the meeting from a desktop, phone or video conferencing device appear in the screen.

Step 3 In the Desktop Access section:

- Select **Meeting URL** to insert a link to the meeting.
- Select **Portal URL** to insert a link to the Desktop portal entry page.
- Select **Client Installation** to insert a link used to ensure that the Desktop Client is installed and up-to-date.

Note The automatically inserted server address is the Desktop Server Fully Qualified Domain Name specified during installation.

Step 4 In the Phone Access area, select **E.164** to insert the required E.164 alias.

Step 5 In the Video-Conference Device Access area, select **E.164** to insert the required E.164 alias.

Step 6 Select **OK** or **Apply**.

How to Configure Dial String Rules

- About Dial String Manipulation, page 32-27
- Adding Dial String Rule, page 32-31
- Editing Dial String Rule, page 32-32
- Delete Dial String Rule, page 32-33

About Dial String Manipulation

In Cisco Unified Videoconferencing Solution deployments dial string manipulation is necessary in these scenarios:

- When a call must be routed to local H.323 PSTN or ISDN gateways. In this case Desktop needs to detect phone numbers and modify the prefix to add routing information.
- When there is a SIP PBX either in enterprise premises or a remote location which Desktop must use to dial phone numbers. In this case Desktop needs to detect phone numbers in the directory and append the SIP URL to forward it to the right gateway.

There are several methods Desktop uses to perform dial string manipulation:

- string normalization
- prefix or suffix substitution
- prefix or suffix addition
- prefix stripping

You must configure rules according to which Desktop manipulates dial strings.

Notice that during substitution this logic is used:

- Desktop performs dial string normalization prior to applying other string manipulation rules. During normalization any non-numeric characters except "+" are removed. See Table 32-3.

Table 32-3 Examples of Dial String Normalization

Initial String	Normalized String
1 (603) 407-5956	1603407-5956
+1 (603) 407-5956	+16034075956
+972 (54) 776-9462	+972547769462

- There is a certain order in which Desktop applies the rules. For example, it first applies more restrictive rules like rules that cause Desktop to match long strings combining specific and non-specific characters.
- If during the rule configuration you leave the replacement string blank, Desktop strips the prefix from the address. In order to keep the string, configure this string as the replacement string.

Related Topics

- Example of Dial String Manipulation for Deployments Including H.323 Gateway, page 32-27
- Example of Dial String Manipulation for Deployments Including SIP Gateway, page 32-30

Example of Dial String Manipulation for Deployments Including H.323 Gateway

What kind of manipulation is necessary?

- Change any phone number that starts with the New Hampshire area code +1603, 1603, or 603 and followed by exactly seven digits to the gatekeeper/gateway prefix of 1370 followed by the seven digits for the local phone extension.
- Route any other long distance number indicated by +1 and followed by 10-digit phone number to the New Jersey gatekeeper/gateway by substituting 11701 for the +1 and keeping the 10 digits.

- Route the international Israel country prefix of +972 followed by any random number of digits to the 10700 Tel Aviv gateway.

Table 32-4 shows what rules are configured for the required dial string manipulation.

Table 32-4 Rule settings

Match Prefix	Replacement	Optional Suffix	Comments
+1603xxxxxxx	1370		603 routed to local call gateway
1603xxxxxxx	1370		603 routed to local call gateway
603xxxxxxx	1370		603 routed to local call gateway
+1xxxxxxxxxx	11701		All other long distance calls routed to other gateway.
+972	10700		International calls to Israel go to the Tel Aviv local call getaway

When Desktop applies these rule, it results in this dial string manipulation:

Table 32-5 Dial String Manipulation Result

Normalized String	Substituted String
16034725956	13704725956
+16034725956	13704725956
+15081234567	117015081234567
+972547769462	10700547769462

Table 32-6 provides an example of the H.323 gateway dial plan

where

- 13—Prefix for the New Hampshire gatekeeper/gateway
- 11—Prefix for the New Jersey gatekeeper/gateway
- 10—Prefix for the Tel Aviv gatekeeper/gateway
- 15—Prefix for the Hong King gatekeeper/gateway
- 70—Prefix for audio gateway

Table 32-6 Example of H.323 Gateway Dial Plan

Match prefix	Replacement	Optional Suffix	Comments
Fixed string length examples			
+91508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
+1508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
1508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
91603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
+1603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
1603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
91xxxxxxxxx	11701		Use New Jersey gateway for long distance calls
+1xxxxxxxxx	11701		Use New Jersey gateway for long distance calls
1xxxxxxxxx	11701		Use New Jersey gateway for long distance calls
Variable string examples			
011972	10700		Use Tel Aviv gateway (needs extra 0)
+972	10700		Use Tel Aviv gateway (needs extra 0)
011852	1570		Use Hong Kong gateway for local calls (without extra 0)
+852	1570		Use Hong Kong gateway for local calls (without extra 0)
011	1170011		Use New Jersey for other international calls

Example of Dial String Manipulation for Deployments Including SIP Gateway

What kind of manipulation is necessary?

- Route any phone number that starts with the New Hampshire area code +1603, 1603 or 603 and then followed by exactly seven digits to New Hampshire SIP gateway by adding the "@sipgateway.nh.com" suffix to the remaining seven digits.
- Route any other long distance number indicated by +1 and followed by 10-digit phone number to the New Jersey SIP gateway by adding the "@sipgateway.nj.com" suffix to the 10 digits.
- Route the international Israel country prefix of +972 followed by any random number of digits to the 10700 Tel Aviv gateway by replacing the prefix with 0 and adding the "@sipgateway.tlv.com" suffix.

Table 32-7 shows what rules are configured for the required dial string manipulation.

Table 32-7 Rule settings

Match Prefix	Replacement	Optional Suffix	Comments
+1603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
1603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
+1xxxxxxxxxx	1	@sipgateway.nj.com	All other long distance calls routed to the New Jersey gateway.
+972	0	@sipgateway.tlv.com	International calls to Israel go to the Tel Aviv international getaway

When Desktop applies these rule, it results in this dial string manipulation:

Table 32-8 Dial String Manipulation Result

Normalized String	Substituted String
16034725956	4725956@@sipgateway.nh.com
+16034725956	4725956@sipgateway.nh.com
+15081234567	15081234567@sipgateway.nj.com
+972547769462	0547769462@sipgateway.tlv.com

Table 32-9 provides an example of the SIP gateway dial plan

where

- 13—Prefix for the New Hampshire gatekeeper/gateway
- 11—Prefix for the New Jersey gatekeeper/gateway
- 10—Prefix for the Tel Aviv gatekeeper/gateway
- 15—Prefix for the Hong King gatekeeper/gateway
- 70—Prefix for audio gateway

Table 32-9 Example of SIP Gateway Dial Plan

Match prefix	Replacement	Optional Suffix	Comments
Fixed string length examples			
+91508xxxxxxx	1508	@sipgateway.nh.com	Use New Hampshire gateway for MA calls
+1508xxxxxxx	1508	@sipgateway.nh.com	Use New Hampshire gateway for MA calls
1508xxxxxxx	1508	@sipgateway.nh.com	Use New Hampshire gateway for MA calls
508xxxxxxx	1508	@sipgateway.nh.com	Use New Hampshire gateway for MA calls
91603xxxxxxx		@sipgateway.nh.com	Use New Hampshire gateway for New Hampshire calls
+1603xxxxxxx		@sipgateway.nh.com	Use New Hampshire gateway for New Hampshire calls
1603xxxxxxx		@sipgateway.nh.com	Use New Hampshire gateway for New Hampshire calls
603xxxxxxx		@sipgateway.nh.com	Use New Hampshire gateway for New Hampshire calls
91xxxxxxxxx	1	@sipgateway.nj.com	Use New Jersey gateway for long distance calls
+1xxxxxxxxx	1	@sipgateway.nj.com	Use New Jersey gateway for long distance calls
1xxxxxxxxx	1	@sipgateway.nj.com	Use New Jersey gateway for long distance calls
Variable string examples			
011972	0	@sipgw.tlv.com	Use Tel Aviv gateway (needs extra 0)
+972	0	@sipgw.tlv.com	Use Tel Aviv gateway (needs extra 0)
011852		@sipgw.hk.com	Use Hong Kong gateway for local calls (without extra 0)
+852		@sipgw.hk.com	Use Hong Kong gateway for local calls (without extra 0)
011	011	@sipgw.nj.com	Use New Jersey for other international calls

Adding Dial String Rule

The prefix matches the beginning of a dialed string. To correctly represent the number of digits in a string, use the “x” character as a wildcard to match any digit. For example, “603” matches any dial string that begins with “603”, while “603xxxxxxx matches only a dial string beginning with “603” and consisting of ten digits. You cannot use any other characters, such as a space, a dash or a parenthesis.

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Dial Strings** tab.

Step 3 Select **Add**.

The Add New Entry window opens.

Step 4 Enter the prefix in the Match Prefix field.

Step 5 Select one of these options:

- **Replace**—A string matching the prefix is replaced with another string.
- **Remove—A string matching the prefix is stripped from the dial string.**
- **Leave As Is**—A string matching the prefix is left as is.

Step 6 If you selected the Replace option, enter the replacing prefix in the field.

Step 7 To add a suffix, select the **Append Suffix** check box, and then enter the suffix in the field.

Step 8 Enter a comment.

Step 9 Select **OK**.

Step 10 To test the new dial string rule:

a. Enter a string in the Test a Dial String field.

b. Select the check box for the rule you want to apply to this string.

c. Select **Test**.

The Dial String Test window appears displaying the dial string after the rule is applied.

Editing Dial String Rule

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Dial Strings** tab.

Step 3 Select the **Edit** icon.

The Edit Entry window opens.

Step 4 Edit the dial string as required.

Step 5 Select **OK**.

Related Topics

- Adding Dial String Rule, page 32-31

Delete Dial String Rule

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Dial Strings** tab.

Step 3 Locate the rule you need to edit and select the check box next to it.

Step 4 Select **Delete**.

Step 5 Select **OK** in the confirmation message.

Configuring Sametime Settings

For Desktop deployments working with Lotus Sametime Web Conferencing plug-in, you must configure Sametime-related administrative settings. For information about configuring Sametime Settings, refer to the *Integration Note for Installing and Configuring the* Cisco Unified Videoconferencing Connector *for IBM Lotus Sametime*.

Configuring a Local Administrator Account

You can define a user and password for a local administrator to access Desktop Administration web user interface. The local administrator cannot sign in to Desktop user portal using credentials defined during this procedure.

Procedure

Step 1 Select **Directory and Authentication** on the sidebar.

The Settings tab is displayed.

Step 2 Enter credentials in the Local Administrator area.

Step 3 Select **OK** or **Apply**.

Configuring Local Directory of Terminals

For basic deployments you can configure a local directory of terminals.

Procedure

Step 1 Select **Directory and Invitations** in the sidebar.

The Settings tab is displayed.

Step 2 Select the **Directory** tab.

Step 3 To add a terminal:

a. Select **Add**.

b. Enter a display name and an IP address.

c. Select **OK**.

Step 4 To edit an endpoint settings:

a. Select the **Edit** icon for the endpoint whose settings you wish to edit.

b. Modify the settings.

c. Select **OK**.

Step 5 To delete a single or multiple endpoints from the local directory:

a. In the endpoint list, select the check box for endpoints you wish to delete.

b. Select **Delete**.

Increasing Cisco Unified Videoconferencing Desktop Server Memory

The default memory for Cisco Unified Videoconferencing Desktop Server is 256M. In basic deployments where Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager are installed on the same server you need to increase the default Cisco Unified Videoconferencing Desktop Server memory to allow large conferences hosting 100 or more participants.We recommend that you increase the Cisco Unified Videoconferencing Desktop Server memory to 650M.

Procedure

Step 1 Navigate to the registry: HKLM\Software\Click to Meet\Conference server\7.11.000.

Step 2 Add a new DWORD key: VirtualHeapSize.

Step 3 Set the VirtualHeapSize value to the desired amount of pre-allocated memory.

Generating a PKCS12 Certificate Using Microsoft Certificate Service

Procedure

Step 1 Connect to the Certificate Authority Server at this link: http://<serverName>/certsrv.

Step 2 On the Welcome page, select **Request a Certificate**.

Step 3 On the Request a Certificate page, select **advanced certificate request**.

Step 4 On the Advanced Certificate Request page, **Create and submit a request to this CA**.

Step 5 On the Advanced Certificate Request page, fill in the following information:

a. Certificate Template: Duplicate Computer (or pick) (If your Certificate Authority server is running Microsoft Windows Server 2003 - Enterprise Edition).

-or-

Type of Certificate Needed=Server Authentication Certificate (If your Certificate Authority server is running Microsoft WIndows Server 2003 R2 - Enterprise Edition)

b. Key options:

- CSP: Microsoft RSA SChannel Cryptographic Provider
- Key Usage: Exchange
- Key Size: 1024
- Automatic key container name
- Check Mark keys as exportable

Step 6 Select **Submit**.

Step 7 If a Potential Scripting Violation warning appears, select **Yes** to request the Certificate.

Step 8 After the certificate has been issued by the certificate authority server, connect to it using this link: http://<serverName>/certsrv.

Step 9 View the status of a pending certificate request. Then select the certificate request you want to view by selecting on the CSR.

Step 10 Select the **Install this certificate link**.

Step 11 If a Potential Scripting Violation warning appears, select **Yes** to request the certificate.

Step 12 Verify that you receive a message stating that the certificate has been successfully installed.

Related Topics

- Verifying That the Certificate Installed, page 32-36
- Exporting the Certificate, page 32-36
- Adding the Certificate to Cisco Unified Videoconferencing Desktop Configuration Tool and Enabling HTPPS, page 32-37

Verifying That the Certificate Installed

Procedure

Step 1 Select **Start > Run**.

Step 2 Type mmc and press Enter.

Step 3 From the File menu select **Add/Remove Snap-in**.

Step 4 Select **Add**.

Step 5 Select **Certificates and Add**.

Step 6 Select **My user account** and **Finish**.

Step 7 Select **Certificates** and **Add**.

Step 8 Select **Computer Account** and **Next**.

Step 9 Select **Local computer: (the computer this console is running on)** and **Finish**.

Step 10 Select **Close** and **OK**.

Step 11 Verify that the MCM Console shows two certificate stores.

The first should be Certificates - Current User and the second should be Certificates (Local Computer).

Step 12 Verify that under Certificates - Current User 'Personal' Certificates that you installed is listed. (The certificate is not installed under local computer).

Exporting the Certificate

Procedure

Step 1 Right-click the **Certificate** and select **All Tasks > Export**.

Step 2 Select **Next**.

Step 3 Select **Yes**, export the private key.

Step 4 Select **Personal Information Exchange - PKCS#12 (.PFK)**.

Step 5 Also select **Include all certificates in the certification path if possible** option and **Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)**, then select **Next**.

Step 6 Enter a password.

Step 7 Re-enter the password to confirm it.

Step 8 Select **Browse** and navigate to the location where you would like to save the certificate and enter a name and save. Verify that it is saved as a .pfx file.

Step 9 Verify the information and select **Finish**.

Adding the Certificate to Cisco Unified Videoconferencing Desktop Configuration Tool and Enabling HTPPS

Procedure

Step 1 On the Cisco Unified Videoconferencing Desktop Server, select **Start > Cisco Unified Videoconferencing Desktop Server > Config Tool**.

Step 2 Select **HTTPS**.

Step 3 Select **Add certificate**.

Step 4 Select the **Configure Certificate via file name** option.

Step 5 Under “Certificate File Name”, browse to the .pfx file created in Step 8 of the Exporting the Certificate, page 32-36.

Step 6 Enter the password as entered in Step 6 of the Exporting the Certificate, page 32-36.

Step 7 Select **Apply**, then **OK**.

Step 8 Check **Enable HTTPS**.

Step 9 Select **Apply**.

Step 10 Select **Restart Services**.

Step 11 You may need to reboot the Cisco Unified Videoconferencing Desktop Server.

Step 12 From another machine, open https://<cuvd-server>/cuvm/admin.

Note When you upgrade or re-install Cisco Unified Videoconferencing Desktop, the HTTPS settings are not preserved and are reset to HTTP; the certificate location is set to the default self-signed certificate. In this case, you need to upload a new certificate and enable HTTPS again for secure connection.

CHAPTER 33

How to Customize The User Interface

Revised: January 27, 2010/OL-21622-01

Customers can change logos and strings which contain the default Cisco or Desktop branding to brand the user interface with their own logos and strings. You can change images and strings using the Desktop Branding application.

- Replacing Images, page 33-1
- Modifying Strings, page 33-2
- Saving or Restoring Branding- Related Changes, page 33-3
- Restoring Default Images and Strings, page 33-4

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 may 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 which you can restore at any time.

Procedure

Step 1 Select **Start**.

Step 2 Choose **Programs > Desktop > Branding Application**.

The branding application starts.

Step 3 Select the **Images** tab.

The images that can be replaced are displayed together with the recommended size and a brief description of each image.

Note 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 Select **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 in order to verify that the image appears correctly.

Step 7 Select Install Image to use the replacement image.This image is replaced.

Note 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, select 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 Select **Start**.

Step 2 Choose **Programs > Cisco Unified Videoconferencing Desktop > Branding Application**.

Step 3 Select the **Strings** tab.

The strings that can be replaced are displayed along with the 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 Select 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 Select **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 affect.

Step 8 To restore default strings:

a. Select **Restore All Default Strings**.

b. Select **Apply**.

c. Restart the “Desktop - Apache Tomcat” service for the changes to take affect.

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 Select **Start**.

Step 2 Choose **Programs > Cisco Unified Videoconferencing 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. Select **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. Select **Import**.

Step 5 Restart the “Desktop - Apache Tomcat” service for the changes to take affect.

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 Select **Start**.

Step 2 Choose **Programs > Cisco Unified Videoconferencing 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.

CHAPTER 34

How to Backup and Restore Recordings and Settings

Revised: January 27, 2010/OL-21622-01

You can backup and restore recordings as well as these Desktop settings:

- dial string rules
- administrative messages
- invitation messages
- recordings and recording attributes
- categories
- local database (used in basic deployments)

- Backing up Recordings, page 34-1
- Backing up Settings, page 34-2
- Restoring Recordings, page 34-3
- Restoring Settings, page 34-3

Backing up Recordings

Desktop saves actual recordings and recording attributes in different folders. In order to restore a recording you need to backup and restore both folders.

Perform the backup procedure described in this section on the Desktop Recording Server. During the backup procedure you copy the xml file which 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*>*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.

Note By default, the recordings are stored in the <*installdir*>*Movies**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. Select **Status** in the sidebar.

c. Select 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

Backing up Settings

Perform the backup procedure described in this section on the Desktop Recording Server. During the backup procedure you copy the xml files which contain these settings:

- dial string rules
- administrative message
- invitation message
- local database

Procedure

Step 1 Navigate to the following directory: <*installdir*>*data*.

Step 2 Copy the relevant files into a location outside the installation directory:

- *motd.html*—for administrator message
- *dialplanhelp.html*—for invitation message
- *memebers.xml*—for local database
- *dial_string_manipulators.xml*—for dial string rules

Restoring Recordings

Desktop saves actual recordings and recording attributes in different folders. In order to restore a recording you need to restore both folders.

Procedure

Step 1 Navigate to the following directory: *<installdir>\data*.

Step 2 Replace *recorder_categories.xml* file with the backup file.

Step 3 Replace the recordings folder with the backup folder.

Note Replacing the recordings folder with the backup folder erases any categories that are currently defined in Desktop.

Step 4 Navigate to the folder in which recordings are stored.

Note By default, the recordings are stored in the *<installdir>\Movies\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. Select **Status** in the sidebar.

c. Select the **Recording Status** tab.

The Recordings Folder information is displayed on the tab.

Step 6 Replace that folder with the backup folder.

Restoring Settings

Procedure

Step 1 Stop the service "Desktop - Apache Tomcat".

Step 2 Navigate to the following directory: *<installdir>\data*.

Step 3 Replace the relevant file with the backup file:

- *motd.html*—for administrator message
- *dialplanhelp.html*—for invitation message
- *memebers.xml*—for local database
- *dial_string_manipulators.xml*—for dial string rules

Step 4 Start the service "Desktop - Apache Tomcat".

INDEX

A

Alarms view 21-4
Auto-Detect 21-3

B

bandwidth 16-5
Bandwidth Rules 26-13
billing 16-7

C

Centralized Log Management 21-4
columns
  sorting 16-2
Conferences and Calls view
  Calls tab 30-1
  Conferences tab 30-3
Configuration Tool
  e-mail server settings 17-4
  MCU command delay 17-6
  meeting settings 17-8
  passwords 17-6
Configuring
  Terminal managers 21-4
Configuring Protocols 25-1

D

Default Dialing Mode 16-6
delay 16-5

E

Element configuration 21-3
Element Managers
  configuration 21-4
endpoint
  unresponsive to connection request 17-4

G

Gatekeeper
  configuration 21-3
  local zones 26-12
  Prefixes 26-13
Gateway
  configuration 21-3

H

host 16-7

I

IP Topology tab 2-3
  Bandwidth 2-3
  Distance 2-3
ISDN
  cost of call 2-3

M

MCU
  command delay 17-6

configuration 21-3
local 16-5
MCU access 30-5

N

Name Display Format 16-2
Network Manager
overview 21-1
Network Status 21-2
Network Tree view 22-1
Elements tab 23-2
Network Views 21-5

R

Registering MPs 25-1
reports
generating 12-4, 13-5
Requirements
system 21-1

S

Services
MCU 25-2
Settings view
Element Logs tab 31-2

V

Viewing conferences 21-2
Viewing events 21-4
Views
Network Tree 22-1