Cisco Unified Serviceability Administration Guide

Release 8.5(1)

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

Text Part Number: OL-22518-01

Cisco Unified Serviceability Administration Guide

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide, and provides information on how to obtain related documentation.

Note This document may not represent the latest Cisco product information that is available. You can obtain the most current documentation by accessing Cisco product documentation page at this URL:

For Cisco Unified Communications Manager:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

For Cisco Unified Communications Manager Business Edition 5000:
http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

For Cisco Unity Connection:
http://www.cisco.com/en/US/products/ps6509/tsd_products_support_series_home.html

The preface covers these topics:

Purpose

The *Cisco Unified Serviceability Administration Guide* provides descriptions and procedures for configuring alarms, traces, SNMP, and so on, through Cisco Unified Serviceability for Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, and Cisco Unity Connection. Use this guide with the documentation for your configuration:

Cisco Unified Communications Manager	*Cisco Unified Real-Time Monitoring Tool Administration Guide*, *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*, and *Cisco Unified Communications Manager Call Detail Records Administration Guide.*
Cisco Unified Communications Manager Business Edition 5000	*Cisco Unified Real-Time Monitoring Tool Administration Guide*, *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*, *Cisco Unified Communications Manager Call Detail Records Administration Guide,* and *Administration Guide for Cisco Unity Connection Serviceability*
Cisco Unity Connection	*Administration Guide for Cisco Unity Connection Serviceability*, and *Cisco Unified Real-Time Monitoring Tool Administration Guide.*

These documents provide the following information:

- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*—This document describes how to configure and use Cisco Unified Communications Manager CDR Analysis and Reporting (CAR), a tool that is used to create user, system, device, and billing reports.
- *Cisco Unified Communications Manager Call Detail Records Administration Guide*—This document includes Call Detail Record (CDR) definitions.
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*—This document describes how to use RTMT, a tool that allows you to monitor many aspects of the system (critical services, alerts, performance counters, and so on).
- *Administration Guide for Cisco Unity Connection Serviceability*—This document provides descriptions and procedures for using alarms, traces, clusters, reports, and so on, through Cisco Unity Connection Serviceability.

Tip For Cisco Unity Connection, you must perform serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability; for example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

Cisco Unified Serviceability supports the functionality that is described in the *Cisco Unified Serviceability Administration Guide*; for tasks that are specific to Cisco Unity Connection Serviceability, refer to the *Administration Guide for Cisco Unity Connection Serviceability Release 8.x*.

Audience

The *Cisco Unified Serviceability Administration Guide* assists administrators that configure, troubleshoot, and support Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, or Cisco Unity Connection. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows the organization for this guide:

Table 1 Organization of Cisco Unified Serviceability Administration Guide

Part	Description
Part 1	"Understanding Cisco Unified Serviceability" Provides an overview of Cisco Unified Serviceability, including browser support and information on how to access and use the GUI.
Part 2	"Alarms" • Provides an overview of Cisco Unified Serviceability alarms and alarm definitions. • Provides procedures for configuring alarms in Cisco Unified Serviceability; provides procedures for searching and editing Cisco Unified Serviceability alarm definitions.
Part 3	"Trace" • Provides an overview for configuring trace parameters in Cisco Unified Serviceability; also provides an overview of trace collection in the Cisco Unified Real-Time Monitoring Tool. • Provides procedures for configuring trace parameters for Cisco Unified Serviceability network and feature services; provides procedures for configuring the troubleshooting trace settings for services in Cisco Unified Serviceability.
Part 4	"Tools" • Provides a description of each network and feature service that displays in Cisco Unified Serviceability; provides procedures and recommendations for activating, deactivating, starting, and stopping Cisco Unified Serviceability feature and network services. • *Unified CM and Unified CM BE 5000 only:* Provides information on using the CDR Management Configuration window to set the amount of disk space to allocate call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure billing application server destinations for CDRs. • Provides an overview on the reports that are generated by the Cisco Serviceability Reporter service; provides procedures for viewing reports that are generated by the Cisco Serviceability Reporter service.
Part 5	"Simple Network Management Protocol" • Provides an overview of Cisco Unified Communications Manager support of SNMP versions 1, 2c, and 3. Administrators use SNMP to troubleshoot and to perform diagnostics and network management tasks. • Provides procedures for configuring SNMP versions 1, 2c, and 3. • Provides procedures for configuring the system contact and system location objects for the MIB-II system group. • Provides procedures for configuring SNMP trap and inform parameters. • Provides troubleshooting tips for SNMP services and MIBs.

Related Documentation

For additional documentation, refer to the documentation guide at the URL for your configuration:

Cisco Unified Communications Manager	*Cisco Unified Communications Manager Documentation Guide*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
Cisco Unified Communications Manager Business Edition 5000	*Cisco Unified Communications Manager Business Edition 5000 Documentation Guide*: http://www.cisco.com/en/US/products/ps7273/products_documentation_roadmaps_list.html
Cisco Unity Connection	*Documentation Guide for Cisco Unity Connection*: http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
——→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Related Documentation

You can browse the related documentation for Cisco Unified Communications Manager by clicking one of the following links:

- All technical documentation for Cisco Unified Communications Manager here.
- The *Cisco Unified Communications Manager Documentation Guide* for your release here.

You can also use the Documentation Custom Search utility to search through the documentation for this product.

To browse the documentation for another Cisco product, search or navigate from here.

Cisco Unified Communications Manager Documentation Guide

The *Cisco Unified Communications Manager Documentation Guide* describes the various documents that comprise the Cisco Unified Communications Manager documentation set. The guide contains hyperlinks that link directly to these documents.

PART 1

Cisco Unified Serviceability

CHAPTER 1

Understanding Cisco Unified Serviceability

Note This document uses the following abbreviations to identify administration differences for these Cisco products:
Unified CM refers to Cisco Unified Communications Manager
Unified CM BE 5000 refers to Cisco Unified Communications Manager Business Edition 5000
Connection refers to Cisco Unity Connection

This chapter contains information on the following topics:

Cisco Unified Serviceability Overview

Cisco Unified Serviceability, a web-based troubleshooting tool, provides the following functionality:

- Saves alarms and events for troubleshooting and provides alarm message definitions.
- Saves trace information to various log files for troubleshooting.
- Monitors real-time behavior of components through the Cisco Unified Real-Time Monitoring Tool (RTMT).
- *Unified CM and Unified CM BE 5000 only:* Generates Cisco Unified Communications Manager reports for Quality of Service, traffic, and billing information through Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).
- Provides audit capability by logging any configuration changes to the system by a user or as a result of the user action. This functionality supports the Information Assurance feature of Cisco Unified Communications Manager and Cisco Unity Connection.
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.

- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Cisco Unified Communications Manager and Cisco Unity Connection to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server.
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.

Tip Cisco RIS Data Collector provides Process and Thread statistic counters in the Cisco Unified Real-Time Monitoring Tool. To configure the maximum number of processes and threads that are allowed, so Cisco RIS Data Collector can provide these associated counters, access the Maximum Number of Threads and Process service parameter for the Cisco RIS Data Collector service in the administration interface for your configuration.

Unified CM and Unified CM BE 5000: For information on configuring service parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.

Connection: For information on configuring service parameters, refer to the *System Administration Guide for Cisco Unity Connection*.

Tip *Unified CM BE 5000 and Connection only*: For Cisco Unity Connection, you must perform serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability; for example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

Cisco Unified Serviceability supports the functionality that is described in the *Cisco Unified Serviceability Administration Guide*; for tasks that are specific to Cisco Unity Connection Serviceability, refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Reporting and Monitoring Tools

Cisco Unified Serviceability provides the following reporting tools:

- Cisco Unified Real-Time Monitoring Tool (RTMT)—Monitors real-time behavior of components through RTMT; creates daily reports that you can access through the Serviceability Reports Archive. For more information, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
- Serviceability Reports Archive—Archives reports that the Cisco Serviceability Reporter service generates.
- *Unified CM and Unified CM BE 5000 only*: Cisco Unified Communications Manager CDR Analysis and Reporting (CAR)—Generates Cisco Unified Communications Manager reports for Quality of Service, traffic, and billing information through Cisco Unified Communications Manager CDR Analysis and Reporting (CAR). For more information, refer to the *CDR Analysis and Reporting Administration Guide*.
- *Unified CM and Unified CM BE 5000 only*: Cisco Unified Communications Manager Dialed Number Analyzer—Allows you to test and diagnose a deployed Cisco Unified Communications Manager dial plan configuration, analyze the test results, and use the results to tune the dial plan. For more information on how to access and use Dialed Number Analyzer, refer to the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

- *Unified CM and Unified CM BE 5000 only*: Cisco Unified Reporting Web Application—Allows you to inspect or troubleshoot data for a standalone server or a cluster. This application, which is separate from Cisco Unified Serviceability, combines data by category from all accessible Cisco Unified Communications Manager servers in a cluster into one output view. Some reports run health checks to identify conditions that could impact server or cluster operations. If you are an authorized user, you access Cisco Unified Reporting in the main navigation menu in Cisco Unified Communications Manager Administration or with the **File > Cisco Unified Reporting** link on the RTMT menu. Refer to the C*isco Unified Reporting Administration Guide* for more information

Note On Cisco Unified Communications Manager Business Edition 5000 servers, the Cisco Unified Reporting application captures data for Cisco Unified Communications Manager only. Due to size constraints, the application does not capture data for Cisco Unity Connection. On these servers, you can use this tool to gather important information about your Cisco Unified Communications Manager installation.

Remote Serviceability Tools

Note The content in this section does not apply to Cisco Unity Connection.

To supplement the management and administration of the Cisco Unified Communications Manager system, you can use remote serviceability tools. Using these tools, you can gather system and debug information for diagnostic help or remote troubleshooting. The tools can process and report on a collection of local or remote Cisco Unified Communications Manager configuration information. With customer permission, technical support engineers log on to a Cisco Unified Communications Manager server and get a desktop or shell that allows them to perform any function that could be done from a local logon session.

Cisco Unified Communications Manager supports the following capabilities for remote serviceability:

- Simple Network Management Protocol (SNMP)—Provides remote management for managed devices such as Cisco Unified Communications Manager
- Show Command Line Interface—Displays Cisco Unified Communications Manager system data.
- CiscoWorks Lan Management Solution—Purchased separately from Cisco Unified Communications Manager, supports maintenance of Cisco networks and devices. The following features, which serve as examples only, show how you can use CiscoWorks Lan Management Solution to manage Cisco Unified Communications Manager operations:

  Path Analysis defines Cisco Unified Communications Manager system paths in the form of maps, trace logs, or discovery tables. Path Analysis, which traces connectivity between two specified points in your network, requires that you enable CDR logging in Cisco Unified Communications Manager Administration.

  Syslog Analysis tools monitor and manage a wide range of events and error messages concurrently on each Cisco Unified Communications Manager server and other Cisco devices at your site.

  Cisco Discovery Protocol (CDP) enables discovery of Cisco Unified Communications Manager servers and management of those servers by CiscoWorks Lan Management Solution. After you use the CDP cache MIB of the direct neighboring device to discover Cisco Unified Communications Manager, you can use CiscoWorks Lan Management Solution to query other Cisco Unified Communications Manager-supported MIBs for provisions or statistics information about topology

services, user tracking, path analysis, and other network management services. When you use CiscoWorks Lan Management Solution, you must keep the CDP driver enabled at all times to discover Cisco Unified Communications Manager.

Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears on the initial Cisco Unified Serviceability window.

For more information and the procedure for uploading your customized log-on message, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Browser Support

Cisco supports these browsers with Cisco Unified Serviceability:

Table 1 Supported Browsers and Operating Systems

You can access Cisco Unified Communications Manager with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 7	Microsoft Windows XP SP3
Microsoft Internet Explorer 8	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2
Mozilla Firefox 3.x	• Microsoft Windows XP SP 3 • Microsoft Windows Vista SP • Apple MAC OS X
Safari 4.x	Apple MAC OS X

To access Cisco Unified Serviceability, you must browse to the application from a machine that runs the supported browser.

Note Cisco Unified Communications Manager CDR Analysis and Reporting, which is a Cisco Unified Serviceability tool, supports these same browsers. Cisco Unified Real-Time Monitoring Tool, a separate plug-in, supports a different set of browsers. Refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information.

Cisco Unified Serviceability uses HTTPS to establish secure connections.

Tip Cisco Unified Serviceability does not support the buttons in your browser. Do not use the browser controls, for example, the Back button, when you perform configuration tasks.

Where to Find More Information

Additional Cisco Documentation

- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Unified CM and Unified CM BE 5000 only: Cisco Unified Communications Manager Dialed Number Analyzer Guide*
- *Unified CM and Unified CM BE 5000 only:* CiscoWorks Lan Management Solution user documentation
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE 5000 and Connection only: Administration Guide for Cisco Unity Connection Serviceability*
- *Unified CM BE 5000 and Connection only: System Administration Guide for Cisco Unity Connection*
- *Cisco Unified Reporting Administration Guide*

CHAPTER 2

Using Cisco Unified Serviceability

This chapter comprises the following topics:

Accessing Cisco Unified Serviceability

You can access the Serviceability application

- by entering **https://<server name or IP address>:8443/ccmservice/** in a browser window and then entering a valid username and password.
- by choosing **Cisco Unified Serviceability** in the Navigation menu in the Cisco Unified Communications Manager Administration console.
- by choosing **Application > Serviceability Webpage** in the Real-Time Monitoring Tool (RTMT) menu and then entering a valid username and password
- by choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco Unity Connection.

Tip After you log in to Cisco Unified Serviceability, you can access all administrative applications that display in the Navigation menu, except for Cisco Unified OS Administration and Disaster Recovery System, without logging in again. The web pages that you can access within Cisco Unified Serviceability depend on your assigned roles and privileges. Cisco Unified OS Administration and Disaster Recovery System require a separate authentication procedure.

The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application.

Tip *Unified CM and Unified CM BE 5000 only:* Any user who has the "Standard CCM Admin Users" role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *Cisco Unified Communications Manager Administration Guide*.

Tip *Connection only:* Any user who has the System Administrator role or Technician role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

If you get a security alert that the site is not trusted, this indicates that the server certificate has not yet downloaded.

To access Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 In a supported browser, browse to the server where the Cisco Unified Serviceability service runs.

Tip In the supported browser, enter **https://<server name or IP address>:8443/ccmservice/**, where server name or IP address equals the server where the Cisco Unified Serviceability service runs and 8443 equals the port number for HTTPS.

If you enter http://<server name or IP address>:8080 in the browser, the system redirects you to use HTTP. HTTP uses the port number, 8080.

Step 2 If the system prompts you about certificates, see the "Installing the Server Certificate" section on page 2-2.

Step 3 Enter a valid username and password; click **Login**.

To clear the username and password, click **Reset**.

Additional Information

See the "Related Topics" section on page 2-8.

Installing the Server Certificate

This section contains information on the following topics:

Note For additional information about using HTTPS with Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Security Guide*.

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS, which ensures the identity of the server, supports applications, such as Cisco Unified Serviceability. HTTPS also ensures that the user login password transports securely via the web.

Note Due to the way IE 7 handles certificates, this browser displays an error status after you import the server certificate. This status persists if you reenter the URL or refresh or relaunch the browser and does not indicate an error. Refer to the "Installing the Certificate with Internet Explorer 7" section on page 2-4 for more information.

HTTPS Overview for Internet Explorer

On the first attempt to access Cisco Unified Serviceability, a Security Alert dialog box, which indicates that the server is not trusted because the server certificate does not exist in the trusted folder, displays. When the dialog box displays, perform one of the following tasks:

- By clicking **Yes**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application: that is, until you install the certificate in the trusted folder.
- By clicking **View Certificate > Install Certificate**, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking **No**, you cancel the action. No authentication occurs, and you cannot access the web application.

Note The system issues the certificate by using the hostname. If you attempt to access a web application by using the IP address, the Security Alert dialog box displays, even though you installed the certificate.

Additional Information

See the "Related Topics" section on page 2-8.

Installing the Certificate with Internet Explorer 6

Perform the following procedure to save the HTTPS certificate in the trusted folder.

Procedure

Step 1 Browse to the application on the Tomcat web server.

Step 2 When the Security Alert dialog box displays, click **View Certificate**. To verify certificate details, click the **Details** tab.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 When the Certificate Import Wizard displays, click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**; select it and click **OK**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

A Security Warning Box displays the certificate thumbprint for you.

Step 9 To install the certificate, click **Yes**.

A message states that the import was successful. Click **OK**.

Step 10 In the lower, right corner of the dialog box, click **OK**.

Step 11 To trust the certificate, so you do not receive the dialog box again, click **Yes**.

Tip You can verify the certificate was installed successfully by clicking the Certification Path tab in the Certificate pane.

Additional Information

See the "Related Topics" section on page 2-8.

Installing the Certificate with Internet Explorer 7

Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager or Cisco Unity Connection server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration or Cisco Unity Connection website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Java Runtime Environment (JRE) must be present to provide Java-related browser support for IE.

Be sure to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1 Browse to application on the Tomcat server by entering the hostname (server name) or IP address in the browser.

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**

The administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

The Certification Path tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

Step 5 Select the General tab in the Certificate window and click **Install Certificate**.

The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.

The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.

A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.

The Import Wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname or IP address or refresh or relaunch the browser.

Additional Information

See the "Related Topics" section on page 2-8.

Installing the Certificate with Netscape

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

If you trust the certificate for one session only, you must repeat this procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Note The address that you use to access Cisco Unified Communications Manager or Cisco Unity Connection must match the name on the certificate or a message will display by default. If you access the web application by using the IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

Perform the following procedure to save the certificate to the trusted folder:

Procedure

Step 1 Browse to the application, for example, Cisco Unified Serviceability, by using Netscape.

The certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Note If you choose Do not accept, the Cisco Unified Serviceability application does not display.

Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials and click **Close**.

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Additional Information

See the "Related Topics" section on page 2-8.

Using the Cisco Unified Serviceability Interface

In addition to performing troubleshooting and service-related tasks in Cisco Unified Serviceability, you can perform the following tasks:

- *Unified CM and Unified CM BE 5000 only*: To access Dialed Number Analyzer to test and diagnose a deployed Cisco Unified Communications Manager dial plan configuration, analyze the test results and use the results to tune the dial plan, activate the Cisco Dialed Number Analyzer service by choosing **Tools > Service Activation** and choosing **Tools > Dialed Number Analyzer**.

  The Cisco Dialed Number Analyzer Server service needs to be activated along with The Cisco Dialed Number Analyzer service by choosing **Tools > Service Activation** and choosing **Tools > Dialed Number Analyzer Server**. This service needs to be activated only on the node that is dedicated specifcally for the Cisco Dialed Number Analyzer service.

For more information on how to use the Dialed Number Analyzer, refer to the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

- *Unified CM and Unified CM BE 5000 only*: To access Cisco Unified Communications Manager CDR Analysis and Reporting from **Tools > CDR Analysis and Reporting**, perform the required procedures, as described in the *CDR Analysis and Reporting Administration Guide*.

Note You cannot access the Cisco Unified Communications Manager CDR Analysis and Reporting tool unless you are a member of the Cisco CAR Administrators user group. Refer to the "Configuring the CDR Analysis and Reporting Tool" chapter in the *CDR Analysis and Reporting Administration Guide* for information on how to become a member of the Cisco CAR Administrators user group.

- To display documentation for a single window, choose **Help > This Page** in Cisco Unified Serviceability.
- To display a list of documents that are available with this release (or to access the online help index), choose **Help > Contents** in Cisco Unified Serviceability.
- To verify the version of Cisco Unified Serviceability that runs on the server, choose **Help > About** or click the **About** link in the upper, right corner of the window.
- To go directly to the home page in Cisco Unified Serviceability from a configuration window, choose **Cisco Unified Serviceability** from the Navigation drop-down list box in the upper, right corner of the window.

Note In some scenarios, you cannot access the Cisco Unified Serviceability from Cisco Unified OS Administration. A "Loading, please wait" message displays indefinitely. If the redirect fails, log out from Cisco Unified OS Administration, select Cisco Unified Serviceability from the navigation menu, and log in to Cisco Unified Serviceability.

- To access other application GUIs, choose the appropriate application from the Navigation drop-down list box in the upper, right corner of the window; then, click **Go**.
- To log out of Cisco Unified Serviceability, click the **Logout** link in the upper, right corner of the Cisco Unified Serviceability window.
- In each Cisco Unified Serviceability configuration window, configuration icons display that correspond to the configuration buttons at the bottom of the window; for example, you can either click the Save icon or the Save button to complete the task.

Tip Cisco Unified Serviceability does not support the buttons in your browser. Do not use the browser buttons, for example, the Back button, when you perform configuration tasks.

Tip When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before indicating that the session has timed out and redirecting you to the login window. After you log in again, you may have to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Using Accessibility Features

Cisco Unified Serviceability provides functionality for users that allows them to access buttons on the window without using a mouse. These navigation shortcuts assist visually impaired or blind attendants to use the application.

Use Table 2-1 as a guide for navigating the interface by using keyboard shortcuts.

Table 2-1 Navigation Shortcuts for Cisco Unified Serviceability

Keystroke	Action
Alt	Moves focus to the browser menu bar.
Enter	Chooses the item with focus (menu option, button, and so on.)
Alt, arrow keys	Moves between browser menus.
Alt+underlined letter	Takes you to the menu; for example, Alt+A moves you to the Alarms menu.
Spacebar	Toggles control; for example, checks and unchecks a check box.
Tab	Moves focus to the next item in the tab order or to next control group.
Shift+Tab	Moves focus to the previous item or group in the tab order.
Arrow keys	Moves among controls within a group.
Home	Moves to the top of the window if more than one screenful of information exists. Also, moves to the beginning of a line of user-entered text.
End	Moves to the end of a line of user-entered text. Moves to the bottom of the window if more than one screenful of information exists.
Page Up	Scrolls up one screen.
Page Down	Scrolls down one screen.

Where to Find More Information

Related Topics

- Accessing Cisco Unified Serviceability, page 2-1
- Installing the Server Certificate, page 2-2
- Using the Cisco Unified Serviceability Interface, page 2-6
- Using Accessibility Features, page 2-8

Additional Cisco Documentation

- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Administration Guide*

- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager System Guide*
- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Security Guide*
- *Unified CM and Unified CM BE 5000 only*: CiscoWorks Lan Management Solution user documentation
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE 5000 and Connection only*: *Administration Guide for Cisco Unity Connection Serviceability*
- *Unified CM BE 5000 and Connection only*: *System Administration Guide for Cisco Unity Connection*

PART 2

Alarms

CHAPTER 3

Understanding Alarms

This chapter, which provides information on Cisco Unified Serviceability alarms, contains the following topics:

Understanding Alarms

Cisco Unified Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting. If you have clusters, this is even true for problems that are not on your local Cisco Unified Communications Manager or Cisco Unity Connection server.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDI trace log file, an SDL trace log file (for Cisco CallManager and CTIManager services only), or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition) (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

Note Cisco Unified Communications Manager supports SNMP traps in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 systems. Cisco Unity Connection SNMP does not support traps.

Tip For the Remote Syslog Server, do not specify a Cisco Unified Communications Manager server, which cannot accept syslog messages from other servers.

You use the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool (RTMT) to collect alarms that get sent to an SDI trace log file or SDL trace log file (for Cisco CallManager and CTIManager services only). You use the SysLog Viewer in RTMT to view alarm information that gets sent to the local syslog.

Alarm Configuration

You can configure alarms for services, such as Cisco Database Layer Monitor, in Cisco Unified Serviceability. Then, you configure the location(s), such as Syslog Viewer (local syslog), where you want the system to send the alarm information. With this option, you can

- Configure alarms for services on a particular server or on all servers *(Unified CM clusters only)*
- Configure different remote syslog servers for the configured service(s) or server(s)
- Configure different alarm event level settings for different destinations

Cisco Syslog Agent enterprise parameters in Cisco Unified Communications Manager Administration allow you to forward all alarms that meet or exceed the configured threshold to a remote syslog server with these two settings: remote syslog server name and syslog severity. To access these Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Cisco Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unified Communications Manager Business Edition 5000	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting > Enterprise Parameters**.

The alarms include system (OS/hardware platform), application (services), and security alarms. If you have a Cisco Unified Communications Manager Business Edition 5000 server, the system also forwards Cisco Unity Connection alarms.

Note If you configure both the Cisco Syslog Agent alarm enterprise parameters and application (service) alarms in Cisco Unified Serviceability, the system can send the same alarm to the remote syslog twice.

If local syslog is enabled for an application alarm, the system sends the alarm to the enterprise remote syslog server only when the alarm exceeds both the local syslog threshold and the enterprise threshold.

If remote syslog is also enabled in Cisco Unified Serviceability, the system forwards the alarm to the remote syslog server by using the application threshold that is configured in Cisco Unified Serviceability, which may result in the alarm getting sent to the remote syslog server twice.

The event level/severity settings provide a filtering mechanism for the alarms and messages that the system collects. This setting helps to prevent the Syslog and trace files from becoming overloaded. The system forwards only alarms and messages that exceed the configured threshold.

For more information about the severity levels attached to alarms and events, see the "Alarm Definitions" section on page 3-3.

Alarm Definitions

Used for reference, alarm definitions describe alarm messages: what they mean and how to recover from them. You search the Alarm Definitions window for alarm information. When you click any service-specific alarm definition, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

You can search for definitions of all alarms that display in Cisco Unified Serviceability. To aid you with troubleshooting problems, the definitions, which exist in a corresponding catalog, include the alarm name, description, explanation, recommended action, severity, parameters, monitors, and so on.

When the system generates an alarm, it uses the alarm definition name in the alarm information, so you can identify the alarm. In the alarm definition, you can view the routing list, which specifies the locations where the system can send the alarm information. The routing list may include the following locations, which correlate to the locations that you can configure in the Alarm Configuration window:

- *Unified CM and Unified CM BE 5000 only*: SDL—The system sends the alarm information to the SDL trace if you enable the alarm for this option and specify an appropriate event level in the Alarm Configuration window.
- SDI —The system sends the alarm information to the SDI trace if you enable the alarm for this option and specify an appropriate event level in the Alarm Configuration window.
- Sys Log—The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an appropriate event level in the Alarm Configuration window, and enter a server name or IP address for the remote syslog server.
- Event Log—The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Cisco Unified Real-Time Monitoring Tool (RTMT), if you enable the alarm for this option and specify an appropriate event level in the Alarm Configuration window.
- Data Collector—System sends the alarm information to the real-time information system (RIS data collector) (for alert purposes only). You cannot configure this option in the Alarm Configuration window.
- *Unified CM and Unified CM BE 5000 only:* SNMP Traps—System generates an SNMP trap. You cannot configure this option in the Alarm Configuration window.

Note Cisco Unified Communications Manager supports SNMP traps in Unified CM and Unified CM BE 5000 systems. Cisco Unity Connection SNMP does not support traps in either Unified CM BE 5000 or Connection systems.

Tip If the SNMP Traps location displays in the routing list, the system forwards the alarm information to the CCM MIB SNMP agent, which generates the appropriate traps according to the definition in CISCO-CCM-MIB.

The system sends an alarm if the configured alarm event level for the specific location in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning,

Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, the system does not send the alarm to the corresponding location.

For each Cisco Unified Serviceability alarm definition, you can include an additional explanation or recommendation. All administrators have access to the added information. You directly enter information into the User Defined Text pane that displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified Serviceability adds the information to the database.

Viewing Alarm Information

You view alarm information to determine whether problems exist. The method that you use to view the alarm information depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the SDI trace log file, or SDL trace log file (Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 only) by using the Trace and Log Central option in RTMT or by using a text editor. You can view alarm information that gets sent to local syslog by using the SysLog Viewer in RTMT.

Tip *Unified CM and Unified CM BE 5000 only*: For Cisco Unified Communications Manager, you can also use CiscoWorks Lan Management Solution report viewer to view remote syslog messages.

Alarm Configuration Checklist

Table 3-1 provides an overview of the steps for configuring alarms.

Table 3-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	In Cisco Unified Communications Manager Administration or in Cisco Unity Connection Administration, configure the Cisco Syslog Agent enterprise parameters to send system, application (services), and security alarms/messages to a remote syslog server that you specify. Skip this step to configure application (services) alarms/messages in Cisco Unified Serviceability.	• Configuring the Cisco Syslog Agent Enterprise Parameters, page 4-1
Step 2	In Cisco Unified Serviceability, configure the server(s), service(s), destination(s), and event level(s) for the applications (services) alarm information that you want to collect. • All services can go to the SDI log (but must be configured in Trace also). • All services can go to the SysLog Viewer. • *Unified CM and Unified CM BE 5000 only*: Only the Cisco CallManager and Cisco CTIManager services use the SDL log. • To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name. If you do not configure the remote server name, Cisco Unified Serviceability does not send the Syslog messages to the remote syslog server. **Tip** Do not configure a Cisco Unified Communications Manager server as a remote Syslog server.	• Understanding Alarms, page 3-1 • Configuring an Alarm for a Service, page 4-2 • Alarm Configuration Settings, page 4-4
Step 3	(Optional) Add a definition to an alarm.	• Alarm Definitions, page 3-3 • Viewing and Updating Alarm Definitions, page 5-1
Step 4	If you chose an SDI trace file or SDL trace file (*Unified CM and Unified CM BE 5000 only*) as the alarm destination, collect traces and view the information with the Trace and Log Central option in RTMT.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 5	If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in RTMT.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 6	See the corresponding alarm definition for the description and recommended action.	Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1

Where to Find More Information

Related Topics

- Configuring the Cisco Syslog Agent Enterprise Parameters, page 4-1
- Configuring an Alarm for a Service, page 4-2
- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1
- System Alarm Catalog Descriptions, page 5-2
- *Unified CM and Unified CM BE 5000 only*: CallManager Alarm Catalog Descriptions, page 5-3

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE 5000 and Connection only*: *Administration Guide for Cisco Unity Connection Serviceability*

CHAPTER 4

Configuring Alarms

This chapter contains the following topics:

Configuring the Cisco Syslog Agent Enterprise Parameters

You can configure the Cisco Syslog Agent enterprise parameters to send system, application, and security alarms/messages that exceed the configured threshold to a remote syslog server that you specify. To access the Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Cisco Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unified Communications Manager Business Edition 5000	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting > Enterprise Parameters**.

Next, configure the remote syslog server name and syslog severity. Then click **Save**. For the valid values to enter, click the **?** button. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Note Do not configure a Cisco Unified Communications Manager as a remote syslog server. The Cisco Unified Communications Manager server does not accept Syslog messages from another server.

Configuring an Alarm for a Service

This section describes how to add or update an alarm for a feature or network service that you manage through Cisco Unified Serviceability.

Note Cisco recommends that you do not change SNMP Trap and Catalog configurations.

Cisco Unity Connection also uses alarms, which are available in Cisco Unity Connection Serviceability. You cannot configure alarms in Cisco Unity Connection Serviceability. For details, see the *Administration Guide for Cisco Unity Connection Serviceability*.

Refer to your online OS documentation for more information on how to use your standard registry editor.

Procedure

Step 1 Choose **Alarm > Configuration**.

The Alarm Configuration window displays.

Step 2 From the Server drop-down list box, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Service Group drop-down list box, choose the category of service, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.

Tip For a list of services that correspond to the service groups, see Table 4-1.

Step 4 From the Service drop-down list box, choose the service for which you want to configure the alarm; then, click **Go**.

Only services that support the service group and your configuration display.

Tip The drop-down list box displays active and inactive services.

In the Alarm Configuration window, a list of alarm monitors with the event levels displays for the chosen service.In addition, the Apply to All Nodes check box displays.

Step 5 *Unified CM only*: If you want to do so, you can apply the alarm configuration for the service to all servers in the cluster by checking the **Apply to All Nodes** check box, provided your configuration supports clusters.

Step 6 Configure the settings, as described in Table 4-2, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Note To set the default, click the **Set Default** button; then, click **Save**.

Services That Use Cisco Tomcat

The following services use Cisco Tomcat for alarm generation:

- Cisco Extension Mobility Application
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer Web

The system login alarm AuthenticationFailed also uses Cisco Tomcat. To generate alarms for these services, perform the following procedure.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Alarm > Configuration**.

Step 2 From the Server drop-down list box, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Services Group drop-down list box, choose **Platform Services**; then, click **Go**.

Step 4 From the Services drop-down list box, choose **Cisco Tomcat**; then, click **Go**.

Step 5 *Unified CM only*: If you want to do so, you can apply the alarm configuration for the service to all servers in the cluster by checking the **Apply to All Nodes** check box, if your configuration supports clusters.

Step 6 Configure the settings, as described in Table 4-2, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Tip The system sends the alarm if the configured alarm event level for the specific destination in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, which are higher severity levels, the system does not send the alarm to the corresponding location.

To access the alarm definitions for the Cisco Extension Mobility Application service, Cisco IP Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer Web Service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window described in Chapter 5, "Viewing and Updating Alarm Definitions".

Additional Information

See the "Related Topics" section on page 4-8.

Service Groups in Alarm Configuration

Table 4-1 lists the services that correspond to the options in the Service Group drop-down list box in the Alarm Configuration window.

Note Not all listed service groups and services apply to all system configurations.

Table 4-1 Service Groups in Alarm Configuration

Service Group	Services	Notes
CM Services	Cisco CTIManager, Cisco CallManager, Cisco CallManager Cisco IP Phone Service, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer Server, Cisco Extended Functions, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, and Cisco Tftp	For a description of these services, see the "Understanding Services" section on page 9-1.
CDR Services	Cisco CDR Agent and Cisco CDR Repository Manager	For a description of these services, see the "Understanding Services" section on page 9-1.
Database and Admin Services	Cisco Bulk Provisioning Service, Cisco Database Layer Monitor, and Cisco License Manager	For a description of these services, see the "Understanding Services" section on page 9-1.
Performance and Monitoring Services	Cisco AMC Service and Cisco RIS Data Collector	For a description of these services, see the "Understanding Services" section on page 9-1.
Directory Services	Cisco DirSync	For a description of this service, see the "Understanding Services" section on page 9-1.
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master	For a description of these services, see the "Understanding Services" section on page 9-1.
System Services	Cisco Trace Collection Service	For a description of these services, see the "Understanding Services" section on page 9-1.
Platform Services	Cisco Tomcat	For a description of this service, see the "Understanding Services" section on page 9-1.

Alarm Configuration Settings

Table 4-2 describes all alarm configuration settings, even though the service may not support the settings. For related procedures, see the "Related Topics" section on page 4-8.

Table 4-2 Alarm Configuration Settings

Name	Description
Server	From the drop-down box, choose the server for which you want to configure the alarm; then, click **Go**.
Service Group	Cisco Unity Connection supports only the following service groups: Database and Admin Services, Performance and Monitoring Services, Backup and Restore Services, System Services, and Platform Services. From the drop-down box, choose the category of services, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.
Service	From the Service drop-down box, choose the service for which you want to configure the alarm; then, click **Go**. Only services that support the service group and your configuration display. **Tip** The drop-down list box displays active and inactive services.
Unified CM only: Apply to All Nodes	To apply the alarm settings for the service to all servers in a cluster, check the check box.
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Table 4-2 Alarm Configuration Settings (continued)

Name	Description
Enable Alarm for Remote Syslogs	The Syslog file serves as the alarm destination. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified Serviceability does not send the Syslog messages. To prevent too many alarms flooding the system, you can check the **Exclude End Point Alarms** checkbox. This ensures that the endpoint phone-related events get logged into a separate file. Exclude End Point Alarms checkbox is displayed only for the Call Manager services, and is not selected by default. You need to select the **Apply to All Nodes** also, while selecting this checkbox. The configuration options for endpoint alarms are given in Table 4-4. **Tip** In the Server field, enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. For example, if you want to send the alarms to CiscoWorks Lan Management Solution, specify the CiscoWorks Lan Management Solution server name. **Tip** Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server.
Enable Alarm for SDI Trace	The SDI trace library serves as the alarm destination. To log alarms in the SDI trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the "Configuring Trace Parameters" section on page 7-1.

Table 4-2 Alarm Configuration Settings (continued)

Name	Description
Unified CM and Unified CM BE 5000 only: Enable Alarm for SDL Trace	The SDL trace library serves as the alarm destination. This destination applies only to the Cisco CallManager service and the CTIManager service. Configure this alarm destination by using Trace SDL configuration. To log alarms in the SDL trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the "Configuring Trace Parameters" section on page 7-1.
Alarm Event Level	From the drop-down list box, choose one of the following options: • **Emergency**—This level designates system as unusable. • **Alert**—This level indicates that immediate action is needed. • **Critical**—The system detects a critical condition. • **Error**—This level signifies an error condition exists. • **Warning**—This level indicates that a warning condition is detected. • **Notice**—This level designates a normal but significant condition. • **Informational**—This level designates information messages only. • **Debug**—This level designates detailed event information that Cisco TAC engineers use for debugging.

Table 4-3 describes the default alarm configuration settings.

Table 4-3 Default Alarm Configuration Settings

	Local Syslogs	Remote Syslogs	SDI Trace	SDL Trace
Enable Alarm	Checked	Unchecked	Checked	Checked
Alarm Event Level	Error	Disabled	Error	Error

Table 4-4 End point Alarm Configuration Options

Exclude End Point Alarms	Local Syslog	Alternate Syslog	Remote Syslog	Syslog Severity and Strangulate Alert	Syslog Traps
Checked	No	Yes	No	No	No
Unchecked	No	Yes	Yes	Yes	Yes

Where to Find More Information

Related Topics

- Configuring the Cisco Syslog Agent Enterprise Parameters, page 4-1
- Configuring an Alarm for a Service, page 4-2
- Service Groups in Alarm Configuration, page 4-3
- Alarm Configuration Settings, page 4-4
- Understanding Alarms, page 3-1

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE 5000 and Connection only*: *Administration Guide for Cisco Unity Connection Serviceability*

CHAPTER 5

Viewing and Updating Alarm Definitions

This chapter, which provides procedural information to search, view, and create user information for alarm definitions that display in Cisco Unified Serviceability, contains the following topics:

Viewing Alarm Definitions and Adding User-Defined Descriptions

This section describes how to search for and view an alarm definition in Cisco Unified Serviceability.

Tip *Unified CM BE 5000 and Connection only*: You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability. You cannot add user-defined descriptions to alarm definitions in Cisco Unity Connection Serviceability.

Cisco Unity Connection also uses certain alarm definitions in Cisco Unified Serviceability, and they must be viewed in Cisco Unified Serviceability. Be aware that alarms that are associated with the catalogs in Table 5-1 are available for viewing.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Alarm > Definitions**.

The Alarm Message Definitions window displays.

Step 2 From the Find alarms where drop-down list box, choose the catalog for which you want to view the definitions.

Step 3 From the Equals drop-down list box, choose a catalog of alarm definitions or enter the alarm name in the Enter Alarm Name field. For a list of System Alarm Catalog options, see Table 5-1. For a list of CallManager Alarm Catalog options (*Unified CM and Unified CM BE 5000 only*), see Table 5-2.

Step 4 Click the **Find** button.

The definitions list displays for the alarm catalog that you chose.

Tip Multiple pages of alarm definitions may exist. To choose another page, click the appropriate navigation button at the bottom of the Alarm Message Definitions window or enter a page number in the Page field. To change the number of alarms that display in the window, choose a different value from the Rows per Page drop-down list box.

Step 5 In the list, click the hyperlink alarm definition for which you want to view alarm details, such as a description, alarm severity, and so on.

The Alarm Information window displays.

Step 6 If you want to add information to the alarm, enter text in the User Defined Text pane and click the **Save** button.

Tip To delete the description from the User Defined Text pane, click the **Clear All** button.

Step 7 To return to the Alarm Message Definitions window, choose **Back to Find/List Alarms** from the Related Links drop-down list box; then, click **Go**.

Additional Information

See the "Related Topics" section on page 5-4.

System Alarm Catalog Descriptions

Table 5-1 contains the System Alarm Catalog alarm descriptions. The System Alarm Catalog supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 5-1 System Catalogs

Name	Description
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishment of security associations between servers in a cluster.
DBAlarmCatalog	All Cisco database (aupair) alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share

Table 5-1 System Catalogs (continued)

Name	Description
JavaApplications	All Java Applications alarm definitions. **Tip** *Unified CM and Unified CM BE 5000 only*: Cisco License Manager, which supports Cisco Unified Communications Manager, uses this catalog. **Tip** You cannot configure JavaApplications alarms by using the alarm configuration GUI. For Cisco Unified Communications Manager and Cisco Unity Connection, you generally configure these alarms to go to the Event Logs; for Cisco Unified Communications Manager, you can configure these alarms to generate SNMP traps to integrate with CiscoWorks Lan Management Solution. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
EMAlarmCatalog	Alarms for Extension Mobility
LoginAlarmCatalog	All login-related alarm definitions
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters.
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services.
TFTPAlarmCatalog	All Cisco TFTP alarm definitions
TVSAlarmCatalog	Alarms for Trust Verification Service
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP traps from the Command Line Interface (CLI). For information on the CLI, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*. **Tip** Cisco Unified Communications Manager supports SNMP traps in Unified CM and Unified CM BE 5000 systems. Cisco Unity Connection SNMP does not support traps in either Unified CM BE 5000 or Connection systems.
CertMonitorAlarmCatalog	All certificate expiration definitions.
CTLproviderAlarmCatalog	Alarms for Certificate Trust List (CTL) Provider service
CDPAlarmCatalog	Alarms for Cisco Discovery Protocol (CDP) service
IMSAlarmCatalog	All user authentication and credential definitions.

Additional Information

See the "Related Topics" section on page 5-4.

CallManager Alarm Catalog Descriptions

The information in this section does not apply to Cisco Unity Connection.

Table 5-2 contains the CallManager Alarm Catalog descriptions.

Table 5-2 CallManager Alarm Catalog

Name	Description
CallManager	All Cisco CallManager service alarm definitions
CDRRepAlarmCatalog	All CDRRep alarm definitions
CARAlarmCatalog	All CDR analysis and reporting alarm definitions
CEFAlarmCatalog	All Cisco Extended Functions alarm definitions
CMIAlarmCatalog	All Cisco messaging interface alarm definitions
CtiManagerAlarmCatalog	All Cisco computer telephony integration (CTI) manager alarm definitions
IpVmsAlarmCatalog	All IP voice media streaming applications alarm definitions
TCDSRVAlarmCatalog	All Cisco telephony call dispatcher service alarm definitions
Phone	Alarms for phone-related tasks, such as downloads
CAPFAlarmCatalog	Alarms for Certificate Authority Proxy Function (CAPF) service

Additional Information

See the "Related Topics" section on page 5-4.

Where to Find More Information

Related Topics

- Understanding Alarms, page 3-1
- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1
- System Alarm Catalog Descriptions, page 5-2
- *Unified CM and Unified CM BE 5000 only*: CallManager Alarm Catalog Descriptions, page 5-3

PART 3

Trace

CHAPTER 6

Understanding Trace

This chapter, which provides information on Cisco Unified Serviceability trace, contains the following topics:

Understanding Trace

Cisco Unified Serviceability provides trace tools to assist you in troubleshooting issues with your voice application. Cisco Unified Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace (for Cisco CallManager and Cisco CTIManager services, applicable to Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 only), and Log4J trace (for Java applications).

You use the Trace Configuration window to specify the level of information that you want traced as well the type of information that you want to be included in each trace file.

Unified CM and Unified CM BE 5000 only: If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateway.

Unified CM and Unified CM BE 5000 only: In the Alarm Configuration window, you can direct alarms to various locations, including SDI trace log files, or SDL trace log files. If you want to do so, you can configure trace for alerts in the Cisco Unified Real-Time Monitoring Tool (RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the trace and log central option in the Cisco Unified Real-Time Monitoring Tool.

Trace Configuration

You can configure trace parameters for any feature or network service that displays in Cisco Unified Serviceability. If you have clusters (Cisco Unified Communications Manager only), you can configure trace parameters for any feature or network service that is available on any Cisco Unified Communications Manager server in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting problems.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files.) If you have clusters (Cisco Unified Communications Manager only), you can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

Unified CM and Unified CM BE 5000 only: If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateways; for example, you can narrow the trace to all enabled phones with a directory number beginning with 555.

If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace window. For more information on troubleshooting trace, see the "Troubleshooting Trace Settings" section on page 6-2.

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in RTMT. For more information regarding trace collection, see the "Trace Collection" section on page 6-3.

Troubleshooting Trace Settings

The Troubleshooting Trace Settings window allows you to choose the services in Cisco Unified Serviceability for which you want to set predetermined troubleshooting trace settings. In this window, you can choose a single service or multiple services and change the trace settings for those services to the predetermined trace settings. If you have clusters (Cisco Unified Communications Manager only), you can choose the services on different Cisco Unified Communications Manager servers in the cluster, so the trace settings of the chosen services get changed to the predetermined trace settings. You can choose specific activated services for a single server, all activated services for the server, specific activated services for all servers in the cluster, or all activated services for all servers in the cluster. In the window, N/A displays next to inactive services.

Note The predetermined troubleshooting trace settings for a Cisco Unified Communications Manager feature or network service include SDL (Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 only), SDI, and Log4j trace settings. Before the troubleshooting trace settings get applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings get restored.

When you open the Troubleshooting Trace Settings window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the Troubleshooting Trace Settings window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for the given service(s). From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the

service. For the given service, the Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings; for example, Maximum No. of Files. You can modify these parameters even after you apply troubleshooting trace settings.

Trace Collection

Use Trace and Log Central, an option in the Cisco Unified Real-Time Monitoring Tool, to collect, view, and zip various service traces and/or other log files. With the Trace and Log Central option, you can collect SDL/SDI traces, Application Logs, System Logs (such as Event View Application, Security, and System logs), and crash dump files.

Tip To collect CSA logs, check the Cisco Security Agent check box in the Select System Logs tab in RTMT. To access user logs that provide information about users that are logging in and out, check the Security Logs check box in the Select System Logs tab.

Tip Do not use NotePad to view collected trace files.

Note *Unified CM and Unified CM BE 5000 only*: For devices that support encryption, the SRTP keying material does not display in the trace file.

For more information on trace collection, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Trace Configuration and Collection Checklist

Table 6-1 provides an overview of the steps for configuring and collecting trace for feature and network services in Cisco Unified Serviceability.

Note You cannot enable or disable trace compression from an enterprise parameter, the user interface (UI) or the command line interface (CLI).

Table 6-1 Trace Configuration and Collection Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Do the applicable step: • *Unified CM and Unified CM BE 5000 only*: Choose **System > Enterprise Parameters** in Cisco Unified Communications Manager Administration and configure the maximum number of devices that are available for tracing**.** Enter a value in the Max Number of Device Level Trace field. The default specifies 12. • *Connection only*: Choose **System Settings > Enterprise Parameters** in Cisco Unity Connection Administration and configure the maximum number of devices that are available for tracing. Enter a value in the Max Number of Device Level Trace field. The default specifies 12.	• *Unified CM and Unified CM BE 5000 only: Cisco Unified Communications Manager Administration Guide* • *Connection only: System Administration Guide for Cisco Unity Connection*
Step 2	Configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service) by doing the applicable step: • *Unified CM and Unified CM BE 5000 only:* Choose **System > Service Parameters** in Cisco Unified Communications Manager Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service). • *Connection only:* Choose **System Settings > Service Parameters** in Cisco Unity Connection Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).	• Configuring Trace and Log Central in RTMT*, Cisco Unified Real-Time Monitoring Tool Administration Guide* • *Unified CM and Unified CM BE 5000 only: Cisco Unified Communications Manager Administration Guide* • *Connection only: System Administration Guide for Cisco Unity Connection*
Step 3	Configure the trace setting for the service for which you want to collect traces. If you have clusters (Cisco Unified Communications Manager only), you can configure trace for the service on one server or on all servers in the cluster. To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields. *Unified CM and Unified CM BE 5000 only*: You can also configure trace for specific devices if you are configuring trace for the Cisco CallManager service or the Cisco CTIManager service. If you want to run predetermined traces on services, set troubleshooting trace for those services.	• Understanding Trace, page 6-1 • Configuring Trace, page 7-1 • Configuring Troubleshooting Trace Settings, page 8-1

Table 6-1 Trace Configuration and Collection Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Install the Cisco Unified Real-Time Monitoring Tool on a local PC.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 5	If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in RTMT. You can find the LogFileSearchStringFound alarm in the LpmTctCatalog. (In Cisco Unified Serviceability, choose **Alarms > Definitions**. In the Find alarms where drop-down list box, choose the **System Alarm Catalog**; in the Equals drop-down list box, choose **LpmTctCatalog**.)	• *Cisco Unified Real-Time Monitoring Tool Administration Guide* • Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1
Step 6	If you want to automatically capture traces for alerts such as CriticalServiceDownand CodeYellow, check the **Enable Trace Download** check box in the Set Alert/Properties dialog box for the specific alert in RTMT; configure how often that you want the download to occur.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 7	Collect the traces.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 8	View the log file in the appropriate viewer.	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Step 9	If you enabled troubleshooting trace, reset the trace settings services, so the original settings get restored. **Note** Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.	Configuring Troubleshooting Trace Settings, page 8-1

Where to Find More Information

Related Topics

- Understanding Alarms, page 3-1
- Alarm Configuration Checklist, page 3-4
- Understanding Trace, page 6-1
- Configuring Troubleshooting Trace Settings, page 8-1

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE 5000 and Connection only*: *Administration Guide for Cisco Unity Connection Serviceability*
- *Connection only*: *System Administration Guide for Cisco Unity Connection*

CHAPTER 7

Configuring Trace

Note Enabling trace decreases system performance; therefore, enable trace only for troubleshooting purposes. For assistance in using trace, contact your technical support team.

This chapter contains the following topics:

Configuring Trace Parameters

This section describes how to configure trace parameters for feature and network services that you manage through Cisco Unified Serviceability.

Tip *Unified CM BE 5000 and Connection only*: For Cisco Unity Connection, you may need to run trace in Cisco Unified Serviceability and Cisco Unity Connection Serviceability to troubleshoot Cisco Unity Connection issues. To troubleshoot services that are supported in Cisco Unified Serviceability, you run trace in Cisco Unified Serviceability. Similarly, to troubleshoot Cisco Unity Connection components, you run trace in Cisco Unity Connection Serviceability. For information on how to run trace in Cisco Unity Connection Serviceability, refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Procedure

Step 1 Choose **Trace > Configuration**.

The Trace Configuration window displays.

Step 2 From the Server drop-down list box, choose the server that is running the service for which you want to configure trace; then, click **Go**.

Step 3 From the Service Group drop-down list box, choose the service group for the service that you want to configure trace; then, click **Go**.

Tip Table 7-1 lists the services and trace libraries that correspond to the options that display in the Service Group drop-down list box.

Step 4 From the Service drop-down list box, choose the service for which you want to configure trace; then, click **Go**.

The drop-down list box displays active and inactive services.

Tip *Unified CM and Unified CM BE 5000 only*: For the Cisco CallManager and CTIManager services, you can configure SDL trace parameters. To do so, open the Trace Configuration window for one of those services, and click the **Go** button that is next to the Related Links drop-down list box.

If you configured Troubleshooting Trace for the service, a message displays at the top of the window that indicates that the Troubleshooting Traces feature is set, which means that the system disables all fields in the Trace Configuration window except for Trace Output Settings. To configure the Trace Output Settings, go to Step 12. To reset Troubleshooting Trace, see the "Configuring Troubleshooting Trace Settings" section on page 8-1.

The trace parameters display for the service that you chose. In addition, the Apply to All Nodes check box displays (Cisco Unified Communications Manager only).

Step 5 *Unified CM only*: If you want to do so, you can apply the trace settings for the service or trace library to all servers in the cluster by checking the **Apply to All Nodes** check box; that is, if your configuration supports clusters.

Step 6 Check the **Trace On** check box.

Step 7 *Unified CM and Unified CM BE 5000 only*: If you are configuring SDL trace parameters, go to Step 10.

Step 8 From the Debug Trace Level drop-down list box, choose the level of information that you want traced, as described in "Debug Trace Level Settings" section on page 7-7.

Step 9 Check the Trace Fields check box for the service that you chose; for example, Cisco Log Partition Monitoring Tool Trace Fields.

Note *Unified CM and Unified CM BE 5000 only*: If you are configuring trace for the Cisco CallManager or the Cisco CTIManager service and you only want trace information for specific Cisco Unified Communications Manager devices, go to Step 11.

Step 10 If the service does not have multiple trace settings where you can specify the traces that you want to activate, check the **Enable All Trace** check box. If the service that you chose has multiple trace settings, check the check boxes next to the trace check boxes that you want to enable, as described in Trace Field Descriptions, page 7-8.

Step 11 *Unified CM and Unified CM BE 5000 only*: If you are configuring trace for the Cisco CallManager or the Cisco CTIManager service and you want trace information for specific Cisco Unified Communications Manager devices, perform the following tasks:

a. Check the **Device Name Based Trace Monitoring** check box.

The Device Name Based Trace Monitoring option traces only the selected devices, thus narrowing the number of trace logs that are generated and reducing the impact on call processing.

b. Click the **Select Devices** button.

The Device Selection for Tracing window displays.

Tip From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**; configure the maximum number of devices that are available for tracing**.** Enter a value in the Max Number of Device Level Trace field. For help on configuring the parameter, click the link for the parameter name or the question mark button in the upper, right corner of the window.

c. From the **Find** drop-down list box, choose the device for which you want a trace.

d. Enter the appropriate search criteria for the device for which you want a trace and click the **Find** button.

The window with the search results displays. If more pages of search results to view exist, click the **First**, **Previous**, **Next**, or **Last** button.

e. Click the Trace check box for the device or devices for which you want device-name-based trace monitoring.

f. Click the **Save** button.

g. When the update finishes, click the browser close button to close the Device Selection for Tracing window and return to the Trace Configuration window.

h. If you want trace to apply to non-devices in addition to devices, check the **Include Non-device Traces** check box. If check box is checked, set the appropriate debug trace level as described in "Debug Trace Level Settings" section on page 7-7.

Step 12 To limit the number and size of the trace files, specify the trace output setting. See Table 7-17 for descriptions and default values.

Step 13 To save your trace parameters configuration, click the **Save** button.

The changes to trace configuration take effect immediately for all services except Cisco Messaging Interface (Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 only). The trace configuration changes for Cisco Messaging Interface take effect in 3 to 5 minutes.

Note To set the default, click the **Set Default** button.

Additional Information

See the "Related Topics" section on page 7-18.

Service Groups in Trace Configuration

Table 7-1 lists the services and trace libraries that correspond to the options in the Service Group drop-down list box in the Trace Configuration window.

Table 7-1 Service Groups in Trace Configuration

Service Group	Services and Trace Libraries	Notes
Unified CM and Unified CM BE 5000 only: CM Services	Cisco CTIManager, Cisco CallManager, Cisco CallManager Cisco IP Phone Service, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer Server, Cisco Extended Functions, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, Cisco TFTP, and Cisco Unified Mobile Voice Access Service	For a description of these services, see the "Understanding Services" section on page 9-1. For most services in the CM Services group, you run trace for specific components, instead of enabling all trace for the service. The "Trace Field Descriptions" section on page 7-8 lists the services for which you can run trace for specific components.
Unified CM and Unified CM BE 5000 only: CTI Services	Cisco IP Manager Assistant, and Cisco Web Dialer Web Service	For a description of these services, see the "Understanding Services" section on page 9-1. For these services, you can run trace for specific components, instead of enabling all trace for the service; see the "Trace Field Descriptions" section on page 7-8.
Unified CM and Unified CM BE 5000 only: CDR Services	Cisco CAR Scheduler, Cisco CAR Web Service, Cisco CDR Agent, and Cisco CDR Repository Manager	For a description of these services, see the "Understanding Services" section on page 9-1. You enable all trace for each service, instead of running trace for specific components. In CAR, when reports are run that call stored procedures, CAR checks the configured debug trace level for the Cisco CAR Scheduler service and the Cisco CAR Web Service in the Trace Configuration window before stored procedure logging begins. For pregenerated reports, CAR checks the level for the Cisco CAR Scheduler service; for on-demand reports, CAR checks the level for the Cisco CAR Web Service. If you choose Debug from the Debug Trace Level drop-down list box, stored procedure logging gets enabled and continues until you choose another option from the drop-down list box. The following CAR reports use stored procedure logging: Gateway Utilization report, Route and Line Group Utilization report, Route/Hunt List Utilization report, Route Pattern/Hunt Pilot Utilization report, Conference Call Details report, Conference Call Summary report, Conference Bridge Utilization report, Voice Messaging Utilization report, and the CDR Search report.

Table 7-1 Service Groups in Trace Configuration (continued)

Service Group	Services and Trace Libraries	Notes
Database and Admin Services	Cisco AXL Web Service, Cisco CCM DBL Web Library, Cisco CCMAdmin Web Service, Cisco CCMUser Web Service, Cisco Database Layer Monitor, and Cisco UXL Web Service *Unified CM and Unified CM BE 5000 only*: Cisco Bulk Provisioning Service, Cisco GRT Communications Web Service, Cisco Role-based Security, Cisco TAPS Service, and Cisco Unified Reporting Web Service *Unified CM BE 5000 only*: Cisco License Manager	For a description of these services (not the Cisco CCM DBL Web Library or Cisco Role-based Security options), see the "Understanding Services" section on page 9-1. Choosing the Cisco CCM DBL Web Library option activates the trace for database access for Java applications. For database access for C++ applications, activate trace for Cisco Database Layer Monitor, as described in the "Cisco Extended Functions Trace Fields" section on page 7-15. Choosing the Cisco Role-based Security option, which supports Cisco Unified Communications Manager, activates trace for user-role authorization. For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components.
Performance and Monitoring Services	Cisco AMC Service, Cisco CCM NCS Web Library, CCM PD Web Service, Cisco CallManager SNMP Service, Cisco Log Partition Monitoring Tool, Cisco RIS Data Collector, Cisco RTMT Web Service, Cisco Audit Event Service, and Cisco RisBean Library. *Unified CM and Unified CM BE 5000 only*: Cisco CCM PD Web Service	For a description of these services (not the Cisco CCM NCS Web Library or the Cisco RTMT Web Service), see the "Understanding Services" section on page 9-1. Choosing the Cisco CCM NCS Web Library option activates trace for database change notification for the Java client. Choosing the Cisco RTMT Web Service option activates trace for the RTMT servlets; running this trace creates the server-side log for RTMT client queries.
Unified CM and Unified CM BE 5000 only: Security Services	Cisco CTL Provider , Cisco Certificate Authority Proxy Function, and Cisco Trust Verification Service.	For a description of these services, see the "Understanding Services" section on page 9-1. You enable all trace for each service, instead of running trace for specific components.
Unified CM and Unified CM BE 5000 only: Directory Services	Cisco DirSync	For a description of this service, see the "Understanding Services" section on page 9-1. You enable all trace for this service, instead of running trace for specific components.

Table 7-1 Service Groups in Trace Configuration (continued)

Service Group	Services and Trace Libraries	Notes
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master	For a description of these services, see the "Understanding Services" section on page 9-1. You enable all trace for each service, instead of running trace for specific components.
System Services	Cisco CCMRealm Web Service, Cisco CCMService Web Service, Cisco Common User Interface, and Cisco Trace Collection Service	For a description of the Cisco Trace Collection service, see the "Understanding Services" section on page 9-1. Choosing the Cisco CCMRealm Web Service option activates trace for login authentication. Choosing the Cisco Common User Interface option activates trace for the common code that multiple applications use; for example, Cisco Unified Operating System Administration and Cisco Unified Serviceability. Choosing the Cisco CCMService Web Service option activates trace for the Cisco Unified Serviceability web application (GUI). You enable all trace for each option/service, instead of running trace for specific components.
SOAP Services	Cisco SOAP Web Service and Cisco SOAPMessage Service	Choosing the Cisco SOAP Web Service option activates the trace for the AXL Serviceability API. You enable all trace for this service, instead of running trace for specific components.
Platform Services	Cisco Unified OS Admin Web Service	The Cisco Unified OS Admin Web Service supports Cisco Unified Operating System Administration, which is the web application that provides management of platform-related functionality such as certificate management, version settings, and installations and upgrades. You enable all trace for this service, instead of running trace for specific components.

Debug Trace Level Settings

Table 7-2 describes the debug trace level settings for services.

Table 7-2 Debug Trace Levels for Services

Level	Description
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation. Traces call-processing events.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.
Entry/Exit	**Note** Not all services use this trace level. Traces all Significant conditions plus entry and exit points of routines.
Arbitrary	**Note** *Unified CM and Unified CM BE 5000 only*: Do not use this trace level with the Cisco CallManager service or the Cisco IP Voice Media Streaming Application service during normal operation. Traces all Entry/Exit conditions plus low-level debugging information.
Detailed	**Note** *Unified CM and Unified CM BE 5000 only*: Do not use this trace level with the Cisco CallManager service or the Cisco IP Voice Media Streaming Application service during normal operation. Traces all Arbitrary conditions plus detailed debugging information.

Table 7-3 describes the debug trace level settings for servlets.

Table 7-3 Debug Trace Levels for Servlets

Level	Description
Fatal	Traces very severe error events that may cause the application to abort.
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path.
Warn	Traces potentially harmful situations.

Table 7-3 Debug Trace Levels for Servlets (continued)

Level	Description
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. Trace level that turns on all logging.

Additional Information

See the "Related Topics" section on page 7-18.

Trace Field Descriptions

For some services, you can activate trace for specific components, instead of enabling all trace for the service. The following list includes the services for which you can activate trace for specific components. Clicking one of the cross-references takes you to the applicable section where a description displays for each trace field for the service. If a service does not exist in the following list, the Enable All Trace check box displays for the service in the Trace Configuration window.

The following services are applicable to Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, and Cisco Unity Connection:

- Cisco Database Layer Monitor Trace Fields, page 7-9
- Cisco RIS Data Collector Trace Fields, page 7-9

The following services are applicable to Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 only:

- Cisco CallManager SDI Trace Fields, page 7-10
- Cisco CallManager SDL Trace Fields, page 7-12
- Cisco CTIManager SDL Trace Fields, page 7-13
- Cisco Extended Functions Trace Fields, page 7-15
- Cisco Extension Mobility Trace Fields, page 7-15
- Cisco IP Manager Assistant Trace Fields, page 7-16
- Cisco IP Voice Media Streaming App Trace Fields, page 7-16
- Cisco TFTP Trace Fields, page 7-17
- Cisco Web Dialer Web Service Trace Fields, page 7-17

Cisco Database Layer Monitor Trace Fields

Table 7-4 describes the Cisco Database Layer Monitor trace fields. The Cisco Database Layer Monitor service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 7-4 Cisco Database Layer Monitor Trace Fields

Field Name	Description
Enable DB Library Trace	Activates database library trace for C++ applications.
Enable Service Trace	Activates service trace.
Enable DB Change Notification Trace	Activates the database change notification traces for C++ applications.
Enable Unit Test Trace	Do not check this check box. Cisco engineering uses it for debugging purposes.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco RIS Data Collector Trace Fields

Table 7-5 describes the Cisco RIS Data Collector trace fields. The Cisco RIS Data Collector service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 7-5 Cisco RIS Data Collector Trace Fields

Field Name	Description
Enable RISDC Trace	Activates trace for the RISDC thread of the RIS data collector service (RIS).
Enable System Access Trace	Activates trace for the system access library in the RIS data collector.
Enable Link Services Trace	Activates trace for the link services library in the RIS data collector.
Enable RISDC Access Trace	Activates trace for the RISDC access library in the RIS data collector.
Enable RISDB Trace	Activates trace for the RISDB library in the RIS data collector.
Enable PI Trace	Activates trace for the PI library in the RIS data collector.

Table 7-5 Cisco RIS Data Collector Trace Fields (continued)

Field Name	Description
Enable XML Trace	Activates trace for the input/output XML messages of the RIS data collector service.
Enable Perfmon Logger Trace	Activates trace for the troubleshooting perfmon data logging in the RIS data collector. Used to trace the name of the log file, the total number of counters that are logged, the names of the application and system counters and instances, calculation of process and thread CPU percentage, and occurrences of log file rollover and deletion.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco CallManager SDI Trace Fields

Table 7-6 describes the Cisco CallManager SDI trace fields. The Cisco CallManager service supports Cisco Unified Communications Manager.

Table 7-6 Cisco CallManager SDI Trace Fields

Field Name	Description
Enable H245 Message Trace	Activates trace of H245 messages.
Enable DT-24+/DE-30+ Trace	Activates the logging of ISDN type of DT-24+/DE-30+ device traces.
Enable PRI Trace	Activates trace of primary rate interface (PRI) devices.
Enable ISDN Translation Trace	Activates ISDN message traces. Used for normal debugging.
Enable H225 & Gatekeeper Trace	Activates trace of H.225 devices. Used for normal debugging.
Enable Miscellaneous Trace	Activates trace of miscellaneous devices. **Note** Do not check this check box during normal system operation.
Enable Conference Bridge Trace	Activates trace of conference bridges. Used for normal debugging.
Enable Music on Hold Trace	Activates trace of music on hold (MOH) devices. Used to trace MOH device status such as registered with Cisco Unified Communications Manager, unregistered with Cisco Unified Communications Manager, and resource allocation processed successfully or failed.

Table 7-6 Cisco CallManager SDI Trace Fields (continued)

Field Name	Description
Enable Unified CMReal-Time Information Server Trace	Activates Cisco Unified Communications Manager real-time information traces that the real-time information server uses.
Enable SIP Stack Trace	Activates trace of SIP stack. **Note** Enabling SIP Stack Trace can cause extreme performance degradation especially during high traffic hours.
Enable Annunciator Trace	Activates trace for the annunciator, a SCCP device that uses the Cisco IP Voice Media Streaming Application service to enable Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices.
Enable CDR Trace	Activates traces for CDR.
Enable Analog Trunk Trace	Activates trace of all analog trunk (AT) gateways.
Enable All Phone Device Trace	Activates trace of phone devices. Trace information includes SoftPhone devices. Used for normal debugging.
Enable MTP Trace	Activates trace of media termination point (MTP) devices. Used for normal debugging.
Enable All Gateway Trace	Activates trace of all analog and digital gateways.
Enable Forward and Miscellaneous Trace	Activates trace for call forwarding and all subsystems that are not covered by another check box. Used for normal debugging.
Enable MGCP Trace	Activates trace for media gateway control protocol (MGCP) devices. Used for normal debugging.
Enable Media Resource Manager Trace	Activates trace for media resource manager (MRM) activities.
Enable SIP Call Processing Trace	Activates trace for SIP call processing. **Note** You can view the SIP messages that get logged into the SDI log file, when **Enable SIP Call Processing Trace** check box is checked and Trace Level is set to any one of the following—State Transition, Significant, Arbitrary or Detailed. For more information on session trace, refer to the *Understanding Session Trace* section in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Table 7-6 Cisco CallManager SDI Trace Fields (continued)

Field Name	Description
Enable SCCP Keep Alive Trace	Activates trace for SCCP keepalive trace information in the Cisco CallManager traces. Because each SCCP device reports keepalive messages every 30 seconds, and each keepalive message creates 3 lines of trace data, the system generates a large amount of trace data when this check box is checked.
Enable SIP Keep Alive (REGISTER Refresh) Trace	Activates trace for SIP keepalive (REGISTER refresh) trace information in the Cisco CallManager traces. Because each SIP device reports keepalive messages every 2 minutes, and each keepalive message can create multiple lines of trace data, the system generates a large amount of trace data when this check box is checked.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco CallManager SDL Trace Fields

Table 7-17 describes the Cisco CallManager SDL trace filter settings. Table 7-8 describes the Cisco CallManager SDL configuration characteristics. The Cisco CallManager service supports Cisco Unified Communications Manager.

Note Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Table 7-7 Cisco CallManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable all Layer 1 traces.	Activates traces for Layer 1.
Enable detailed Layer 1 traces.	Activates detailed Layer 1 traces.
Enable all Layer 2 traces.	Activates traces for Layer 2.
Enable Layer 2 interface trace.	Activates Layer 2 interface traces.
Enable Layer 2 TCP trace.	Activates Layer 2 Transmission Control Program (TCP) traces.
Enable detailed dump Layer 2 trace.	Activates detailed traces for dump Layer 2.
Enable all Layer 3 traces.	Activates traces for Layer 3.
Enable all call control traces.	Activates traces for call control.
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.

Table 7-7 Cisco CallManager SDL Configuration Trace Filter Settings (continued)

Setting Name	Description
Enable message translation signals trace.	Activates traces for message translation signals.
Enable UUIE output trace.	Activates traces for user-to-user informational element (UUIE) output.
Enable gateway signals trace.	Activates traces for gateway signals.
Enable CTI trace.	Activates CTI trace.
Enable network service data trace	Activates network service data trace.
Enable network service event trace	Activates network service event trace.
Enable ICCP admin trace	Activates ICCP administration trace.
Enable default trace	Activates default trace.

Table 7-8 Cisco CallManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for intracluster communication protocol (ICCP) link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP event trace.	Activates SDL TCP event trace.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco CTIManager SDL Trace Fields

Table 7-9 describes the Cisco CTIManager SDL configuration trace filter settings. Table 7-10 describes the Cisco CTIManager SDL configuration trace characteristics. The Cisco CTIManager service supports Cisco Unified Communications Manager.

Tip Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Tip When you choose the CTIManager service from the Service Groups drop-down list box, the Trace Configuration window displays for SDI traces for this service. To activate SDI trace for the Cisco CTI Manager service, check the **Enable All Trace** check box in the Trace Configuration window for the Cisco CTIManager service. To access the SDL Configuration window, choose **SDL Configuration** from the Related Links drop-down list box; the settings that are described in Table 7-9 and Table 7-10 display.

Table 7-9 Cisco CTIManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.
Enable CTI trace.	Activates CTI trace.
Enable Network Service Data Trace	Activates network service data trace.
Enable Network Service Event Trace	Activates network service event trace.
Enable ICCP Admin Trace	Activates ICCP administration trace.
Enable Default Trace	Activates default trace.

Table 7-10 Cisco CTIManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for ICCP link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP Event trace	Activates SDL TCP event trace.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco Extended Functions Trace Fields

Table 7-11 describes the Cisco Extended Functions trace fields. The Cisco Extended Functions service supports Cisco Unified Communications Manager.

Table 7-11 Cisco Extended Functions Trace Fields

Field Name	Description
Enable QBE Helper TSP Trace	Activates telephony service provider trace.
Enable QBE Helper TSPI Trace	Activates QBE helper TSP interface trace.
Enable QRT Dictionary Trace	Activates quality report tool service dictionary trace.
Enable DOM Helper Traces	Activates DOM helper trace.
Enable Redundancy and Change Notification Trace	Activates database change notification trace.
Enable QRT Report Handler Trace	Activates quality report tool report handler trace.
Enable QBE Helper CTI Trace	Activates QBE helper CTI trace.
Enable QRT Service Trace	Activates quality report tool service related trace.
Enable QRT DB Traces	Activates QRT DB access trace.
Enable Template Map Traces	Activates standard template map and multimap trace.
Enable QRT Event Handler Trace	Activates quality report tool event handler trace.
Enable QRT Real-Time Information Server Trace	Activates quality report tool real-time information server trace.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco Extension Mobility Trace Fields

Table 7-12 describes the Cisco Extension Mobility trace fields. The Cisco Extension Mobility service supports Cisco Unified Communications Manager.

Table 7-12 Cisco Extension Mobility Trace Fields

Field Name	Description
Enable EM Service Trace	Activates trace for the extension mobility service.

Tip When you activate trace for the Cisco Extension Mobility Application service, you check the Enable All Trace check box in the Trace Configuration window for the Cisco Extension Mobility Application service.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco IP Manager Assistant Trace Fields

Table 7-13 describes the Cisco IP Manager Assistant trace fields. The Cisco IP Manager Assistant service supports Cisco Unified Communications Manager Assistant.

Table 7-13 Cisco IP Manager Assistant Trace Fields

Field Name	Description
Enable IPMA Service Trace	Activates trace for the Cisco IP Manager Assistant service.
Enable IPMA Manager Configuration Change Log	Activates trace for the changes that you make to the manager and assistant configurations.
Enable IPMA CTI Trace	Activates trace for the CTI Manager connection.
Enable IPMA CTI Security Trace	Activates trace for the secure connection to CTIManager.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco IP Voice Media Streaming App Trace Fields

The information in this section does not apply to Cisco Unity Connection.

Table 7-14 describes the Cisco IP Voice Media Streaming App trace fields. The Cisco IP Voice Media Streaming App service supports Cisco Unified Communications Manager.

Table 7-14 Cisco IP Voice Media Streaming Application Trace Fields

Field Name	Description
Enable Service Initialization Trace	Activates trace for initialization information.
Enable MTP Device Trace	Activates traces to monitor the processed messages for media termination point (MTP).
Enable Device Recovery Trace	Activates traces for device-recovery-related information for MTP, conference bridge, and MOH.
Enable Skinny Station Messages Trace	Activates traces for skinny station protocol.
Enable WinSock Level 2 Trace	Activates trace for high-level, detailed WinSock-related information.
Enable Music On Hold Manager Trace	Activates trace to monitor MOH audio source manager.
Enable Annunciator Trace	Activates trace to monitor annunciator.
Enable DB Setup Manager Trace	Activates trace to monitor database setup and changes for MTP, conference bridge, and MOH.

Table 7-14 Cisco IP Voice Media Streaming Application Trace Fields (continued)

Field Name	Description
Enable Conference Bridge Device Trace	Activates traces to monitor the processed messages for conference bridge.
Enable Device Driver Trace	Activates device driver traces.
Enable WinSock Level 1 Trace	Activates trace for low-level, general, WinSock-related information.
Enable Music on Hold Device Trace	Activates traces to monitor the processed messages for MOH.
Enable TFTP Downloads Trace	Activates trace to monitor the download of MOH audio source files.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco TFTP Trace Fields

Table 7-15 describes the Cisco TFTP trace fields. The Cisco TFTP service supports Cisco Unified Communications Manager.

Table 7-15 Cisco TFTP Trace Fields

Field Name	Description
Enable Service System Trace	Activates trace for service system.
Enable Build File Trace	Activates trace for build files.
Enable Serve File Trace	Activates trace for serve files.

Additional Information

See the "Related Topics" section on page 7-18.

Cisco Web Dialer Web Service Trace Fields

Table 7-16 describes the Cisco Web Dialer Web Service trace fields. The Cisco Web Dialer Web Service supports Cisco Unified Communications Manager.

Table 7-16 Cisco Web Dialer Web Service Trace Fields

Field Name	Description
Enable Web Dialer Servlet Trace	Activates trace for Cisco Web Dialer servlet.
Enable Redirector Servlet Trace	Activates trace for the Redirector servlet.

Additional Information

See the "Related Topics" section on page 7-18.

Trace Output Settings Descriptions and Defaults

Table 7-17 contains the trace log file descriptions and defaults.

Caution When you change either the Maximum No. of Files or the Maximum File Size settings in the Trace Configuration window, the system deletes all service log files except for the current file, that is, if the service is running; if the service has not been activated, the system deletes the files immediately after you activate the service. Before you change the Maximum No. of Files setting or the Maximum File Size setting, download and save the service log files to another server if you want to keep a record of the log files; to perform this task, use Trace and Log Central in RTMT.

Table 7-17 Trace Output Settings

Field	Description
Maximum number of files	This field specifies the total number of trace files for a given service. Cisco Unified Serviceability automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum file size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

Additional Information

See the "Related Topics" section on page 7-18.

Where to Find More Information

Related Topics

- Configuring Trace Parameters, page 7-1
- Service Groups in Trace Configuration, page 7-4
- Debug Trace Level Settings, page 7-7
- Trace Field Descriptions, page 7-8
- Trace Output Settings Descriptions and Defaults, page 7-18

CHAPTER 8

Configuring Troubleshooting Trace Settings

The Troubleshooting Trace Settings window allows you to choose the services for which you want to set predetermined troubleshooting trace settings. This chapter contains information on how to set and reset troubleshooting trace settings for services that exist in Cisco Unified Serviceability.

Note Leaving Troubleshooting Trace enabled for a long time increases the size of the trace files and may impact the performance of the services.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Trace > Troubleshooting Trace Settings**.

Step 2 From the Server drop-down list box, choose the server where you want to troubleshoot trace settings; then, click **Go**.

Note A list of services displays. The services that are not activated display as N/A.

Step 3 Perform one of the following tasks:

- To check specific services for the server that you chose in the Server drop-down list box, check the service(s) check box(es) in the Services pane; for example, the Database and Admin Services, Performance and Monitoring Services, or the Backup and Restore Services pane (and so on).

  This task affects only the server that you chose in the Server drop-down list box.

- Check one of the following check boxes:
  - **Check All Services**—Automatically checks all check boxes for the services on the current server that you chose in the Server drop-down list box.
  - *Unified CM clusters only*: **Check Selected Services on All Nodes**—Allows you to check specific service check boxes in the Troubleshooting Trace Setting window. This setting applies for all servers in the cluster where the service is activated.
  - *Unified CM clusters only*: **Check All Services on All Nodes** —Automatically checks all check boxes for all services for all servers in the cluster. When you check this check box, the **Check All Services** and **Check Selected Services on All Nodes** check boxes automatically get checked.

Step 4 Click the **Save** button.

Step 5 After you configure troubleshooting trace for one or more services, you can restore the original trace settings. If you want to restore the original trace settings, click one of the following buttons:

- **Reset Troubleshooting Traces—**Restores the original trace settings for the services on the server that you chose in the Server drop-down list box; also displays as an icon that you can click.
- *Unified CM clusters only*: **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all servers in the cluster.

After you click the reset button, the window refreshes, and the service check boxes display as unchecked.

Additional Information

See the "Related Topics" section on page 8-2.

Where to Find More Information

Related Topics

- Configuring Trace, page 7-1
- Understanding Trace, page 6-1

PART 4

Tools

CHAPTER 9

Understanding Services

Cisco Unified Serviceability service management includes working with feature and network services and servlets, which are associated with the Tomcat Java Webserver. Feature services allow you to use application features, such as Serviceability Reports Archive, while network services are required for your system to function.

If something is wrong with a service or servlet, an alarm gets written to an alarm monitor. After viewing the alarm information, you can run a trace on the service. Be aware that services and servlets display different trace levels in the Trace Configuration window.

This chapter, which provides a description of services/servlets, Service Activation, and Control Center, contains information on the following topics:

Feature Services

In Cisco Unified Serviceability, you can activate, start, and stop feature services. Activation turns on and starts the service. After you activate a service in the Service Activation window, you do not need to start it in the Control Center—Feature Services window. If the service does not start for any reason, you must start it in the Control Center—Features Services window.

After the system is installed, it does not automatically activate feature services, which are related services that are required if you want to use your configuration features; for example, the Serviceability Reports Archive feature.

Unified CM and Unified CM BE 5000 only: After you activate feature services, you can modify associated service parameters in Cisco Unified Communications Manager Administration.

Connection only: After you activate feature services, you can modify associated settings in Cisco Unity Connection Administration.

Unified CM only: If you are upgrading Cisco Unified Communications Manager, those services that you activated on the system prior to the upgrade automatically activate and start after the upgrade.

In the Service Activation window, Cisco Unified Serviceability categorizes feature services into the following groups:

In the Control Center—Feature Services window, Cisco Unified Serviceability categorizes services into the same groups that display in the Service Activation window.

Tip For service activation recommendations, see the "Service Activation" section on page 9-17 and the "Activating and Deactivating Feature Services" section on page 11-1.

Database and Admin Services

This section describes the Database and Admin Services.

Cisco AXL Web Service

The Cisco AXL Web Service allows you to modify database entries and execute stored procedures from client-based applications that use AXL.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco UXL Web Service

The TabSync client in Cisco IP Phone Address Book Synchronizer uses the Cisco UXL Web Service for queries to the Cisco Unified Communications Manager database, which ensures that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them. The Cisco UXL Web Service performs the following functions:

- Conducts authentication checks by verifying the end user name and password when an end user logs in to Cisco IP Phone Address Book Synchronizer.
- Conducts a user authorization check by only allowing the user that is currently logged in to Cisco IP Phone Address Book Synchronizer to perform functions such as listing, retrieving, updating, removing, and adding contacts.

Cisco Bulk Provisioning Service

This service does not support Cisco Unity Connection.

If your configuration supports clusters (Cisco Unified Communications Manager only), you can activate the Cisco Bulk Provisioning Service only on the first server. If you use the Cisco Unified Communications Manager Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco TAPS Service

This service does not support Cisco Unity Connection.

The Cisco TAPS Service supports the Cisco Unified Communications Manager Auto-Register Phone Tool, which allows a user to upload a customized configuration on an auto registered phone after a user responds to Interactive Voice Response (IVR) prompts.

If your configuration supports clusters (Cisco Unified Communications Manager only), you activate this service on the first server. When you want to create dummy MAC addresses for the tool, ensure that the Cisco Bulk Provisioning Service is activated on the same server.

Tip The Cisco Unified Communications Manager Auto-Register Phone Tool relies on Cisco Customer Response Solutions (CRS). Before the tool can work as designed, verify that the CRS server is configured and running, as described in the CRS documentation.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Performance and Monitoring Services

This section describes the Performance Monitoring Services.

Cisco Serviceability Reporter

The Cisco Serviceability Reporter service generates the daily reports that are described in "Understanding Serviceability Reports Archive" section on page 10-1.

If your configuration supports clusters (Cisco Unified Communications Manager only), this service gets installed on all the Cisco Unified Communications Manager servers in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco Unified Serviceability from the Tools menu. Each summary report comprises different charts that display the statistics for that particular report. After you activate the service, report generation may take up to 24 hours.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco CallManager SNMP Service

This service does not support Cisco Unity Connection.

This service, which implements the CISCO-CCM-MIB, provides SNMP access to provisioning and statistics information that is available for Cisco Unified Communications Manager.

If your configuration supports clusters (Cisco Unified Communications Manager only), activate this service on all servers in the cluster.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager.

CM Services

This section describes the CM Services and does not apply to Cisco Unity Connection.

Cisco CallManager

The Cisco CallManager service provides software-only call processing as well as signaling and call control functionality for Cisco Unified Communications Manager.

Tip *Unified CM clusters only*: Before you activate this service, verify that the Cisco Unified Communications Manager server displays in the Find and List Cisco Unified CMs window in Cisco Unified Communications Manager Administration. If the server does not display, add the Cisco Unified Communications Manager server before you activate this service. For information on how to find and add the server, refer to the *Cisco Unified Communications Manager Administration Guide*.

Tip *Unified CM clusters only*: If you deactivate the Cisco CallManager or CTIManager services in Service Activation, the Cisco Unified Communications Manager server where you deactivated the service no longer exists in the database, which means that you cannot choose that Cisco Unified Communications Manager server for configuration operations in Cisco Unified Communications Manager Administration because it does not display in the graphical user interface (GUI). If you then reactivate the services on the same Cisco Unified Communications Manager server, the database creates an entry for Cisco Unified Communications Manager again and adds a "CM_" prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager or CTIManager service on a server with an IP address of 172.19.140.180, then CM_172.19.140.180 displays in Cisco Unified Communications Manager Administration. You can now choose the server, with the new "CM_" prefix, in Cisco Unified Communications Manager Administration.

The following services rely on Cisco CallManager service activation:

- Cisco CTIManager, page 9-5
- CDR Services, page 9-7

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files that are consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

Unified CM only: A configuration file includes a list of Cisco Unified Communications Managers to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (DHCP) server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. The device requests a configuration file from the TFTP server. The configuration file contains a list of Cisco Unified Communications Managers and the TCP port through which the device connects to those Cisco Unified Communications Managers. The configuration file contains a list of Cisco Unified Communications Managers and the TCP port through which the device connects to those Cisco Unified Communications Managers.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Messaging Interface

The Cisco Messaging Interface allows you to connect a simplified message desk interface (SMDI)-compliant external voice-messaging system with the Cisco Unified Communications Manager. The SMDI defines a way for a phone system to provide a voice-messaging system with the information that is needed to intelligently process incoming calls.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Unified Mobile Voice Access Service

The Cisco Unified Voice Access Service starts the mobile voice access capability within Cisco Unified Mobility; mobile voice access, which is an integrated voice response (IVR) system, allows Cisco Unified Mobility users to perform the following tasks:

- Make calls from the cellular phone as if the call originated from the desk phone.
- Turn Cisco Unified Mobility on.
- Turn Cisco Unified Mobility off.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for Cisco Unified Communications Manager for use with MTP, conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from Cisco Unified Communications Manager to the IP voice media streaming driver, which handles RTP streaming.

The Cisco IP Voice Media Streaming Application service does not generates the Call Management Record (CMR) files for call legs that involve any IP Voice Media Streaming App components like conference, MOH, Annunciator or MTP.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco CTIManager

The Cisco CTI Manager contains the CTI components that interface with applications. This service allows applications to monitor/control phones and virtual devices to perform call control functionality.

Unified CM clusters only: With CTI Manager, applications can access resources and functionality of all Cisco Unified Communications Managers in the cluster and have improved failover capability. Although one or more CTI Managers can be active in a cluster, only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can only use one connection at a time to open a device with media termination.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Extension Mobility

This service, which supports the Cisco Extension Mobility feature, performs the login and automatic logout functionality for the feature.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager.

Cisco Dialed Number Analyzer

The Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. When activated, this application consumes a lot of resources, so activate this service only during off-peak hours when minimal call-processing interruptions may occur.

Unified CM clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Dialed Number Analyzer Server

The Cisco Dialed Number Analyzer Server service along with the Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

Unified CM clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco DHCP Monitor Service

Cisco DHCP Monitor Service monitors IP address changes for IP phones in the database tables. When a change is detected, it modifies the /etc./dhcpd.conf file and restarts the DHCPD daemon.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

CTI Services

This section describes the CTI Services and does not apply to Cisco Unity Connection.

Cisco IP Manager Assistant

This service supports Cisco Unified Communications Manager Assistant. After service activation, Cisco Unified Communications Manager Assistant enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified Communications Manager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco WebDialer Web Service for Cisco Unified Communications Manager Systems

Cisco Web Dialer provides click-to-dial functionality. It allows users inside a Cisco Unified Communications Manager cluster to initiate a call to other users inside or outside the cluster by using a web page or a desktop application. Cisco Web Dialer provides a web page that enables users to call each other within a cluster. Cisco Web Dialer comprises two components: Web Dialer servlet and Redirector servlet.

The Redirector servlet provides the ability for third-party applications to use Cisco Web Dialer. The Redirector servlet finds the appropriate Cisco Unified Communications Manager cluster for the Cisco Web Dialer user and redirects the request to the Cisco Web Dialer in that cluster. The Redirector functionality only applies for HTTP/HTML-based Web Dialer client applications because it is not available for Simple Object Access Protocol (SOAP)-based Web Dialer applications.

Cisco WebDialer Web Service for Cisco Unified Communications Manager Business Edition 5000 Systems

Cisco Web Dialer, which is used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

This service supports Cisco Unified Communications Manager.

CDR Services

This section describes the CDR Services and does not apply to Cisco Unity Connection.

Cisco SOAP - CDRonDemand Service

The Cisco SOAP - CDRonDemand Service, a SOAP/HTTPS-based service, runs on the CDR Repository server.It receives SOAP requests for CDR file name lists that are based on a user-specified time interval (up to a maximum of 1 hour) and returns a list of file names that fit the time duration that is specified in the request. This service also receives requests for delivery of a specific CDR/CMR file with the file name and the transfer method (SFTP/FTP, server name, login info, directory) that is specified in the request.

If you are using a third-party billing application that accesses CDR data via an HTTPS/SOAP interface, activate this service.

CAR Web Service

The Cisco CAR Web Service loads the user interface for CAR, a web-based reporting application that generates either CSV or PDF reports by using CDR data.

Security Services

This section describes the Security Services and does not apply to Cisco Unity Connection.

Cisco CTL Provider

Unified CM only: The Cisco CTL Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Cisco Unified Communications Manager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster. You must install and configure the Cisco CTL Client and activate this service for the clusterwide security mode to change from nonsecure to secure.

Unified CM BE 5000 only: The Cisco CTL Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the clusterwide security mode for the server from nonsecure to mixed mode. You must install and configure the Cisco CTL Client and activate this service for the security mode to change from nonsecure to secure.

After you activate the service, the Cisco CTL Provider service reverts to the default CTL port, which is 2444. If you want to change the port, refer to the *Cisco Unified Communications Manager Security Guide* for more information.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Certificate Authority Proxy Function (CAPF)

Working in conjunction with the CAPF application, the Cisco Certificate Authority Proxy Function (CAPF) service can perform the following tasks, depending on your configuration:

- Issue locally significant certificates to supported Cisco Unified IP Phone models.
- Using SCEP, request certificates from third-party certificate authorities on behalf of supported Cisco Unified IP Phone models.
- Upgrade existing certificates on the phones.
- Retrieve phone certificates for troubleshooting.
- Delete locally significant certificates on the phone.

Note *Unified CM only*: When you view real-time information in RTMT, the Cisco Certificate Authority Proxy Function (CAPF) service displays only for the first server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager.

Directory Services

This section describes the Directory Services.

Cisco DirSync

Cisco Unified Communications Manager Business Edition 5000: This service displays in Cisco Unified Serviceability, but the system does not save the configuration for the activation; after you attempt to activate the service, a message displays in the Service Activation window to tell you that you cannot activate this service for Cisco Unified Communications Manager Business Edition 5000.

Unified CM: The Cisco DirSync service ensures that the Cisco Unified Communications Manager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Cisco Unified Communications Manager, the Cisco DirSync service migrates the user data to the Cisco Unified Communications Manager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.

Cisco Unity Connection: When Connection is integrated with an LDAP directory, the Cisco DirSync service synchronizes a small subset of user data (first name, last name, alias, phone number, and so on) in the Cisco Unified CM database on the Connection server with the corresponding data in the LDAP directory. Another service (CuCmDbEventListener) synchronizes data in the Connection user database with data in the Cisco Unified CM database. When a Connection cluster is configured, the Cisco DirSync service runs only on the publisher server.

Voice Quality Reporter Services

This section describes the Voice Quality Reporter Services and does not apply to Cisco Unity Connection.

Cisco Extended Functions

The Cisco Extended Functions service provides support for Cisco Unified Communications Manager voice-quality features, including Quality Report Tool (QRT). For more information about individual features, refer to the *Cisco Unified Communications Manager System Guide* and the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Network Services

Installed automatically, network services include services that the system requires to function; for example, database and platform services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Call Control—Network Services window.

After the installation of your application, network services start automatically, as noted in the Call Control—Network Services window. In the Control Center—Network Services window, Cisco Unified Serviceability categorizes services into the following groups:

- Performance and Monitoring Services, page 9-10
- Backup and Restore Services, page 9-11
- System Services, page 9-11
- Platform Services, page 9-12
- Security Services, page 9-14
- DB Services, page 9-15
- SOAP Services, page 9-15
- CM Services, page 9-15
- CDR Services, page 9-7

- Admin Services, page 9-17

Performance and Monitoring Services

This section describes the Performance and Monitoring Services.

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT servlet supports the Cisco Unified Real-Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor devices, system performance, CTI applications, and so on.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco RTMT Reporter Servlet

The Cisco RTMT Reporter servlet allows you to publish reports for RTMT.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on a server (or all servers in the cluster) by using configured thresholds and a polling interval.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco Tomcat Stats Servlet

The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the Command Line Interface. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as the Cisco Unified Real-Time Monitoring Tool (RTMT), SOAP applications, and so on, to retrieve the information that is stored in the RIS server (or in all RIS servers in the cluster).

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco AMC Service

Used for the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server (or on all servers in the cluster).

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any configuration change to the Cisco Unified Communications Manager system by a user or as a result of the user action.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco RisBean Library

Cisco RisBean Library comprises a library that some webapps use to communicate with other internal services.

You should leave trace settings at default level unless you are instructed by TAC to change them to debug an issue.

Backup and Restore Services

This section describes the Backup and Restore Services.

Cisco DRF Master

The CiscoDRF Master Agent service supports the DRF Master Agent, which works with the Disaster Recovery System graphical user interface (GUI) or command line interface (CLI) to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

System Services

This section describes the System Services.

Cisco CallManager Serviceability

The Cisco CallManager Serviceability service supports Cisco Unified Serviceability, the web application/interface that you use to troubleshoot issues and manage services. This service, which is installed automatically, allows you access to the Cisco Unified Serviceability graphical user interface (GUI). If you stop this service, you cannot access the Cisco Unified Serviceability GUI when you browse into that server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco CDP

Cisco CDP advertises the voice application to other network management applications, so the network management application, for example, SNMP or CiscoWorks Lan Management Solution, can perform network management tasks for the voice application.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using RTMT. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Tip If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Platform Services

This section describes the Platform Services.

A Cisco DB

A Cisco DB service supports the Progres database engine.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

A Cisco DB Replicator

Unified CM only: The A Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent servers in the cluster.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in Cisco Unified Serviceability, you must restart the SNMP Master Agent service in the Control Center—Network Features window.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

MIB2 Agent

This service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables; for example, system, interfaces, IP, and so on.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. This service implements the HOST-RESOURCES-MIB.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Native Agent Adaptor

This service, which supports vendor MIBs, allows you to forward SNMP requests to another SNMP agent that runs on the system.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified Communications Manager or Cisco Unity Connection server. This service implements the CISCO-CDP-MIB.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco Syslog Agent

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the network. Do not stop the services unless the your technical support team tells you to do so.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date. You manage the certificates that use this service in Cisco Unified Operating System Administration.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco License Manager

This service is not supported by Cisco Unity Connection.

Cisco License Manager keeps track of the Cisco Unified Communications Manager-related licenses that a customer purchases and uses. It controls license checkins and checkouts, and it takes responsibility for issuing and reclaiming Cisco Unified Communications Manager-related licenses. For Cisco Unified Communications Manager, Cisco License Manager manages the Cisco Unified Communications Manager application and the number of IP phone unit licenses. When the number of phones exceeds the number of licenses, it issues alarms.

Unified CM clusters only: This service runs on all the servers, but the service on the first server has the responsibility for issuing and reclaiming licenses.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Tip *Unified CM BE 5000 only*: For information on issuing Cisco Unity Connection licenses, refer to the *Cisco Unified Communications Manager System Guide*.

Security Services

This section describes the Security Services.

Cisco Trust Verification Service

Cisco Trust Verification Service is a service running on a CallManager server or a dedicated server, that authenticates certificates on behalf of phones and other endpoints. It associates a list of roles for the owner of the certificate. A certificate or the owner can be associated with one or many roles.

The protocol between phones and Trust Verification Service allows phones to request for verification. Trust Verification Service validates the certificate and returns a list of roles associated with it. The protocol allows Trust Verification Service to authenticate a request and conversely, a phone to authenticate the response from Trust Verification Service. The protocol protects the integrity of the request and the response. Confidentiality of the request and the response is not required.

Multiples instances of Cisco Trust Verification Service run on different servers in the cluster to provide scalability. These servers may or may not be the same as the ones hosting the Cisco Unified CallManager. Phones obtain a list of Trust Verification Services in the network and connect to one of them using a selection algorithm (example: Round Robin). If the contacted Trust Verification Service does not respond, the phone switches to the next Trust Verification Service in the list.

DB Services

This section describes the DB Services.

Cisco Database Layer Monitor

The Cisco Database Layer Monitor service monitors aspects of the database layer. This service takes responsibility for change notification and monitoring.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

SOAP Services

This section describes the SOAP Services.

Cisco SOAP-Real-Time Service APIs

The Cisco SOAP-Real-Time Service APIs allow you to collect real-time information for devices and CTI applications. This service also provides APIs for activating, starting, and stopping services.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco SOAP-Performance Monitoring APIs

The Cisco SOAP-Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service, CPU usage, performance monitoring counters, and so on.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco SOAP-Log Collection APIs

The Cisco SOAP-Log Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, Cisco application trace files, and so on.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

CM Services

This section describes the CM Services and does not apply to Cisco Unity Connection.

Cisco CallManager Personal Directory

The Cisco CallManager Personal Directory service supports Cisco Personal Directory.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco Extension Mobility Application

The Cisco Extension Mobility Application service allows you to define login settings such as duration limits on phone configuration for the Cisco Extension Mobility feature.

Unified CM only: The Cisco Extension Mobility feature allows users within a Cisco Unified Communications Manager cluster to temporarily configure another phone in the cluster as their own phone by logging in to that other phone. After a user logs in, the phone adopts the personal phone number(s), speed dials, services links, and other user-specific properties of the user. After logout, the phone adopts the original user profile.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco CallManager Cisco IP Phone Services

The Cisco CallManager Cisco IP Phone Service initializes the service URLs for the Cisco Unified IP Phone services that you configured in Cisco Unified Communications Manager Administration.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

CDR Services

This section describes the CDR Services and does not apply to Cisco Unity Connection.

Cisco CDR Repository Manager

This service maintains and moves the generated CDRs that are obtained from the Cisco CDR Agent service. In a system that supports clusters (Cisco Unified Communications Manager only), the service exists on the first server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco CDR Agent

Note Cisco Unified Communications Manager supports Cisco CDR Agent in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 systems. This service does not support Cisco Unity Connection.

This service does not support Cisco Unity Connection.

The Cisco CDR Agent service transfers CDR and CMR files that are generated by Cisco Unified Communications Manager from the local host to the CDR repository server, where the CDR Repository Manager service runs over a SFTP connection.

This service transfers CDR and CMR files generated from the local host to the CDR repository server in a cluster. The CDR Agent in the CDR Repository Node/Standalone server (Files generated in the Standalone server itself) transfers the files to the Cisco CDR Repository Manager, over a SFTP connection, which maintains /moves the files.

For this service to work, activate the Cisco CallManager service on the server and ensure that it is running. If your configuration supports clusters (Cisco Unified Communications Manager only), activate the Cisco CallManager service on the first server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Cisco CAR Scheduler

This service does not support Cisco Unity Connection.

The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Admin Services

This section describes the Admin Services and does not apply to Cisco Unity Connection.

Cisco CallManager Admin

The Cisco CallManager Admin service supports Cisco Unified Communications Manager Administration, the web application/interface that you use to configure Cisco Unified Communications Manager settings. After the Cisco Unified Communications Manager installation, this service starts automatically and allows you to access the graphical user interface (GUI). If you stop this service, you cannot access the Cisco Unified Communications Manager Administration graphical user interface when you browse into that server.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

Service Activation

You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in Cisco Unified Serviceability.

Note Starting with Cisco Unified Communications Manager Release 6.1.1, end users can no longer access Cisco Unified Serviceability to start and stop services.

Cisco Unified Serviceability activates feature services in automatic mode and checks for service dependencies. When you choose to activate a feature service, Cisco Unified Serviceability prompts you to select all the other services, if any, that depend on that service to run. When you click the Set Default button, Cisco Unified Serviceability chooses those services that are required to run on the server.

Unified CM only: Even in a configuration that supports clusters, this process is based on a single-server configuration.

Activating a service automatically starts the service. You start/stop services from Control Center.

Control Center

From Control Center in Cisco Unified Serviceability, you can view status and start and stop one service at a time. In a cluster configuration (Cisco Unified Communications Manager only), you can perform these functions for one server in the cluster. To perform these tasks, Cisco Unified Serviceability provides two Control Center windows. To start, stop, and restart network services, access the Control Center—Network Services window. To start, stop, and restart feature services, access the Control Center—Feature Services window.

Tip Use the Related Links drop-down list box and the Go button to navigate to Control Center and Service Activation windows.

Unified CM only: Starting and stopping a feature service causes all Cisco Unified IP Phones and gateways that are currently registered to that service to fail over to their secondary service. Devices and phones need to restart only if they cannot register with their secondary service. Starting and stopping a service may cause other installed applications (such as a conference bridge or Cisco Messaging Interface) that are homed to that Cisco Unified Communications Manager to start and stop as well.

Caution *Unified CM and Unified CM BE 5000 only*: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, but other types of calls drop.

Services Configuration Checklist

Table 9-1 lists the steps for working with services.

Table 9-1 Services Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate the feature services that you want to run.	• Feature Services, page 9-1 • Activating and Deactivating Feature Services, page 11-1
Step 2	Configure the appropriate service parameters.	• *Unified CM and Unified CM BE 5000 only*: All service parameters for the services in Cisco Unified Serviceability display in Cisco Unified Communications Manager Administration. For service parameter configuration, see the *Cisco Unified Communications Manager Administration Guide*. • *Connection only*: You configure service parameters in Cisco Unity Connection Administration. For service parameter configuration, see the *System Administration Guide for Cisco Unity Connection.*
Step 3	If necessary, troubleshoot problems by using the Cisco Unified Serviceability trace tools.	• Configuring Trace, page 7-1 • *Cisco Unified Real-Time Monitoring Tool Administration Guide*

Where to Find More Information

Related Topics

- Control Center, page 9-17
- Feature Services, page 9-1
- Network Services, page 9-9

Additional Cisco Documentation

- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager System Guide*
- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Administration Guide*
- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Features and Services Guide*
- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Security Guide*
- *Unified CM and Unified CM BE 5000 only*: *Troubleshooting Guide for Cisco Unified Communications Manager*
- *Unified CM BE 5000 and Connection only*: *Administration Guide for Cisco Unity Connection Serviceability*
- *Connection only*: *System Administration Guide for Cisco Unity Connection*
- *Command Line Interface Reference Guide for Cisco Unified Solutions*

CHAPTER 10

Understanding Serviceability Reports Archive

The Cisco Serviceability Reporter service generates daily reports in Cisco Unified Serviceability. Each report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

The following sections provide additional information, including detailed information about each report that Serviceability Reporter generates:

Note *Unified CM clusters only*: Because the Cisco Serviceability Reporter is only active on the first server, at any time, Reporter generates reports only on the first server, not the other servers.

You view reports from **Cisco Unified Serviceability > Tools > Serviceability Reports Archive**. You must activate the Cisco Serviceability Reporter service before you can view reports. After you activate the service, report generation may take up to 24 hours.

The reports contain 24-hour data for the previous day. A suffix that is added to the report names shows the date for which Reporter generated them; for example, AlertRep_mm_dd_yyyy.pdf. The Serviceability Reports Archive window uses this date to display the reports for the relevant date only. The reports generate from the data that is present in the log files, with the timestamp for the previous day. The system considers log files for the current date and the previous two days for collecting data. For cluster configurations (Cisco Unified Communications Manager only), this takes into account the time zone differences between the server locations.

The time that is shown in the report reflects the server “System Time.” In cluster configurations (Cisco Unified Communications Manager only), the time that is shown in the report reflects the first server “System Time.” If the first server and subsequent server(s) are in different time zones, the first server “System Time” shows in the report.

Note You can pick up log files from the server while you are generating reports, or in a cluster configuration (Cisco Unified Communications Manager only), from all servers in the cluster.

Note The Cisco Unified Reporting web application provides snapshot views of data into one output and runs data checks. In a cluster configuration (Cisco Unified Communications Manager only), this includes cluster data from all accessible servers. The application also allows you to archive generated reports. See the *Cisco Unified Reporting Administration Guide* for more information.

Serviceability Reporter Service Parameters

Cisco Serviceability Reporter uses the following service parameters:

- RTMT Reporter Designated Node—Specifies the designated node on which RTMT Reporter runs. This default equals the IP address of the server on which the Cisco Serviceability Reporter service is first activated.

  Unified CM only: Because the Serviceability Reporter service is CPU intensive, Cisco recommends that you specify a non-call processing node.
- Report Generation Time—Specifies the number of minutes after midnight. Reports generate at this time for the most recent day. The minimum value equals 0 and the maximum value equals 1439.
- Report Deletion Age—Specifies the number of days that the report must be kept on the disk. The system deletes reports that are older than the specified age. The minimum value equals 0, and the maximum value equals 30.

Tip You can disable reports by setting the service parameter Report Deletion Age to a value of 0.

For more information about service parameter configuration, refer to the following guides:

- *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Administration Guide*
- *Connection only*: *System Administration Guide for Cisco Unity Connection*

Note *Unified CM only*: If a node gets removed completely from the network (the node should be removed from the network and also from the list of servers in Cisco Unified Communications Manager Administration), Reporter does not consider this node while it is generating reports, even if the log file contains the data for that node.

Device Statistics Report

The Device Statistics Report does not apply to Cisco Unity Connection.

The Device Statistics Report provides the following line charts:

- Number of Registered Phones per Server, page 10-3
- Number of H.323 Gateways in the Cluster, page 10-4

- Number of Trunks in the Cluster, page 10-4

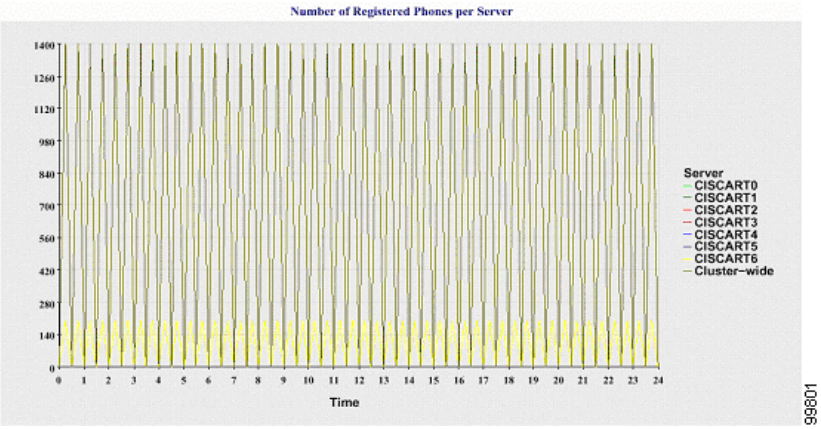
In a Cisco Unified Communications Manager Business Edition 5000 system, the Device Statistics Report supports Cisco Unified Communications Manager only.

Number of Registered Phones per Server

A line chart displays the number of registered phones for each Cisco Unified Communications Manager server (and cluster in a Cisco Unified Communications Manager cluster configuration). Each line in the chart represents the data for a server for which data is available, and one extra line displays the clusterwide data (Cisco Unified Communications Manager clusters only). Each data value in the chart represents the average number of phones that are registered for a 15-minute duration. If a server shows no data, Reporter does not generate the line that represents that server. If no data exists for the server (or for all servers in a Cisco Unified Communications Manager cluster configuration), for registered phones, Reporter does not generate the chart. The message "No data for Device Statistics report available" displays.

Figure 10-1 shows an example of a line chart that represents the number of registered phones per Cisco Unified Communications Manager server in a Cisco Unified Communications Manager cluster configuration.

Figure 10-1 Line Chart That Depicts Number of Registered Phones Per Server

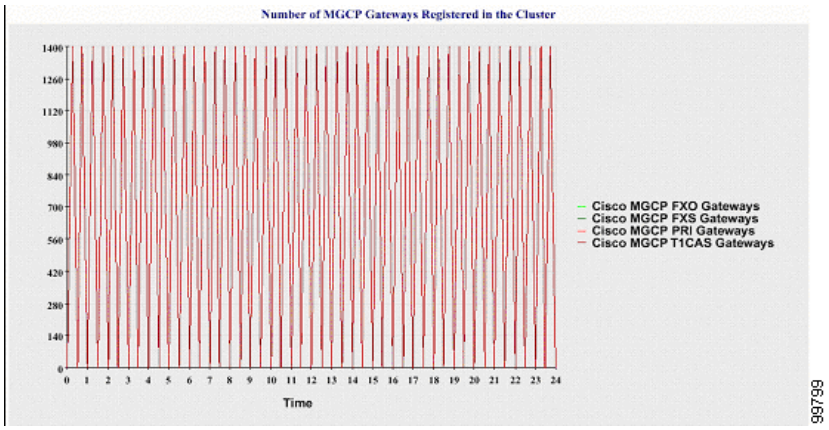


Number of MGCP Gateways Registered in the Cluster

A line chart displays the number of registered MGCP FXO, FXS, PRI, and T1CAS gateways. Each line represents data only for the Cisco Unified Communications Manager server (or cluster in a Cisco Unified Communications Manager cluster configuration); so, four lines show server (or clusterwide) details for each gateway type. Each data value in the chart represents the average number of MGCP gateways that are registered for a 15-minute duration. If no data exists for a gateway for the server (or all the servers in a cluster), Reporter does not generate the line that represents data for that particular gateway. If no data exists for all gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

Figure 10-2 shows an example of a line chart that represents the number of registered gateways per cluster, in a Cisco Unified Communications Manager cluster configuration.

Figure 10-2 Line Chart That Depicts Number of Registered Gateways Per Cluster

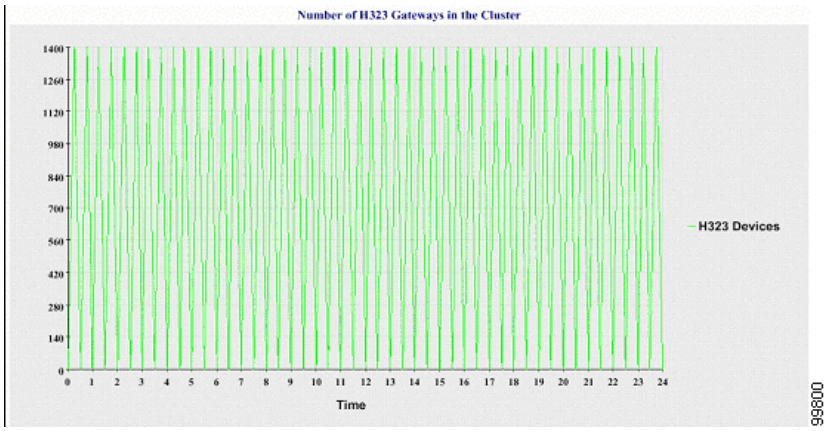


Number of H.323 Gateways in the Cluster

A line chart displays the number of H.323 gateways. One line represents the details of the H.323 gateways (or the clusterwide details in a Cisco Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 gateways for a 15-minute duration. If no data exists for H.323 gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

Figure 10-3 shows an example line chart that represents the number of H.323 gateways per cluster in a Cisco Unified Communications Manager cluster configuration.

Figure 10-3 Line Chart That Depicts Number of Registered H.323 Gateways Per Cluster

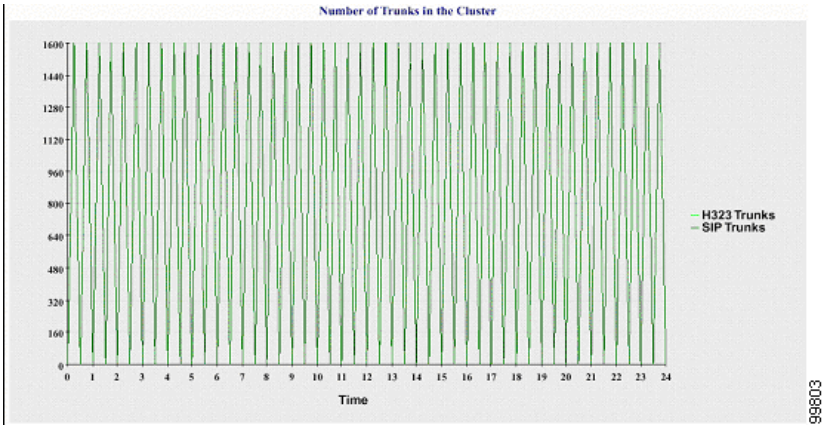


Number of Trunks in the Cluster

A line chart displays the number of H.323 and SIP trunks. Two lines represent the details of the H.323 trunks and SIP trunks (or the clusterwide details in a Cisco Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 and SIP trunks for a 15-minute duration. If no data exists for H.323 trunks for the server (or for all servers in a cluster), Reporter does not generate the line that represents data for the H.323 trunks. If no data exists for SIP trunks for the server (or for all servers in the cluster), Reporter does not generate the line that represents data for SIP trunks. If no data exists for trunks at all, Reporter does not generate the chart.

Figure 10-4 shows an example line chart that represents the number of trunks per cluster in a Cisco Unified Communications Manager cluster configuration.

Figure 10-4 Line Chart That Depicts Number of Trunks Per Cluster



The server (or each server in the cluster) contains log files that match the file name pattern DeviceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Number of registered phones on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of registered MGCP FXO, FXS, PRI, and T1CAS gateways on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of registered H.323 gateways on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of SIP trunks and H.323 trunks

Server Statistics Report

The Server Statistics Report provides the following line charts:

- Percentage of CPU per Server, page 10-5
- Percentage of Memory Usage per Server, page 10-6
- Percentage of Hard Disk Usage of the Largest Partition per Server, page 10-7

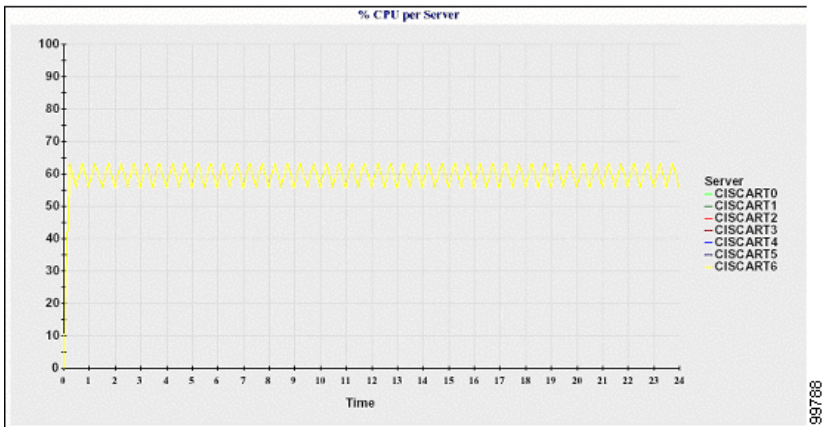
In a Cisco Unified Communications Manager Business Edition 5000 system, the Server Statistics Report supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Percentage of CPU per Server

A line chart displays the percentage of CPU usage for the server (or for each server in a Cisco Unified Communications Manager cluster). The line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster) for which data is available. Each data value in the chart represents the average CPU usage for a 15-minute duration. If no data exists for the server (or for any one server in a Cisco Unified Communications Manager cluster), Reporter does not generate the line that represents that server. If there are no lines to generate, Reporter does not create the chart. The message “No data for Server Statistics report available” displays.

Figure 10-5 shows a line chart example that represents the percentage of CPU usage per server in a Cisco Unified Communications Manager cluster configuration.

Figure 10-5 Line Chart That Depicts the Percentage of CPU Per Server

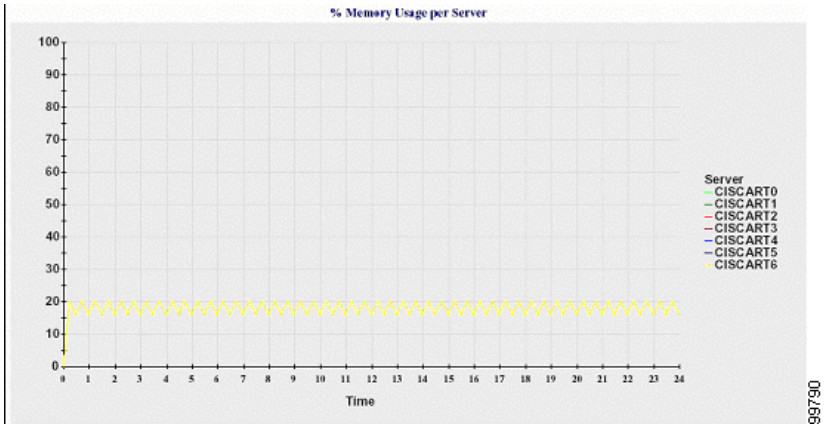


Percentage of Memory Usage per Server

A line chart displays the percentage of Memory Usage for the Cisco Unified Communications Manager server (%MemoryInUse). In a Cisco Unified Communications Manager cluster configuration, there is one line per server in the cluster for which data is available. Each data value in the chart represents the average memory usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 10-6 shows a line chart example that represents the percentage of memory usage per Cisco Unified Communications Manager server in a Cisco Unified Communications Manager cluster configuration.

Figure 10-6 Line Chart That Depicts Percentage of Memory Usage Per Server

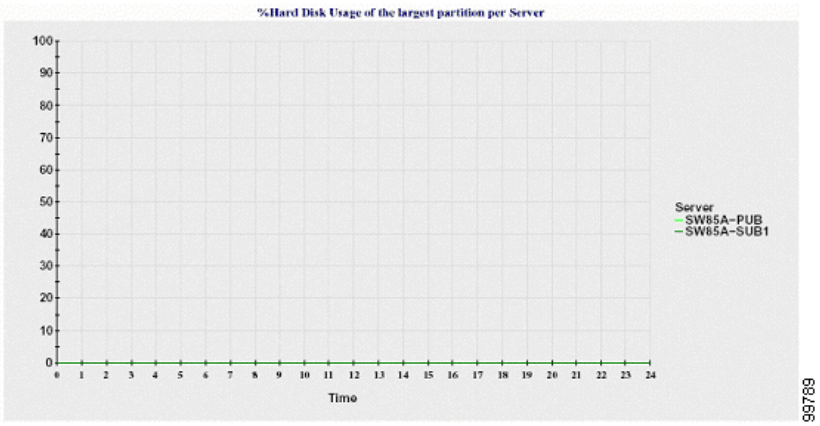


Percentage of Hard Disk Usage of the Largest Partition per Server

A line chart displays the percentage of disk space usage for the largest partition on the server (%DiskSpaceInUse), or on each server in a Cisco Unified Communications Manager cluster configuration. Each data value in the chart represents the average disk usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a cluster configuration, Reporter does not generate the line that represents that server.

Figure 10-7 shows a line chart example that represents the percentage of hard disk usage for the largest partition per server in a Cisco Unified Communications Manager cluster configuration.

Figure 10-7 Line Chart That Depicts Percentage of Hard Disk Usage of the Largest Partition Per Server



The server (or each server in a Cisco Unified Communications Manager cluster configuration) contains log files that match the file name pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- % CPU usage on the server (or each server in a Cisco Unified Communications Manager cluster)
- % Memory usage (%MemoryInUse) on the server (or on each server in a Cisco Unified Communications Manager cluster)
- % Hard disk usage of the largest partition (%DiskSpaceInUse) on the server (or on each server in a Cisco Unified Communications Manager cluster)

Service Statistics Report

The Service Statistics Report does not support Cisco Unity Connection.

The Service Statistics Report provides the following line charts:

- Cisco CTI Manager: Number of Open Devices, page 10-8
- Cisco CTI Manager: Number of Open Lines, page 10-8
- Cisco TFTP: Number of Requests, page 10-9
- Cisco TFTP: Number of Aborted Requests, page 10-9

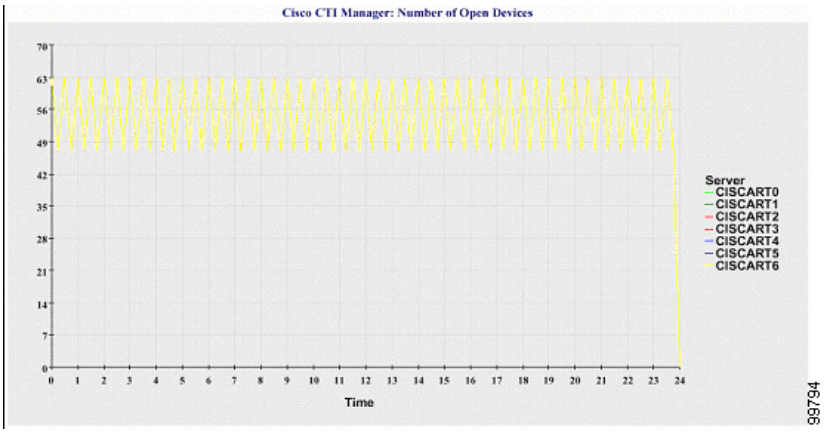
In a Cisco Unified Communications Manager Business Edition 5000 system, the Service Statistics Report supports Cisco Unified Communications Manager only.

Cisco CTI Manager: Number of Open Devices

A line chart displays the number of CTI Open Devices for the CTI Manager (or for each CTI Manager in a Cisco Unified Communications Manager cluster configuration). Each line chart represents the data for the server (or on each server in a Cisco Unified Communications Manager cluster) on which service is activated. Each data value in the chart represents the average number of CTI open devices for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server. The message "No data for Service Statistics report available" displays.

Figure 10-8 shows a line chart example that represents the number of open devices per Cisco CTI Manager in a Cisco Unified Communications Manager cluster configuration.

Figure 10-8 Line Chart That Depicts Cisco CTI Manager: Number of Open Devices

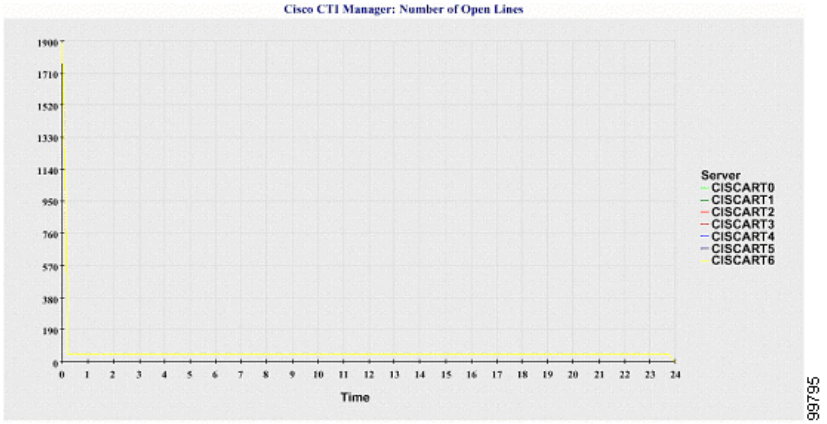


Cisco CTI Manager: Number of Open Lines

A line chart displays the number of CTI open lines for the CTI Manager (or per CTI Manager in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster configuration) where the Cisco CTI Manager service is activated. Each data value in the chart represents the average number of CTI open lines for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 10-9 shows a line chart example that represents the number of open lines per Cisco CTI Manager in a Cisco Unified Communications Manager cluster configuration.

Figure 10-9 Line Chart That Depicts Cisco CTI Manager: Number of Open Lines

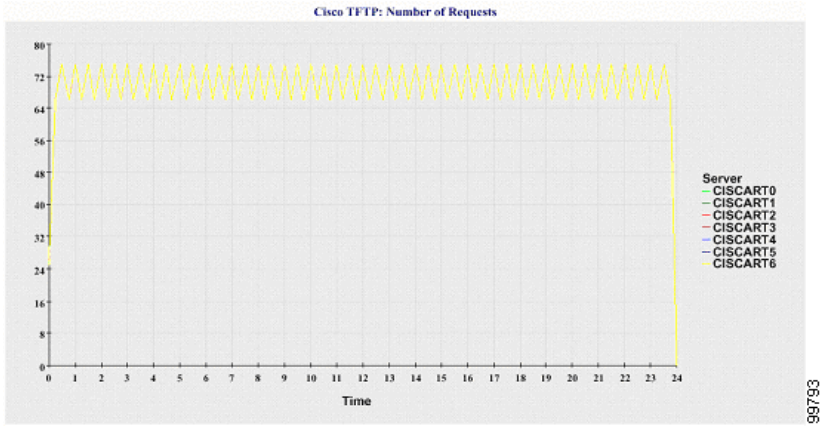


Cisco TFTP: Number of Requests

A line chart displays the number of Cisco TFTP requests for the TFTP server (or per TFTP server in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the average number of TFTP requests for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 10-10 shows a line chart example that represents the number of Cisco TFTP requests per TFTP server.

Figure 10-10 Line Chart That Depicts Cisco TFTP: Number of Requests



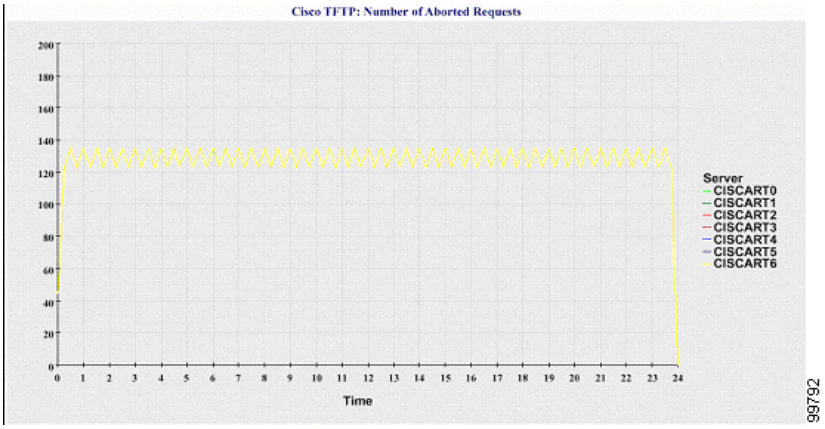
Cisco TFTP: Number of Aborted Requests

A line chart displays the number of Cisco TFTP requests that were aborted for the TFTP server (or per TFTP server in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the

average of TFTP requests that were aborted for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 10-11 shows a line chart example that represents the number of Cisco TFTP requests that were aborted per TFTP server.

Figure 10-11 Line Chart That Depicts Cisco TFTP: Number of Aborted Requests



The server (or each server in a Cisco Unified Communications Manager cluster) contains log files that match the file name pattern ServiceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- For each CTI Manager - Number of open devices
- For each CTI Manager - Number of open lines
- For each Cisco TFTP server - TotalTftpRequests
- For each Cisco TFTP server - TotalTftpRequestsAborted

Call Activities Report

The Call Activities Report does not support Cisco Unity Connection.

The Call Activities Report provides the following line charts:

- Cisco Unified Communications Manager Call Activity for the Cluster, page 10-10
- H.323 Gateways Call Activity for the Cluster, page 10-11
- MGCP Gateways Call Activity for the Cluster, page 10-12
- MGCP Gateways, page 10-12
- Trunk Call Activity for the Cluster, page 10-13

In a Cisco Unified Communications Manager Business Edition 5000 system, the Server Statistics Report supports Cisco Unified Communications Manager only.

Cisco Unified Communications Manager Call Activity for the Cluster

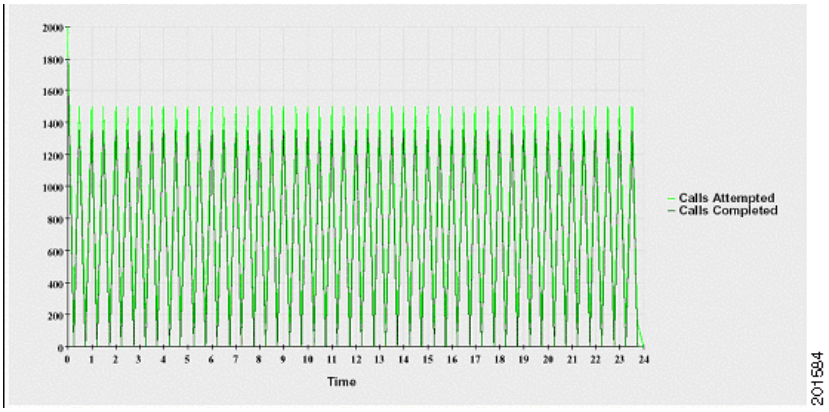
A line chart displays the number of Cisco Unified Communications Manager calls that were attempted and calls that were completed. In a Cisco Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart

comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration.

If no data exists for Cisco Unified Communications Manager calls that were completed, Reporter does not generate the line that represents data for the calls that were completed. If no data exists for Cisco Unified Communications Manager calls that were attempted, Reporter does not generate the line that represents data for the calls that were attempted. In a Cisco Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for Cisco Unified Communications Manager call activities at all, Reporter does not generate the chart. The message "No data for Call Activities report available" displays.

Figure 10-12 shows a line chart example that represents the number of attempted and completed calls for a Cisco Unified Communications Manager cluster.

Figure 10-12 Line Chart That Depicts Cisco Unified Communications Manager Call Activity for a Cluster

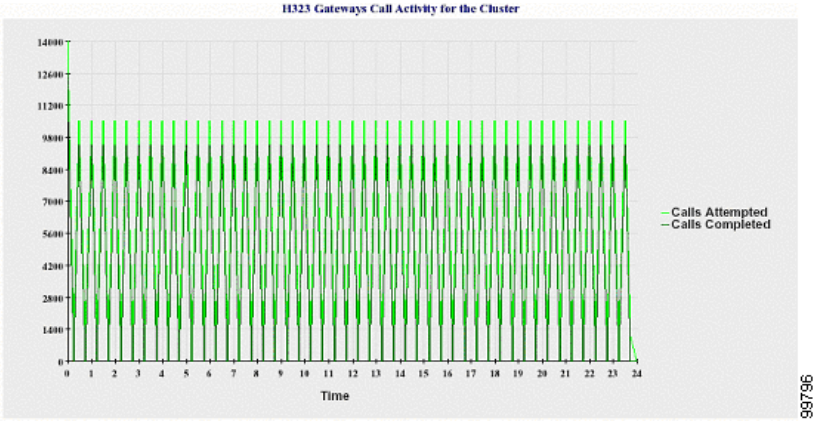


H.323 Gateways Call Activity for the Cluster

A line chart displays the number of calls that were attempted and calls that were completed for H.323 gateways. In a Cisco Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which equals the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration. If no data exists for H.323 gateways calls that were completed, Reporter does not generate the line that represents data for calls that were completed. If no data exists for H.323 gateways calls that were attempted, Reporter does not generate the line that represents data for calls that were attempted. In a Cisco Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for H.323 gateways call activities at all, Reporter does not generate the chart.

Figure 10-13 shows a line chart example that represents the H.323 gateway call activity for a Cisco Unified Communications Manager cluster.

Figure 10-13 Line Chart That Depicts H.323 Gateways Call Activity for the Cluster

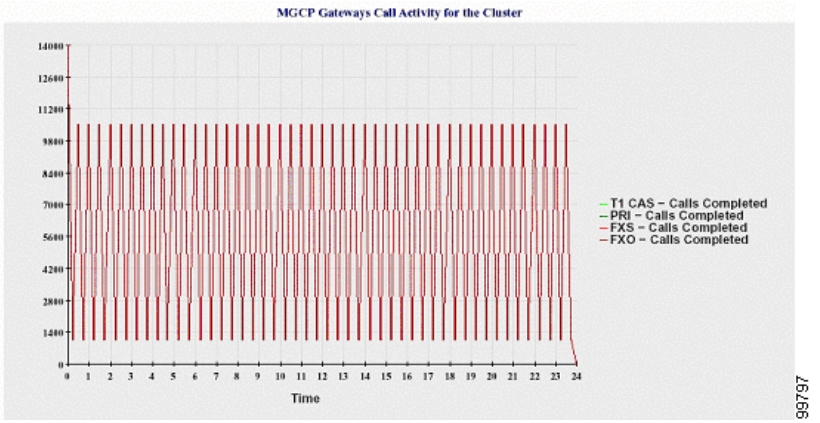


MGCP Gateways Call Activity for the Cluster

A line chart displays the number of calls that were completed in an hour for MGCP FXO, FXS, PRI, and T1CAS gateways. In a Cisco Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed for the entire Cisco Unified Communications Manager cluster. The chart comprises four lines at the most, one for the number of calls that were completed for each of the gateway types (for which data is available). Each data value in the chart represents the total number of calls that were completed for a 15-minute duration. If no data exists for a gateway, Reporter does not generate the line that represents data for calls that were completed for a particular gateway. If no data exists for all gateways, Reporter does not generate the chart.

Figure 10-14 shows a line chart example that represents the MGCP gateways call activity for a Cisco Unified Communications Manager cluster.

Figure 10-14 Line Chart That Depicts MGCP Gateways Call Activity for the Cluster



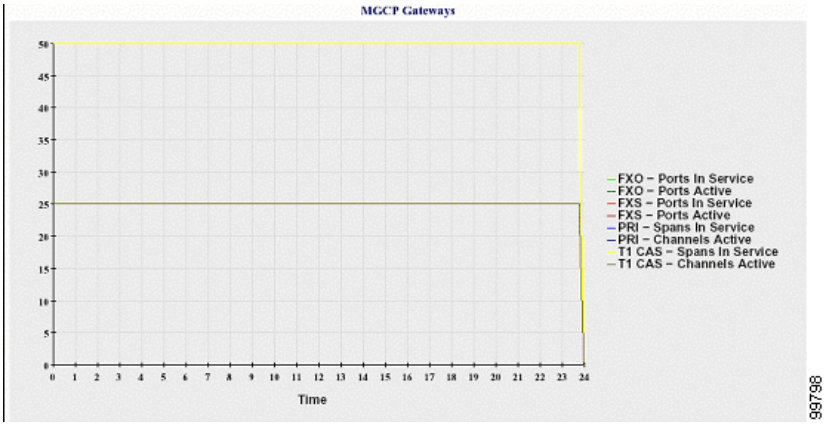
MGCP Gateways

A line chart displays the number of Ports In Service and Active Ports for MGCP FXO, FXS gateways and the number of Spans In Service or Channels Active for PRI, T1CAS gateways. For a Cisco Unified Communications Manager cluster configuration, the chart displays the data for the entire Cisco Unified Communications Manager cluster. The chart comprises eight lines, two lines each for the number of

Ports In Service for MGCP FXO and FXS, and two lines each for the number of Active Ports for MGCP FXO and FXS. Four more lines for the number of Spans In Service and Channels Active for PRI and T1CAS gateways exist. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all servers in the cluster (for which data is available). Each data value in the chart represents the total Number of Ports In Service, Number of Active Ports, Spans In Service or Channels Active for a 15-minute duration. If no data exists for the number of Spans In Service or the Channels Active for a gateway (MGCP PRI, T1CAS) for all servers, Reporter does not generate the line that represents data for that particular gateway.

Figure 10-15 shows a line chart example that represents the MGCP gateways.

Figure 10-15 Line Chart That Depicts MGCP Gateways

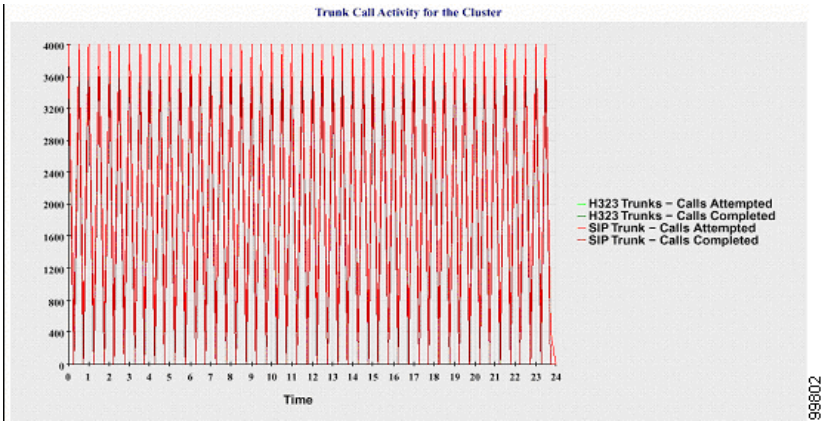


Trunk Call Activity for the Cluster

A line chart displays the number of calls that were completed and calls that were attempted in an hour for SIP trunk and H.323 trunk. For a Cisco Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed and calls that were attempted for the entire Cisco Unified Communications Manager cluster. The chart comprises four lines, two for the number of calls that were completed for each SIP and H.323 trunk (for which data is available) and two for the number of calls that were attempted. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all nodes in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were completed or number of calls that were attempted for a 15-minute duration. If no data exists for a trunk, Reporter does not generate the line that represents data for the calls that were completed or the calls that were attempted for that particular trunk. If no data exists for both trunk types, Reporter does not generate the chart.

Figure 10-16 shows a line chart example that represents the trunk call activity for a Cisco Unified Communications Manager cluster.

Figure 10-16 Line Chart That Depicts Trunk Call Activity for the Cluster



The server (or each server in a Cisco Unified Communications Manager cluster configuration) contains log files that match the file name pattern CallLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Calls that were attempted and calls that were completed for Cisco Unified Communications Manager (or for each server in a Cisco Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for the H.323 gateways (or for the gateways in each server in a Cisco Unified Communications Manager cluster)
- Calls that were completed for the MGCP FXO, FXS, PRI, and T1CAS gateways (or for the gateways in each server in a Cisco Unified Communications Manager cluster)
- Ports in service, active ports for MGCP FXO and FXS gateways and spans in service, channels active for PRI, and T1CAS gateways (in each server in a Cisco Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for H.323 trunks and SIP trunks

Alert Summary Report

The Alert Summary Report provides the details of alerts that are generated for the day. The Alert report comprises the following charts:

- Number of Alerts per Server, page 10-14
- Number of Alerts per Severity for the Cluster, page 10-15
- Top 10 Alerts in the Cluster, page 10-16

In a Cisco Unified Communications Manager Business Edition 5000 system, the Server Statistics Report supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Number of Alerts per Server

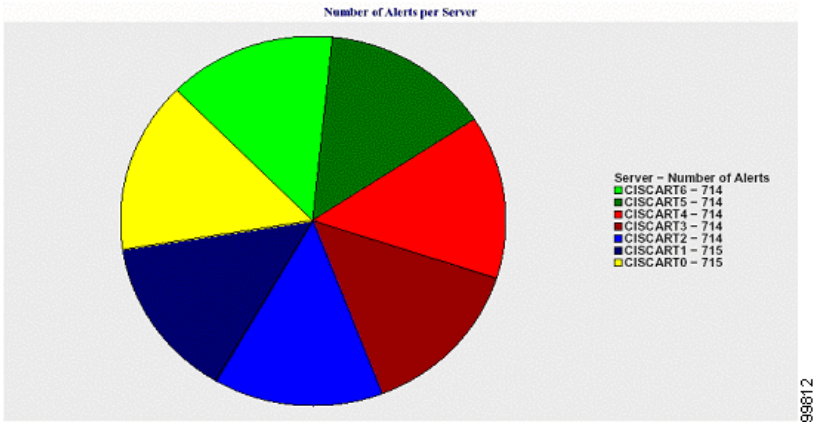
Unified CM only: A pie chart provides the number of alerts per Cisco Unified Communications Manager node. The chart displays the serverwide details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated for a particular server in the Cisco Unified Communications Manager cluster. The chart includes as many number of sectors as there are servers (for

which Reporter generates alerts in the day) in the cluster. If no data exists for a server, no sector in the chart represents that server. If no data exists for all servers, Reporter does not generate the chart. The message "No alerts were generated for the day" displays.

Unified CM BE 5000 and Connection only: A pie chart provides the number of alerts for the server. The chart displays the serverwide details of the alerts that are generated. If no data exists for the server, Reporter does not generate the chart. The message "No alerts were generated for the day" displays.

Figure 10-17 shows a pie chart example that represents the number of alerts per server in a Cisco Unified Communications Manager cluster.

Figure 10-17 Pie Chart That Depicts Number of Alerts Per Server

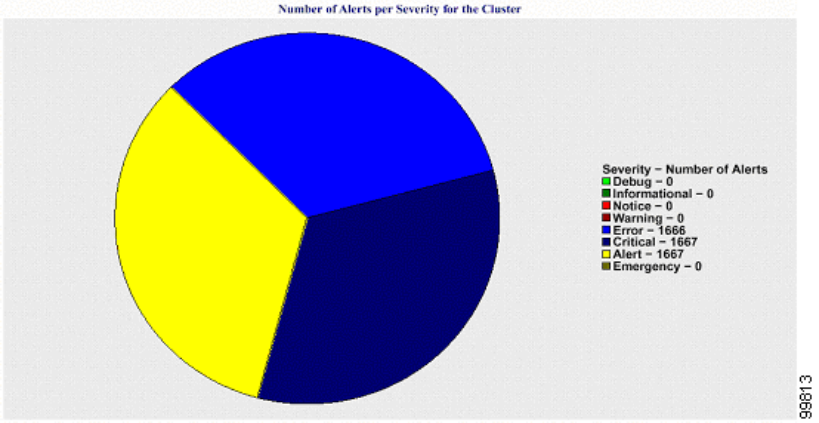


Number of Alerts per Severity for the Cluster

A pie chart displays the number of alerts per alert severity. The chart displays the severity details of the alerts that are generated. Each sector of the pie chart represents the number of alerts that are generated of a particular severity type. The chart provides as many number of sectors as there are severities (for which Reporter generates alerts in the day). If no data exists for a severity, no sector in the chart represents that severity. If no data exists, Reporter does not generate the chart.

Figure 10-18 shows a pie chart example that represents the number of alerts per severity for a Cisco Unified Communications Manager cluster.

Figure 10-18 Pie Chart That Depicts Number of Alerts Per Severity for the Cluster

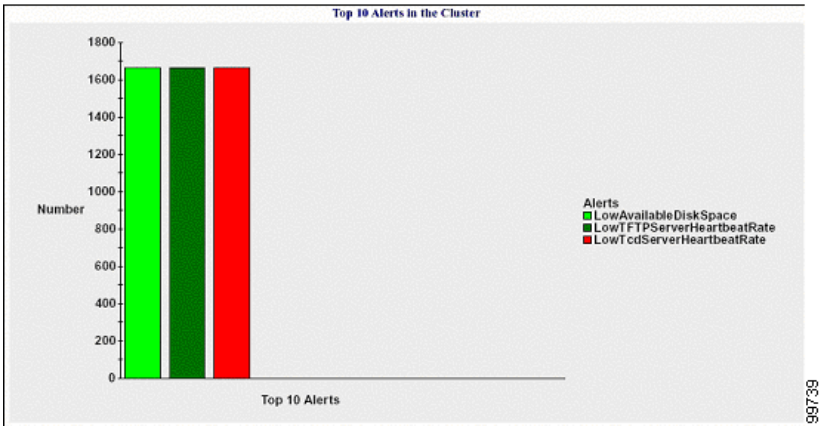


Top 10 Alerts in the Cluster

A bar chart displays the number of alerts of a particular Alert Type. The chart displays the details of the alerts that are generated on the basis of the alert type. Each bar represents the number of alerts for an alert type. The chart displays details only for the first 10 alerts based on the highest number of alerts in descending order. If no data exists for a particular alert type, no bar represents that alert. If no data exists for any alert type, RTMT does not generate the chart.

Figure 10-19 shows a bar chart example that represents the top 10 alerts in a Cisco Unified Communications Manager cluster.

Figure 10-19 Bar Chart That Depicts Top 10 Alerts in the Cluster



The server (or each server in a Cisco Unified Communications Manager cluster) contains log files that match the file name pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Time—Time at which the alert occurred
- Alert Name—Descriptive name
- Node Name—Server on which the alert occurred
- Monitored object—The object that is monitored

- Severity—Severity of this alert

Performance Protection Report

The Performance Protection Report does not apply to Cisco Unity Connection.

The Performance Protection Report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

The Performance Protection Report provides trend analysis information on default monitoring objects for the last seven that allows you to track information about Cisco Intercompany Media Engine. The report includes the Cisco IME Client Call Activity chart that shows the total calls and fallback call ratio for the Cisco IME client.

The Performance Protection report comprises the following charts:

- Cisco Unified Communications Manager Call Activity, page 10-17
- Number of registered phones and MGCP gateways, page 10-17
- System Resource Utilization, page 10-17
- Device and Dial Plan Quantities, page 10-18

For a Cisco Unified Communications Manager Business Edition 5000 system, the Server Statistics Report supports Cisco Unified Communications Manager only.

Cisco Unified Communications Manager Call Activity

A line chart displays the hourly rate of increase or decrease for number of calls that were attempted and calls that were completed as the number of active calls. For a Cisco Unified Communications Manager cluster configuration, the data is charted for each server in the cluster. The chart comprises three lines, one for the number of calls that were attempted, one for the calls that were completed, and one for the active calls. If no data exists for call activity, Reporter does not generate the chart.

Number of registered phones and MGCP gateways

A line chart displays the number of registered phones and MGCP gateways. For a Cisco Unified Communications Manager cluster configuration, the chart displays the data for each server in the cluster.The chart comprises two lines, one for the number of registered phones and another for the number of MGCP gateways. If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

System Resource Utilization

A line chart displays the CPU load percentage and the percentage of memory that is used (in bytes) for the server (or for the whole cluster in a Cisco Unified Communications Manager cluster configuration). The chart comprises two lines, one for the CPU load and one for the memory usage. In a Cisco Unified Communications Manager cluster, each line represents the cluster value, which is the average of the values for all the servers in the cluster (for which data is available). If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

Device and Dial Plan Quantities

Two tables display information from the Cisco Unified Communications Manager database about the numbers of devices and number of dial plan components. The device table shows the number of IP phones, Unity connection ports, H.323 clients, H.323 gateways, MGCP gateways, MOH resources, and MTP resources. The dial plan table shows the number of directory numbers and lines, route patterns, and translation patterns.

Serviceability Reports Archive Configuration Checklist

Table 10-1 provides a configuration checklist for configuring the serviceability report archive feature.

Table 10-1 Serviceability Reports Archive Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Activate the Cisco Serviceability Reporter service.	Activating and Deactivating Feature Services, page 11-1
Step 2	Configure the Cisco Serviceability Reporter service parameters.	• *Unified CM and Unified CM BE 5000 only*: *Cisco Unified Communications Manager Administration Guide* • *Connection only*: *System Administration Guide for Cisco Unity Connection* • Serviceability Reporter Service Parameters, page 10-2
Step 3	View the reports that the Cisco Serviceability Reporter service generates.	Configuring Serviceability Reports Archive, page 12-1

Where to Find More Information

Related Topics

- Configuring Serviceability Reports Archive, page 12-1

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Reporting Administration Guide*

CHAPTER 11

Configuring Services

This chapter contains information on the following topics:

Activating and Deactivating Feature Services

You activate and deactivate feature services in the Service Activation window in Cisco Unified Serviceability. Services that display in the Service Activation window do not start until you activate them.

Cisco Unified Serviceability allows you to activate and deactivate only features services (not network services). You may activate or deactivate as many services as you want at the same time. Some feature services depend on other services, and the dependent services get activated before the feature service activates.

Tip *Unified CM only*: Before you activate services in the Service Activation window, review Table 11-1.

To activate or deactivate feature services in Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 Choose **Tools > Service Activation**.

The Service Activation window displays.

Step 2 From the Server drop-down list box, choose the server where you want to activate the service; then, click **Go**.

For the server that you chose, the window displays the service names and the activation status of the services.

Step 3 To activate all services in the Service Activation window, check the **Check All Services** check box.

Step 4 You can choose all services that are required to run on a single server by clicking the Set Default button. This action not only chooses all required services but also checks for service dependencies. To activate services for a single-server configuration, click the **Set Default** button or activate the services that you want to use.

Step 5 *Unified CM only*: For a cluster configuration, review Table 11-1 for service activation recommendations; then, check the check boxes next to the services that you want to activate.

Step 6 After you check the check boxes for the services that you want to activate, click **Save**.

Tip To deactivate services that you activated, uncheck the check boxes next to the services that you want to deactivate; then, click **Save**.

To obtain the latest status of the services, click the **Refresh** button.

Additional Information

See the "Related Topics" section on page 11-6.

Cluster Service Activation Recommendations

This section does not apply to Cisco Unified Communications Manager Business Edition 5000 or Cisco Unity Connection.

Before you activate services in a cluster, review Table 11-1, which provides service recommendations for multiserver configurations.

Table 11-1 Service Activation Recommendations

Service/Servlet	Activation Recommendations
CM Services	
Cisco CallManager	This service supports Cisco Unified Communications Manager. In the Control Center—Network Services, ensure that the Cisco RIS Data Collector service and Database Layer Monitor service are running on the node. **Tip** Before you activate this service, verify that the Cisco Unified Communications Manager server displays in the Cisco Unified Communications Manager Find/List window in Cisco Unified Communications Manager Administration. If the server does not display, add the Cisco Unified Communications Manager server before you activate this service. For information on how to add the Cisco Unified Communications Manager server, refer to the *Cisco Unified Communications Manager Administration Guide*.
Cisco TFTP	If you have more than one node in the cluster, activate this service on one node that is dedicated specifically for the Cisco TFTP service. Configure Option 150 if you activate this service on more than one node in the cluster.
Cisco Messaging Interface	Activate on only one node in the cluster. Do not activate this service if you plan to use Cisco Unity voice-messaging system.

Table 11-1 Service Activation Recommendations (continued)

Service/Servlet	Activation Recommendations
Cisco Unified Mobile Voice Access Service	For mobile voice access to work, you must activate this service on the first node in the cluster after you configure the H.323 gateway to point to the first VXML page. In addition, make sure that the Cisco CallManager and the Cisco TFTP services run on one server in the cluster, not necessarily the same server where the Cisco Unified Mobile Voice Access Service runs.
Cisco IP Voice Media Streaming App	If you have more than one node in the cluster, activate on one or two servers per cluster. You may activate on a node that is dedicated specifically for music on hold. This service requires that you activate Cisco TFTP on one node in the cluster. Do not activate this service on the first node or on any nodes that run the Cisco CallManager service.
Cisco CTIManager	Activate on each node to which JTAPI/TAPI applications will connect. CTIManager activation requires the Cisco CallManager service also to be activated on the node. See the "Cisco CallManager" section on page 9-4 for more information on CTIManager and Cisco CallManager services interaction.
Cisco Extension Mobility	Activate on all nodes in the cluster.
Cisco Extended Functions	Activate this service, which supports the Quality Report Tool (QRT), on one or more servers that run the Cisco RIS Data Collector. Make sure that you activate the Cisco CTIManager service on a node in the cluster.
Cisco Dialed Number Analyzer	If you are planning to use Cisco Unified Communications Manager Dialed Number Analyzer, activate this service. This service may consume a lot of resources, so only activate this service on the node with the least amount of call-processing activity or during off-peak hours.
Cisco Dialed Number Analyzer Server	If you have more than one node in the cluster, activate this service on one node that is dedicated specifically for the Cisco Dialed Number Analyzer service.
Cisco DHCP Monitor Service	When the DHCP Monitor service is enabled, it detects changes in the database that affect IP addresses for the IP phones, modifies the /etc/dhcpd.conf file, and stops and restarts the DHCPD daemon with the updated configuration file. Activate this service on the node that has DHCP enabled.
CTI Services	
Cisco IP Manager Assistant	If you are planning to use Cisco Unified Communications Manager Assistant, activate this service on any two servers (Primary and Backup) in the cluster. Ensure that Cisco CTI Manager service is activated in the cluster. Refer to *Cisco Unified Communications Manager Features and Services Guide* for other recommendations.
Cisco WebDialer Web Service	Activate on one node per cluster.
CDR Services	
Cisco SOAP-CDROnDemand Service	You can activate the Cisco SOAP-CDROnDemand Service only on the first server, and it requires that the Cisco CDR Repository Manager and Cisco CDR Agent services are running on the same server.

Table 11-1 Service Activation Recommendations (continued)

Service/Servlet	Activation Recommendations
Cisco CAR Web Service	You can activate the Cisco CAR Web Service only on the first server, and it requires that the Cisco CAR Scheduler service is activated and running on the same server and that the CDR Repository Manager service also is running on the same server.
Database and Admin Services	
Cisco AXL Web Service	Activate on the first node only. Failing to activate this service causes the inability to update Cisco Unified Communications Manager from client-based applications that use AXL.
Cisco Bulk Provisioning Service	You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.
Cisco TAPS Service	Before you can use the Cisco Unified Communications Manager Auto-Register Phone Tool, you must activate this service on the first node. When you create dummy MAC addresses for the Cisco Unified Communications Manager Auto-Register Phone Tool, ensure that the Cisco Bulk Provisioning Service is activated on the same node.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Activate on only the first node. **Note** The service only generates reports on the first node even if you activate the service on other nodes.
Cisco CallManager SNMP Service	If you use SNMP, activate this service on all servers in the cluster.
Security Services	
Cisco CTL Provider	Activate on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	Activate on only the first node.
Directory Services	
Cisco DirSync	Activate only on the first node.

Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center

Unified CM only: Control Center in Cisco Unified Serviceability allows you to view status, refresh the status, and to start, stop, and restart feature and network services.

Unified CM only: Starting, stopping, or restarting a service causes all Cisco Unified IP Phones and gateways that are currently registered to that service to fail over to their secondary Cisco CallManager service. Devices and phones need to restart only if they cannot register with another service.

Unified CM and Unified CM BE 5000 only: Starting, stopping, or restarting a service causes other installed applications (such as conference bridge or Cisco Messaging Interface) that are homed to the Cisco Unified Communications Manager to start and stop as well.

Note *Unified CM only*: If you are upgrading Cisco Unified Communications Manager, those services that were already started on your system automatically start after the upgrade.

Caution *Unified CM and Unified CM BE 5000 only*: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, and other types of calls get dropped.

Perform the following procedure to start, stop, restart, or view the status of services for a server (or for a server in a cluster in a Cisco Unified Communications Manager cluster configuration). You can start, stop, or refresh only one service at a time. Be aware that when a service is stopping, you cannot start it until after the service is stopped. Likewise, when a service is starting, you cannot stop it until after the service is started.

Procedure

Step 1 Depending on the service type that you want to start/stop/restart/refresh, perform one of the following tasks:

- Choose **Tools > Control Center—Feature Services**.

Tip Before you can start/stop/restart a feature service, it must be activated. To activate a service, see the "Activating and Deactivating Feature Services" section on page 11-1.

- Choose **Tools > Control Center—Network Services**.

Step 2 From the Server drop-down list box, choose the server; then, click **Go**.

The window displays the following items:

- The service names for the server that you chose.
- The service group.
- The service status; for example, Started, Running, Not Running, and so on. (Status column)
- The exact time that the service started running. (Start Time column)
- The amount of time that the service has been running. (Up Time column)

Step 3 Perform one of the following tasks:

- Click the radio button next to the service that you want to start and click the **Start** button.

  The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to stop and click the **Stop** button.

  The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to restart and click the **Restart** button.

  A message indicates that restarting may take a while. Click **OK**.
- To get the latest status of the services, click the **Refresh** button.

- To go to the Service Activation window or to the other Control Center window, choose an option from the Related Links drop-down list box and click **Go**.

Additional Information

See the "Related Topics" section on page 11-6.

Using a Command Line Interface to Start and Stop Services

You can start and stop some services through the Command Line Interface (CLI). For a list of services that you can start and stop through the CLI and for information on how to perform these tasks, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Tip You must start and stop most services from Control Center in Cisco Unified Serviceability.

Additional Information

See the "Related Topics" section on page 11-6.

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Activating and Deactivating Feature Services, page 11-1
- *Unified CM only*: Cluster Service Activation Recommendations, page 11-2
- Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center, page 11-4
- Using a Command Line Interface to Start and Stop Services, page 11-6

CHAPTER 12

Configuring Serviceability Reports Archive

The Cisco Serviceability Reporter service generates daily reports in Cisco Unified Serviceability. Each report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

This section describes how to use the Serviceability Reports Archive window.

Before you Begin

Activate the Cisco Serviceability Reporter service, which is CPU intensive. After you activate the service, report generation may take up to 24 hours.

Unified CM only: Cisco recommends that you activate the service on a non-callprocessing server.

Procedure

Step 1 Choose **Tools > Serviceability Reports Archive**.

The Serviceability Reports Archive window displays the month and year for which the reports are available.

Step 2 From the Month-Year pane, choose the month and year for which you want to display reports.

A list of days that correspond to the month displays.

Step 3 To view reports, click the link that corresponds to the day for which reports were generated.

The report files for the day that you chose display.

Step 4 To view a particular PDF report, click the link of the report that you want to view.

Tip If you browsed into Cisco Unified Serviceability by using the server name, you must log in to Cisco Unified Serviceability before you can view the report.

Tip If your network uses Network Address Translation (NAT) and you are trying to access serviceability reports inside the NAT, enter the IP address for the private network that is associated with the NAT in the browser URL. If you are trying to access the reports outside the NAT, enter the public IP address, and NAT will accordingly translate/map to the private IP address.

Tip To view PDF reports, you must install Acrobat ® Reader on your machine. To download Acrobat Reader, click the link at the bottom of the Serviceability Reports Archive window.

A window opens and displays the PDF file of the report that you chose.

Additional Information

See the "Related Topics" section on page 12-2.

Where to Find More Information

Related Topics

- Understanding Serviceability Reports Archive, page 10-1

Additional Cisco Documentation

Cisco Unified Real-Time Monitoring Tool Administration Guide

CHAPTER 13

Configuring CDR Repository Manager

Use the CDR Management Configuration window to set the amount of disk space to allocate to call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs. The CDR repository manager service repeatedly attempts to deliver CDR and CMR files to the billing servers that you configure in the CDR Management Configuration window until it delivers the files successfully, until you change or delete the billing application server on the CDR Management Configuration window, or until the files fall outside the preservation window and are deleted.

Unified CM BE 5000 only: The CDR and CMR files get offloaded to the external billing application servers by using the time interval that you have previously specified in the **CDR File Time Interval** enterprise parameter in Cisco Unified Communications Manager. After the Communications Manager generates the files, the CDR Agent and CDR Repository Manager take over. On each Communications Manager server, the CDR agent pushes the CDR flat files to the publisher. The CDR Repository Manager pushes the files to the external billing application servers.

Note To access the Enterprise Parameters Configuration window, open Cisco Unified Communications Manager Administration and choose **System** -> **Enterprise Parameters**. The **CDR File Time Interval** parameter specifies the time interval for collecting CDR data. For example, if this value is set to 1, each file will contain 1 minute of CDR data (CDRs and CMRs, if enabled). The external billing server and CAR database will not receive the data in each file until the interval has expired, so consider how quickly you want access to the CDR data when you decide what interval to set for this parameter. For example, setting this parameter to 60 means that each file will contain 60 minutes worth of data, but that data will not be available until the 60-minute period has elapsed, and the records are written to the CAR database. and the CDR files are sent to the configured billing server(s). The default value equals 1. The minimum value specifies 1, and the maximum value specifies 1440. The unit of measure for this required field represents a minute.

Both the CDR Agent and the CDR Repository Manager process files with an interval that is independent of the CDR File Time Interval. The CDR Repository Manager sends all existing CDR files to the billing application servers, sleeps for 6 seconds before checking the new files to send, and continues that 6-second interval. If the destination (the external billing application servers) does not respond, the system attempts the process again by using a doubled length of the sleep interval (12 seconds). Each delivery failure results in double the sleep time (6, 12, 24, 48,and so on, seconds) until 2 minutes occurs, then stays at 2-minute intervals until successful delivery occurs. After successful delivery, the 6-second interval automatically resumes.

Users cannot configure the 6-second processing time, with the sleep time interval doubling in case of failure. Users can configure only the **CDR File Time Interval** enterprise parameter. No alert gets sent after the first file delivery failure. By default, the system generates the CDRFileDeliveryFailed alert after

the second delivery failure of the Cisco CDR Repository Manager service to deliver files to any billing application server. You can configure the alert to send you an e-mail or to page you. For information on configuring alerts, see the "Working with Alerts" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

The system generates the CDRFileDeliveryFailureContinues syslog alarm upon subsequent failures to deliver the files to the billing application servers.

The CDR Agent behaves in almost the same manner. First, it sends all the existing CDR files to the publisher. If no additional files to send exist, the CDR Agent sleeps for 6 seconds before checking for new files. Each delivery failure results in the immediate change of the sleep interval to 1 minute, then says at 1-minute intervals until successful delivery. After the first successful delivery of files, the 6-second interval resumes.

The system sends no alert after the first file delivery failure by the CDR Agent. By default, the system generates the CDRAgentSendFileFailed alert after the second delivery failure of the CDR Agent. You can configure the alert to send you an e-mail or to page you. For information on configuring alerts, see the "Working with Alerts" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*

The system generates the CDRAgentSendFileFailedContinues syslog alarm upon subsequent failures to deliver the files.

If you need to start or restart the file transfer timer for any reason, you can restart the Cisco CDR Repository Manager or CDR Agent process by going to the Cisco Unified Serviceability window and selecting **Tools -> Control Center -> Network Services**.

When you enable the file deletion based on high water mark parameter, the CDR repository manager service monitors the amount of disk space that CDR and CMR files use. If disk usage exceeds the high water mark that you configure, the system purges the CDR and CMR files that have been successfully delivered to all destinations and loaded into the CAR database (if CAR is activated) until the disk space reaches the low water mark or the system deletes all successfully delivered files. If disk usage still exceeds the high water mark after the system deletes all successfully delivered files, it does not delete any more files, unless the disk usage still exceeds the disk allocation that you configure. If the disk usage still exceeds the disk allocation that you configure, the system purges files beginning with the oldest, regardless of whether the files fall within the preservation window or have been successfully delivered, until the disk usage falls below the high water mark.

Note Regardless of whether you enable the deletion of files based on the high water mark parameter, if disk usage exceeds the disk allocation that you configure, the CDR repository manager service deletes CDR and CMR files, beginning with the oldest files, until disk utilization falls below the high water mark.

The Cisco Log Partition Monitoring Tool service monitors the disk usage of CDR and CMR flat files that have not been delivered to the CDR repository manager.

Unified CM only: If the disk usage of the log partition on a server exceeds the configured limit and the service has deleted all other log and trace files, the log partition monitor service deletes CDR/CMR files on the subsequent nodes that have not been delivered to the CDR repository manager.

For more information on log partition monitoring, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

This chapter contains the following topics:

Configuring the CDR Repository Manager General Parameters

To set disk utilization and file preservation parameters for CDRs, perform the following procedure:

Procedure

Step 1 Choose **Tools > CDR Management**.

The CDR Management window displays.

Step 2 Click the CDR Manager general parameter value that you want to change.

Step 3 Enter the appropriate parameters, as described in Table 13-1.

Step 4 Click **Update**.

Tip At any time, you can click **Set Default** to specify the default values. After you set the defaults, click **Update** to save the default values.

Additional Information

See the "Related Topics" section on page 13-8.

CDR Repository Manager General Parameter Settings

Table 13-1 describes the available settings in the General Parameters section of the CDR Management Configuration window. For related procedures, see the "Related Topics" section on page 13-8.

Table 13-1 CDR Repository Manager General Parameter Settings

Field	Description
Disk Allocation (MB)	Choose the number of megabytes that you want to allocate to CDR and CMR flat file storage. The default disk allocation and range vary depending on the size of the server hard drive. **Note** The maximum CAR database size equals 6 GB for a Cisco Unified Communications Manager server and 3 GB for a Cisco Unified Communications Manager Business Edition 5000 server. **Note** If disk usage exceeds the allocated maximum disk space for CDR files, the system generates the CDRMaximumDiskSpaceExceeded alert and deletes all successfully processed files (those delivered to billing servers and loaded to CAR). If disk usage still exceeds the allocated disk space, the system deletes undelivered files and files within the preservation duration, starting with the oldest, until disk utilization falls below the high water mark. **Note** If you have a large system and do not allocate enough disk space, the system may delete the CDR and CMR files before the CAR Scheduler loads the files into the CAR database. For example, if you configure the CAR Scheduler to run once a day and you set the disk allocation to a value that is not large enough to hold the CDR and CMR files that are generated in a day, the system will delete the files before they are loaded into the CAR database.

Table 13-1 CDR Repository Manager General Parameter Settings (continued)

Field	Description
High Water Mark (%)	This field specifies the maximum percentage of the allocated disk space for CDR and CMR files. For example, if you choose 2000 megabytes from the Disk Allocation field and 80% from the High Water Mark (%) field, the high water mark equals 1600 megabytes. In addition to the high water mark percentage, the number of CDRs in the CAR database cannot exceed two million records for a Cisco Unified Communications Manager server and one million records for a Cisco Unified Communications Manager Business Edition 5000 server. When the disk usage exceeds the percentage that you specify, or the total number of CDRs is exceeded, and the Disable CDR/CMR Files Deletion Based on HWM check box is unchecked, the system automatically purges all successfully processed CDR and CMR files (those delivered to billing servers and loaded to CAR) beginning with the oldest files to reduce disk usage to the amount that you specify in the Low Water Mark (%) drop-down list box. If the disk usage still exceeds the low water mark or high water mark, the system does not delete any undelivered or unloaded files, unless the disk usage exceeds the disk allocation. If you check the Disable CDR/CMR Files Deletion Based on HWM check box, the system does not delete CDRs and CMRs based on the percentage that you specify in this field. **Note** If CDR disk space exceeds the high water mark, the system generates the CDRHWMExceeded alert.
Low Water Mark (%)	This field specifies the percentage of disk space that is allocated to CDR and CMR files that is always available for use. For example, if you choose 2000 megabytes from the Disk Allocation field and 40% from the Low Water Mark (%) field, the low water mark equals 800 megabytes.
CDR / CMR Files Preservation Duration (Days)	Choose the number of days that you want to retain CDR and CMR files. The CDR Repository Manager deletes files that fall outside the preservation window. **Note** If you continuously receive the CDRMaximumDiskSpaceExceeded alarm, you either must increase the disk allocation or lower the number of preservation days.

Table 13-1 CDR Repository Manager General Parameter Settings (continued)

Field	Description
Disable CDR/CMR Files Deletion Based on HWM	**Note** Regardless of whether you enable the deletion of files based on the high-water mark parameter, if disk usage exceeds the disk allocation that you configure, the maximum database size, or the maximum number of records for your installation, the CDR repository manager service deletes CDR and CMR files, beginning with the oldest files, until disk utilization falls below the high water mark. If you do not want to delete CDRs and CMRs even if disk usage exceeds the percentage that you specify in the High Water Mark (%) field, check this check box. By default, this check box remains unchecked, so the system deletes CDRs and CMRs if disk usage exceeds the high water mark.
CDR Repository Manager Host Name	This field lists the host name of the CDR repository manager server.
CDR Repository Manager Host Address	This field lists the IP address of the CDR repository manager server.

Configuring Application Billing Servers

Use the following procedure to configure application billing servers to which you want to send CDRs. You can configure up to three billing servers.

Procedure

Step 1 Choose **Tools > CDR Management Configuration**.

The CDR Management Configuration window displays.

Step 2 Perform one of the following tasks:

- To add a new application billing server, click the **Add New** button.
- To update an existing application billing server, click the server host name/IP address.

Step 3 Enter the appropriate settings, as described in Table 13-2.

Step 4 Click **Add** or **Update**.

Additional Information

See the "Related Topics" section on page 13-8.

Application Billing Server Parameter Settings

Table 13-2 describes the available settings in the Billing Application Server Parameters section of the CDR Management Configuration window. For related procedures, see the "Related Topics" section on page 13-8.

Table 13-2 Application Billing Server Parameter Settings

Field	Description
Host Name/IP Address	Enter the host name or IP address of the application billing server to which you want to send CDRs. If you change the value in this field, a prompt asks whether you want to send the undelivered files to the new destination. Perform one of the following tasks: • To deliver the files to the new server, click **Yes**. • To change the server host name/IP address without sending undelivered files, click **No**. The CDR Management service marks the CDR and CMR files as successfully delivered.
User Name	Enter the user name of the application billing server.
Protocol	Choose the protocol, either FTP or SFTP, that you want to use to send the CDR files to the configured billing servers.
Directory Path	Enter the directory path on the application billing server to which you want to send the CDRs. You should end the path that you specify with a "/" or "\", depending on the operating system that is running on the application billing server. **Note** Make sure the FTP user has write permission to the directory.
Password	Enter the password that is used to access the application billing server.
Resend on Failure	When you check the Resend on Failure box, this option informs CDRM to send outdated CDR and CMR files to the billing server after the FTP or SFTP connection is restored. When the box is checked, the Resend on Failure flag is set to True. When the box is not checked, the Resend on Failure flag is set to False.[1]
Generate New Key	Click on the **Reset** button to generate new keys and reset the connection to the SFTP server.

1. There are several different scenarios that can occur. When the billing server Resend on Failure flag is set to True, all CDR files get moved to the billing server. When the Resend On Failure flag is set to False, CDR files that get generated during shutdown of the billing server get moved to the processed folder, but do not get moved to the billing server. When the Resend on Failure flag gets set to True at the beginning, and then gets changed several times, the result is that the CDR files get moved to the billing server whenever the Resend on Failure box gets checked.

Deleting Application Billing Servers

Use the following procedure to delete an application billing server.

Step 1 Choose **Tools > CDR Management**.

The CDR Management Configuration window displays.

Step 2 Check the check box next to the application billing server that you want to delete and click **Delete Selected**.

A message displays that indicates that if you delete this server, any CDR or CMR files that have not been sent to this server will not be delivered to this server and will be treated as successfully delivered files.

Tip When you delete a server, the system does not generate the CDRFileDeliveryFailed alert for the files that are not sent to that server.

Step 3 To complete the deletion, click **OK**.

Additional Information

See the "Related Topics" section on page 13-8.

Where to Find More Information

Related Topics

- Configuring the CDR Repository Manager General Parameters, page 13-3
- CDR Repository Manager General Parameter Settings, page 13-4
- Configuring Application Billing Servers, page 13-6
- Application Billing Server Parameter Settings, page 13-7
- Deleting Application Billing Servers, page 13-7

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*

CHAPTER 14

Configuring the Audit Log

With audit logging, configuration changes to the Cisco Unified Communications Manager or Cisco Unity Connection system get logged in separate log files for auditing. This chapter contains the following topics:

Understanding Audit Logging

With audit logging, configuration changes to the Cisco Unified Communications Manager or Cisco Unity Connection system get logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center—Network Services in Cisco Unified Serviceability, monitors and logs any configuration change to the Cisco Unified Communications Manager or Cisco Unity Connection system by a user or as a result of the user action. For a Cisco Unified Communications Manager Business Edition 5000 system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

You access the Audit Log Configuration window in Cisco Unified Serviceability to configure the settings for the audit logs.

Audit logging contains the following parts:

- Audit logging framework—The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different Cisco Unified Communications Manager or Cisco Unity Connection components provide their own logging.

  The following example displays an API that a Cisco Unified Communications Manager component can use to send an alarm:

```
User ID: CCMAdministrator
Client IP Address: 172.19.240.207
Severity: 3
EventType: ServiceStatusUpdated
ResourceAccessed: CCMService
EventStatus: Successful
Description: CallManager Service status is stopped
```

- Audit event logging—An audit event represents any event that is required to be logged. The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: Call Manager Service status is stopped App ID:Cisco Tomcat
Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

Tip Be aware that audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.

The following components generate audit events:

- Cisco Unified Serviceability, page 14-2
- Cisco Unified Real-Time Monitoring Tool, page 14-2
- Cisco Unified Communications Manager CDR Analysis and Reporting, page 14-3
- Cisco Unified Communications Manager Administration, page 14-3
- Command-Line Interface, page 14-3
- Cisco Unity Connection Administration, page 14-3
- Cisco Personal Communications Assistant (Cisco PCA), page 14-4
- Cisco Unity Connection Serviceability, page 14-4
- Cisco Unity Connection Clients that Use the Representational State Transfer APIs, page 14-4

Cisco Unified Serviceability

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR management. *(Cisco Unified Communications Manager only)*
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node. *(Cisco Unified Communications Manager only)*

Cisco Unified Real-Time Monitoring Tool

Cisco Unified Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.

- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Cisco Unified Communications Manager CDR Analysis and Reporting

Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) creates audit logs for these events:

- Loader scheduling.
- Daily, weekly, and monthly reports scheduling.
- Mail parameters configuration.
- Dial plan configuration.
- Gateway configuration.
- System preferences configuration.
- Autopurge configuration.
- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configuration.

Cisco Unified Communications Manager Administration

The following events get logged for various components of Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts).
- User role membership updates (user added, user deleted, user role updated).
- Role updates (new roles added, deleted, or updated).
- Device updates (phones and gateways).
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and Cisco Unified Communications Manager server additions or deletions).

Command-Line Interface

All commands issued via the command-line interface are logged (for both Cisco Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts).
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony.
- Task management (enabling or disabling a task).
- Bulk Administration Tool (bulk creates, bulk deletes).

- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA)

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts).
- All configuration changes made via the Messaging Assistant.

Cisco Unity Connection Serviceability

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface (CUPI).

Configuring the Audit Log

To configure the audit log, perform the following procedure:

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools > Audit Log Configuration**.

The Audit Log Configuration window displays.

Step 2 Configure the settings in Table 14-1.

Step 3 Click **Save**.

Tip At any time, you can click **Set to Default** to specify the default values. After you set the defaults, click **Save** to save the default values.

Additional Information

See the "Related Topics" section on page 14-8.

Audit Log Configuration Settings

Table 14-1 describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability. For more information on audit logging, see the "Where to Find More Information" section on page 14-8.

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, for Cisco Unified Communications Manager, the CCMAdministrator possesses the audit role after fresh installs and upgrades. The CCMAdministrator can assign any user that has auditing privileges to the Standard Audit Users group in the User Group Configuration window in Cisco Unified Communications Manager Administration. If you want to do so, you can then remove CCMAdministrator from the Standard Audit Users group.

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Standard Audit Log Configuration role in Cisco Unified Communications Manager provides the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, Trace Collection Tool, RTMT Alert Configuration, Control Center—Network Services in Cisco Unified Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified Serviceability, and a resource that is called Audit Traces.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified Real-Time Monitoring Tool.

For information on roles, users, and user groups in Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager Administration Guide*. For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Table 14-1 Audit Log Configuration Settings

Field	Description
Select Server	
Server	Choose the server where you want to configure audit logs; then, click **Go**.
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to all Nodes** box.
Application Audit Log Settings	

Table 14-1 Audit Log Configuration Settings (continued)

Field	Description
Enable Audit Log	When you enable this check box, an audit log gets created for the application audit log. For Cisco Unified Communications Manager, the application audit log supports configuration updates for Cisco Unified Communications Manager graphical user interfaces (GUIs), such as Cisco Unified Communications Manager Administration, Cisco Unified Real-Time Monitoring Tool, Cisco Unified Communications Manager CDR Analysis and Reporting, and Cisco Unified Serviceability. For Cisco Unity Connection, the application audit log supports configuration updates for Cisco Unity Connection graphical user interfaces, including Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant, and clients that use the Connection REST APIs. This setting displays as enabled by default.
Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the Enable Purging check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central > Audit Logs** in RTMT.
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1 MB and 10 MB. You must specify a number between 1 and 10.
Database Audit Log Filter Settings	
Enable Audit Log	When you enable this check box, an audit log gets created for the Cisco Unified Communications Manager and Cisco Unity Connection databases. Use this setting in conjunction with the Debug Audit Level setting, which allows you create a log for certain aspects of the database.

Table 14-1 Audit Log Configuration Settings (continued)

Field	Description
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, choose one of the following options. Be aware that each audit log filter level is cumulative. • **Schema**—Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks**—Tracks all administrative changes to the Cisco Unified Communications Manager system (for example, any changes to maintain the system) plus all Schema changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates**—Tracks all changes to the database plus all schema changes and all administrative tasks changes. • **Database Reads**—Tracks every read to the Cisco Unified Communications Manager system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Cisco Unified Communications Manager or Cisco Unity Connection system. This level uses significant amounts of system resources and only should be used for a short time.
Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the Audit Enable Rotation option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting is unchecked, audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the Max No. of Files setting; for example, if you enter 40 in the Maximum No. of Files field, the highest number that you can enter in the No. of Files Deleted on Log Rotation field is 38.

Where to Find More Information

Related Topics

- Understanding Audit Logging, page 14-1
- Configuring the Audit Log, page 14-4
- Audit Log Configuration Settings, page 14-5
- Configuring Trace, page 7-1
- Configuring Troubleshooting Trace Settings, page 8-1
- Network Services, page 9-9

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*

PART 5

Simple Network Management Protocol (SNMP)

CHAPTER 15

Understanding Simple Network Management Protocol

This chapter provides information on the following topics:

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)

Titan (refer to http://www.titanftp.com/)

For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

You use Cisco Unified Serviceability to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. The settings that you configure in Cisco Unified Serviceability apply to the local node; however, if your Cisco Unified Communications Manager or Cisco Unity Connection configuration supports clusters, you can apply settings to all servers in the cluster with the "Apply to All Nodes" option in the SNMP configuration windows.

Tip *Unified CM only*: SNMP configuration parameters that you specified in Cisco Unified CallManager or Cisco Unified Communications Manager 4.X do not migrate during a Cisco Unified Communications Manager 6.0 and later upgrade. You must perform the SNMP configuration procedures again in Cisco Unified Serviceability.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

This section contains information on the following topics:

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  Unified CM BE 5000 only: The server where Cisco Unified Communications Manager is installed acts as the managed device.

  Unified CM only: In a configuration that supports clusters, the first node in the cluster acts as the managed device.

- Agent—A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  Cisco Unified Communications Manager and Cisco Unity Connection use a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few MIB variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Cisco Unified Communications Manager subagent interacts with the local Cisco Unified Communications Manager only. The Cisco Unified Communications Manager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).
- Network Management System (NMS)—A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Cisco Unified Communications Manager works with the following NMS:
  - CiscoWorks Lan Management Solution
  - HP OpenView
  - Third-party applications that support SNMP and Cisco Unified Communications Manager SNMP interfaces

SNMP Configuration Requirements

The system provides no default SNMP configuration. You must configure SNMP settings after installation to access MIB information. Cisco supports SNMP V1, V2c, and V3 versions.

SNMP agent provides security with community names and authentication traps. You must configure a community name to access MIB information. Table 15-1 provides the required SNMP configuration settings.

Table 15-1 SNMP Configuration Requirements

Configuration	Cisco Unified Serviceability Page
V1/V2c Community String	**SNMP > V1/V2c >Community String**
V3 Community String	**SNMP > V3 > User**
System Contact and Location for MIB2	**SNMP > SystemGroup > MIB2 System Group**
Trap Destinations (V1/V2c)	**SNMP > V1/V2c > Notification Destination**
Trap Destinations (V3)	**SNMP > V3 > Notification Destination**

SNMP Version 1 Support

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In Cisco Unified Serviceability, you configure SNMP v1 support in the V1/V2c Configuration window.

SNMP Version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In Cisco Unified Serviceability, you configure SNMP v2c support in the V1/V2c Configuration window.

SNMP Version 3 Support

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the "SNMP Community Strings and Users" section on page 15-5.

In Cisco Unified Serviceability, you configure SNMP v3 support in the V3 Configuration window.

SNMP Services

The services in Table 15-2 support SNMP operations. For a description of each service, see the "Understanding Services" section on page 9-1.

Note SNMP Master Agent serves as the primary service for the MIB interface. You must manually activate Cisco CallManager SNMP service; all other SNMP services should be running after installation.

Table 15-2 SNMP Services

MIB	Service	Window
CISCO-CCM-MIB	Cisco CallManager SNMP service	**Cisco Unified Serviceability > Tools > Control Center - Feature Services.** Choose a server; then, choose Performance and Monitoring category.
SNMP Agent	SNMP Master Agent	**Cisco Unified Serviceability > Tools > Control Center - Network Services.** Choose a server; then, choose Platform Services category.
CISCO-CDP-MIB	Cisco CDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
Hardware MIBs	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**Cisco Unity Connection Serviceability > Tools > Service Management.** Choose a server; then, choose Base Services category.

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the Cisco Unified Communications Manager or Cisco Unity Connection network. Do not stop the services unless your technical support team tells you to do so.

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMP V1 and V2c only.

SNMP V3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In Cisco Unified Serviceability, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments. You configure the notification destinations by using the SNMP Notification Destination Configuration windows in Cisco Unified Serviceability.

Note Cisco Unified Communications Manager supports SNMP traps in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 systems.

For all notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, the CallManager alarms and system level log messages get sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages get logged locally in the syslog files and also get converted into SNMP traps/notifications.

The following list contains Cisco Unified Communications Manager SNMP trap/inform messages that are sent to a configured trap destination:

- Cisco Unified Communications Manager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

Tip Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string/user correctly.

You configure the SNMP trap destination by choosing **SNMP > V1/V2 > Notification Destination** or **SNMP > V3> Notification Destination** in Cisco Unified Serviceability.

Table 15-3 comprises information about Cisco Unified Communications Manager trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in Table 15-3 by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note All the parameters that are listed in Table 15-3 are part of CISCO-CCM-MIB except for the last two parameters. The last two, clogNotificationsEnabled and clogMaxSeverity, comprise part of CISCO-SYSLOG-MIB.

Table 15-3 Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change **Note** Although you can configure a Cisco ATA 186 device as a phone in Cisco Unified Communications Manager Administration, when Cisco Unified Communications Manager sends SNMP traps for the Cisco ATA device, it sends a gateway type trap; for example, ccmGatewayFailed.	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600. See Configuring CISCO-CCM-MIB Trap Parameters, page 19-2.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600. See Configuring CISCO-CCM-MIB Trap Parameters, page 19-2.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.

Table 15-3 Cisco Unified Communications Manager Trap/Inform Configuration Parameters (continued)

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmQualityReportAlarmEnable	True	**Note** This trap gets generated only if the Cisco Extended Functions service is activated and running on the server; or, in the case of a cluster configuration (Cisco Unified Communications Manager only), on the local Cisco Unified Communications Manager server. ccmQualityReport	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True. See Configuring CISCO-SYSLOG-MIB Trap Parameters, page 19-1.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when Cisco Unified Communications Manager applications generate a syslog message with at least a warning severity level.Configuring CISCO-SYSLOG-MIB Trap Parameters, page 19-1.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

Note Cisco Unified Communications Manager supports the following MIBs except for CISCO-UNITY-MIB. Cisco Unified Communications Manager Business Edition 5000 supports all the following MIBs. Cisco Unity Connection supports the following MIBs except for CISCO-CCM-MIB.

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CCM-MIB
- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

The Simple Network Management Protocol (SNMP) extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In the case of a cluster configuration, the SNMP extension agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

For vendor-specific supported hardware MIBS, refer to the "Vendor-Specific MIBs" section.

Cisco Unified Communications Manager SNMP Interface supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco Unified Communications Manager CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco Unified Communications Manager and Cisco Unity Connection to advertise themselves to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun

- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the Cisco Unified Communications Manager and its associated devices, such as phones, gateways, and so on, that are visible on this Cisco Unified Communications Manager node. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

Note Cisco Unified Communications Manager supports this MIB in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000 systems. Cisco Unity Connection does not support this MIB.

To view the support lists for the CISCO-CCM-MIB and MIB definitions, go to the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

To view MIB dependencies and MIB contents, including obsolete objects, across Cisco Unified Communications Manager releases, go to the following link: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

Dynamic tables (see Table 15-4) get populated only if the Cisco CallManager service is up and running (or the local Cisco CallManager service in the case of a Cisco Unified Communications Manager cluster configuration); static tables (see Table 15-5) get populated when the Cisco CallManager SNMP Service is running.

Table 15-4 Cisco-CCM-MIB Dynamic Tables

Table(s)	Contents
ccmTable	This table stores the version and installation ID for the local Cisco Unified Communications Manager. The table also stores information about all the Cisco Unified Communications Manager in a cluster that the local Cisco Unified Communications Manager knows about but shows “unknown” for the version detail. If the local Cisco Unified Communications Manager is down, the table remains empty, except for the version and installation ID values.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match Cisco Unified Communications Manager/RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone. The ccmPhoneExtnTable uses a combined index, ccmPhoneIndex and ccmPhoneExtnIndex, for relating the entries in the ccmPhoneTable and ccmPhoneExtnTable.
ccmCTIDevice, ccmCTIDeviceDirNum	The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Cisco Unified Communications Manager MIB get updated.
ccmSIPDevice	The CCMSIPDeviceTable stores each SIP trunk as one device.

Table 15-4 Cisco-CCM-MIB Dynamic Tables (continued)

Table(s)	Contents
ccmH323Device	The ccmH323DeviceTable contains the list of H323 devices for which Cisco Unified Communications Manager contains information (or the local Cisco Unified Communications Manager in the case of a cluster configuration). For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Cisco Unified Communications Manager. Cisco Unified Communications Manager generates the H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H323 trunk information.
ccmVoiceMailDevice, ccmVoiceMailDirNum	For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable includes one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisco Unified Communications Manager MIB get updated.
ccmGateway	The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively. Cisco Unified Communications Manager generates alarms at the device or port level. The ccmGatewayTable, based on CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports. Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.
ccmMediaDeviceInfo	The table contains a list of all media devices which have tried to register with the local CallManager at least once.
ccmGroup	This tables contains the Cisco Unified CM groups in a Cisco Unified Communications Manager cluster.
ccmGroupMapping	This table maps all Cisco Unified CMs in a cluster to a Cisco Unified CM group. The table remains empty when the local Cisco Unified CM node is down

Table 15-5 CISCO-CCM-MIB Static Tables

Table(s)	Content
ccmProductType	The table contains the list of product types that are supported with Cisco Unified Communications Manager (or cluster, in the case of a Cisco Unified Communications Manager cluster configuration), including phone types, gateway types, media device types, H323 device types, CTI device types, voice-messaging device types, and SIP device types.
ccmRegion, ccmRegionPair	ccmRegionTable contains the list of all geographically separated regions in a Cisco Communications Network (CCN) system. The ccmRegionPairTable contains the list of geographical region pairs for a Cisco Unified Communications Manager cluster. Geographical region pairs are defined by Source region and Destination region.
ccmTimeZone	The table contains the list of all time zone groups in a Cisco Unified Communications Manager cluster.
ccmDevicePool	The tables contains the list of all device pools in a Cisco Unified Communications Manager cluster. Device pools are defined by Region, Date/Time Group, and Cisco Unified CM Group.

Note 'The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that the "SNMP Management Information Base (MIB)" section on page 15-8 describes.

CISCO-UNITY-MIB

The CISCO-UNITY-MIB uses the Connection SNMP Agent to get information about Cisco Unity Connection.

To view the CISCO-UNITY-MIB definitions, go to the following link and click **SNMP V2 MIBs**:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note Cisco Unity Connection supports this MIB. Cisco Unified Communications Manager does not support this MIB.

The Connection SNMP Agent supports the following objects.

Table 15-6 CISCO-UNITY-MIB Objects

Object	Description
ciscoUnityTable	This table contains general information about the Cisco Unity Connection servers such as host name and version number.
ciscoUnityPortTable	This table contains general information about the Cisco Unity Connection voice messaging ports.
General Unity Usage Info objects	This group contains information about capacity and utilization of the Cisco Unity Connection voice messaging ports.

Vendor-Specific MIBs

The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that the hardware vendors develop; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 15-7—Describes supported IBM MIBs
- Table 15-8—Describes supported HP MIBs

Table 15-7 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SERVERAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.159.1.1.200 .1	Provides RAID status
IBM-SYSTEM-STORAGE-MIB	1.3.6.1.4.1.2.6.159.3.1	Provides RAID status

Table 15-8 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

SNMP Trace Configuration

For Cisco Unified Communications Manager, you can configure trace for the Cisco CallManager SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco CallManager SNMP Service in the Performance and Monitoring Services service group. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you use the CLI to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For Cisco Unity Connection, you can configure trace for the Connection SNMP agent in the Trace Configuration window in Cisco Unity Connection Serviceability by choosing the Connection SNMP Agent component.

SNMP Configuration Checklist

Table 15-9 provides an overview of the steps for configuring SNMP.

Table 15-9 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the Control Center—Network Services window, verify that the system started the SNMP services.	• SNMP Services, page 15-4 • Understanding Services, page 9-1 • Configuring Services, page 11-1
Step 3	*Unified CM and Unified CM BE 5000 only:* In the Service Activation window, activate the Cisco CallManager SNMP service. *Connection only:* The Connection SNMP Agent service automatically activates.	• SNMP Services, page 15-4 • Understanding Services, page 9-1 • Activating and Deactivating Feature Services, page 11-1
Step 4	If you are using SNMP V1/V2c, configure the community string.	Configuring a Community String, page 16-2
Step 5	If you are using SNMP V3, configure the SNMP user.	Configuring the SNMP User, page 17-2
Step 6	Configure the notification destination for traps or informs.	• For SNMP v1/v2c—Configuring a Notification Destination for SNMP V1/V2c, page 16-6 • For SNMP v3—Configuring a Notification Destination for SNMP V3, page 17-6 • SNMP Management Information Base (MIB), page 15-8
Step 7	Configure the system contact and location for the MIB2 system group.	Configuring the MIB2 System Group, page 18-1
Step 8	Configure trap settings for CISCO-SYSLOG-MIB.	Configuring CISCO-SYSLOG-MIB Trap Parameters, page 19-1
Step 9	*Unified CM and Unified BE only:* Configure trap settings for CISCO-CCM-MIB.	Configuring CISCO-CCM-MIB Trap Parameters, page 19-2
Step 10	Restart the Master Agent service.	• SNMP Services, page 15-4 • Understanding Services, page 9-1 • Understanding Services, page 9-1
Step 11	On the NMS, configure the Cisco Unified Communications Manager trap parameters.	• SNMP Management Information Base (MIB), page 15-8 • SNMP product documentation that supports the NMS

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Configuring Services, page 11-1
- Configuring SNMP V1/V2c, page 16-1

- Configuring SNMP V3, page 17-1
- Configuring SNMP System Group, page 18-1
- Configuring SNMP Trap/Inform Parameters, page 19-1
- *Cisco Unified Communications Manager Troubleshooting Guide* (for SNMP troubleshooting information)
- *Troubleshooting Guide for Cisco Unity Connection* (for SNMP troubleshooting information)

CHAPTER 16

Configuring SNMP V1/V2c

This chapter, which describes how to configure SNMP versions 1 and 2c, so the network management system can monitor Cisco Unified Communications Manager, contains the following topics:

Tip If you use SNMP version 3, see the "Configuring SNMP V3" section on page 17-1.

Finding a Community String

Tip The Add New button does not display in the SNMP Community String Configuration window until you click the Find button. If no community strings exist and you want to add a community string, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a community string, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V1/V2c > Community String**.

The Find/List window displays.

Step 2 From the Find Community Strings where Name drop-down list box, choose the specific search criteria that you want to use for the community string.

Step 3 Enter the community string for which you want to search.

Step 4 In the Server field, enter the hostname or IP address of the server where the community string exists.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 *Unified CM clusters only*: If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the community string that you want to view.

Step 8 To add or update a community string, see the "Configuring a Community String" section on page 16-2.

Additional Information

See the "Where to Find More Information" section on page 16-8.

Configuring a Community String

Because the SNMP agent provides security by using community strings, you must configure the community string to access any management information base (MIB) in a Cisco Unified Communications Manager system. Change the community string to limit access to the Cisco Unified Communications Manager system. To add, modify, and delete community strings, access the SNMP Community String configuration window.

Procedure

Step 1 Perform the procedure in the "Finding a Community String" section on page 16-1.

Step 2 Perform one of the following tasks:

- To add a new community string, click the **Add New** button and go to Step 3.
- To modify an existing community string, locate the community string, as described in the "Finding a Community String" section on page 16-1; click the name of the community string that you want to edit and go to Step 3.

  You cannot change the name of the community string or the server.
- To delete a community string, see the "Deleting a Community String" section on page 16-4.

Step 3 Enter the configuration settings, as described in Table 16-1.

Tip Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 4 After you complete the configuration, click **Add New** to save a new community string or click **Save** to save changes to an existing community string.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Note Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

The system refreshes and displays the SNMP Community String Configuration window. The community string that you created displays in the window.

Additional Information

See the "Where to Find More Information" section on page 16-8.

Community String Configuration Settings

Table 16-1 describes the community string configuration settings. For related procedures, see the "Where to Find More Information" section on page 16-8.

Table 16-1 Community String Configuration Settings

Field	Description
Server	This setting in the Community String configuration window displays as read only because you specified the server choice when you performed the procedure in the "Finding a Community String" section on page 16-1. To change the server for the community string, perform the procedure in the "Finding a Community String" section on page 16-1.
Community String	Enter a name for the community string. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Choose community string names that will be hard for outsiders to figure out. When you edit a community string, you cannot change the name of the community string.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click this radio button.
Accept SNMP Packets only from these hosts	To accept SNMP only from specified hosts, click this radio button. **Tip** In the Host IP Address field, enter a host from which you want to accept packets and click **Insert**. Repeat this process for each host from which you want to accept packets. To delete a host, choose that host from the Host IP Addresses list box and click **Remove**.

Table 16-1 Community String Configuration Settings (continued)

Field	Description
Access Privileges	From the drop-down list box, choose the appropriate access level from the following list: • **ReadOnly**—The community string can only read the values of MIB objects. • **ReadWrite**—The community string can read and write the values of MIB objects. • **ReadWriteNotify**—The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The community string can only send MIB object values for a trap and inform messages. • **ReadNotifyOnly**—The community string can read values of MIB objects and also send the values for trap and inform messages. • **None**—The community string cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a community string with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
Unified CM clusters only: Apply To All Nodes	To apply the community string to all nodes in the cluster, check this check box.

Deleting a Community String

To delete a community string, perform the following procedure:

Procedure

Step 1 Locate the community string, as described in the "Finding a Community String" section on page 16-1.

Step 2 From the list of matching records, check the check box next to the community string that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message indicates that the system will delete notification entries that relate to this community string. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 11-4.

After the window refreshes, the string that you deleted no longer displays in the results.

Additional Information

See the "Where to Find More Information" section on page 16-8.

SNMP Notification Destination

The following sections apply to SNMP V1/V2c notification destination configuration.

Finding a Notification Destination for SNMP V1/V2c

Tip The Add New button does not display in the SNMP Notification Destination Configuration window until you click the Find button. If no notification destinations exist and you want to add a notification destination, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a notification destination for V1/V2c, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V1/V2c > Notification Destination**.

The Find/List window displays.

Step 2 From the Find Notification where Destination IP drop-down list box, choose the specific search criteria that you want to use to find the notification destination.

Step 3 Enter the notification destination for which you want to search.

Step 4 In the Server field, enter the hostname or IP address of the server that supports the notification destination.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 *Unified CM clusters only*: If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 To view the configuration for one of the items in the search results, click the item.

Step 8 To add or update a notification string, see the "Configuring a Notification Destination for SNMP V1/V2c" section on page 16-6.

Additional Information

See the "Where to Find More Information" section on page 16-8.

Configuring a Notification Destination for SNMP V1/V2c

To configure the notification destination (trap/inform receiver) for V1/V2c, perform the following procedure.

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V1/V2c" section on page 16-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP notification destination, click the **Add New** button and go to Step 3.

  You configure the notification destination for the server that you choose in the Server drop-down list box in the Find/List window.
- To modify an existing SNMP notification destination, locate the notification destination, as described in the "Finding a Notification Destination for SNMP V1/V2c" section on page 16-5; click the name of the SNMP notification destination that you want to edit and go to Step 3.
- To delete an SNMP notification destination, see the "Deleting a Notification Destination for SNMP V1/V2c" section on page 16-8.

Step 3 Enter the configuration settings, as described in Table 16-2.

Tip Before you save the configuration, you can click the **Clear** button at any time to delete all information that you entered for all settings in the window.

Step 4 To save a notification destination, click **Insert**, or click **Save** to save changes to an existing notification destination.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent, click **OK**.

Note Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Additional Information

See the "Where to Find More Information" section on page 16-8.

Notification Destination Configuration Settings for SNMP V1/V2c

Table 16-2 describes the notification destination configuration settings for V1/V2c. For related procedures, see the "Where to Find More Information" section on page 16-8.

Table 16-2 Notification Destination Configuration Settings for V1/V2

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V1/V2c" section on page 16-5. To change the server for the notification destination, perform the procedure in the "Finding a Community String" section on page 16-1.
Host IP Addresses	From the drop-down list box, choose the Host IP address of the trap destination or choose **Add New**. If you choose Add New, enter the IP address of the trap destination. For existing notification destinations, you cannot modify the host IP address configuration.
Port Number	In the field, enter the notification-receiving port number on the destination server that receives SNMP packets.
V1 or V2c	From the SNMP Version Information pane, click the appropriate SNMP version radio button, either V1 or V2c, which depends on the version of SNMP that you are using. • If you choose V1, configure the community string setting. • If you choose V2c, configure the notification type setting and then configure the community string.
Community String	From the drop-down list box, choose the community string name to be used in the notification messages that this host generates. Only community strings with minimum notify privileges (ReadWriteNotify or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click the **Create New Community String** button to create a community string, as described in the "Configuring a Community String" section on page 16-2.
Notification Type	From the drop-down list box, choose the appropriate notification type.
Unified CM clusters only: Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box.

Deleting a Notification Destination for SNMP V1/V2c

To delete a notification destination, perform the following procedure:

Procedure

Step 1 Locate the notification destination, as described in the "Finding a Notification Destination for SNMP V1/V2c" section on page 16-5.

Step 2 From the list of matching records, check the check box next to the notification destination that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message asks whether you want to delete the notification entries. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

After the window refreshes, the notification destination that you deleted no longer displays in the results.

Additional Information

See the "Where to Find More Information" section on page 16-8.

Where to Find More Information

Related Topics

CHAPTER 17

Configuring SNMP V3

This chapter, which describes how to configure SNMP v3, so the network management system can monitor Cisco Unified Communications Manager or Cisco Unity Connection, contains the following topics:

Tip If you use SNMP v1 or v2c, see the "Configuring SNMP V1/V2c" section on page 16-1.

Finding the SNMP User

Tip The Add New button does not display in the SNMP User Configuration window until you click the Find button. If no users exist and you want to add a user, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a SNMP user, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V3 > User**.

The SNMP User Configuration window displays.

Step 2 From the Find User where Name list box, choose the specific search criteria that you want to use to find the user; for example, begins with.

Step 3 Enter the user name for which you want to search.

Step 4 From the Server drop-down list box, choose the hostname or IP address of the server where you access the user.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 *Unified CM clusters only*: If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the user that you want to view.

Step 8 To add or update a user, see the "Configuring the SNMP User" section on page 17-2.

Additional Information

See the "Related Topics" section on page 17-9.

Configuring the SNMP User

To configure user(s) for SNMP, perform the following procedure:

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 17-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP user, click the **Add New** button in the SNMP User Configuration Find/List window and go to Step 3.
- To modify an existing SNMP user, locate the user, as described in the "Finding a Notification Destination for SNMP V3" section on page 17-5; click the name of the SNMP user that you want to edit and go to Step 3.
- To delete an SNMP user, see the "Deleting the SNMP User" section on page 17-4.

Step 3 Enter the configuration settings, as described in Table 17-1.

Tip Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 4 To add a new user, click **Insert**, or click **Save** to save changes to an existing user.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Note To access this server that has the user that you configure, make sure that you configure this user on the NMS with the appropriate authentication and privacy settings.

Additional Information

See the "Related Topics" section on page 17-9.

SNMP User Configuration Settings

Table 17-1 describes the SNMP user configuration settings for V3. For related procedures, see the "Related Topics" section on page 17-9.

Table 17-1 SNMP User Configuration Settings for V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V3" section on page 17-5. To change the server where you want to provide access, perform the procedure in the "Finding the SNMP User" section on page 17-1.
User Name	In the field, enter the name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS). For existing SNMP users, this setting displays as read only.
Authentication Required	To require authentication, check the check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol. The password must contain at least 8 characters.
Privacy Required	If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the check box, enter the password in the Password and Reenter Password fields, and check the protocol check box. The password must contain at least 8 characters. **Tip** After you check the Privacy Required check box, the DES (Data Encryption Standard) check box automatically appears checked. The DES protocol prevents packets from being disclosed.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.

Table 17-1 SNMP User Configuration Settings for V3 (continued)

Field	Description
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Host IP Address field, enter a host from which you want to accept SNMP packets and click **Insert**. Repeat this process for each host from which you want to accept SNMP packets. To delete a host, choose that host from the Host IP Addresses pane and click **Remove**.
Access Privileges	From the drop-down list box, choose one of the following options for the access level: • **ReadOnly**—The user can only read the values of MIB objects. • **ReadWrite**—The user can read and write the values of MIB objects. • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages. • **None**—The user cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
Unified CM clusters only: Apply To All Nodes	To apply the user configuration to all nodes in the cluster, check this check box.

Deleting the SNMP User

To delete a user for SNMP, perform the following procedure:

Procedure

Step 1 Locate the SNMP user, as described in the "Finding the SNMP User" section on page 17-1.

Step 2 From the list of matching records, check the check box next to the user that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message indicates that the system will delete notification entries that relate to this user. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

After the window refreshes, the user that you deleted no longer displays in the results.

Additional Information

See the "Related Topics" section on page 17-9.

SNMP Notification Destination

The following sections apply to SNMP V3 notification destination configuration.

Finding a Notification Destination for SNMP V3

Tip The Add New button does not display in the SNMP Notification Destination Configuration window until you click the Find button. If no users exist and you want to add want a user, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a notification destination for V3, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V3 > Notification Destination**.

Step 2 From the Find Notification where Destination IP drop-down list box, choose the specific search criteria that you want to use to find the notification destination; for example, begins with.

Step 3 Enter the IP address/hostname of notification destination for which you want to search.

Step 4 In the Server field, choose the hostname or IP address of the server that supports the notification destination.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 *Unified CM clusters only*: If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the notification destination that you want to view.

Step 8 To add or update a notification destination, see the "Configuring a Notification Destination for SNMP V3" section on page 17-6.

Additional Information

See the "Related Topics" section on page 17-9.

Configuring a Notification Destination for SNMP V3

To configure the trap/Inform receiver, perform the following procedure:

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 17-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP notification destination, click the **Add New** button in the search results window and go to Step 3.
- To modify an existing SNMP notification destination, locate the notification destination in the search results window; click the name of the SNMP notification destination that you want to edit and go to Step 3.
- To delete an SNMP notification destination, see the "Deleting a Notification Destination for SNMP V3" section on page 17-8.

Step 3 Configure the settings, as described in Table 17-2.

Tip Before you save the configuration, you can click the **Clear** button at any time to delete all information that you entered for all settings in the window.

Step 4 To save a notification destination, click **Insert**, or click **Save** to save changes to an existing notification destination.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Additional Information

See the "Related Topics" section on page 17-9.

Notification Destination Configuration Settings for SNMP V3

Table 17-2 describes the notification destination configuration settings for V3. For related procedures, see the "Related Topics" section on page 17-9.

Table 17-2 Notification Destination Configuration Settings for V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V3" section on page 17-5. To change the server for the notification destination, perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 17-5.
Host IP Addresses	From the drop-down list box, choose the Host IP address or choose **Add New**. If you chose Add New, enter the IP address for the host.
Port Number	In the field, enter the notification-receiving port number on the destination server.
Notification Type	From the drop-down list box, choose **Inform** or **Trap**. **Tip** Cisco recommends that you choose the Inform option. The Inform function retransmits the message until it is acknowledged, thus, making it more reliable than traps.
Remote SNMP Engine Id	This setting displays if you chose Inform from the Notification Type drop-down list box. From the drop-down list box, choose the engine ID or choose **Add New**. If you chose Add New, enter the ID in the Remote SNMP Engine Id field, which requires a hexidecimal value.
Security Level	From the drop-down list box, choose the appropriate security level for the user. • **noAuthNoPriv**—No authentication or privacy configured. • **authNoPriv**—Authentication configured, but no privacy configured. • **authPriv**—Authentication and privacy configured.

Table 17-2 Notification Destination Configuration Settings for V3 (continued)

Field	Description
User Information pane	From the pane, perform one of the following tasks to associate or disassociate the notification destination with the user. • To create a new user, click the **Create New User** button and see the "Configuring the SNMP User" section on page 17-2. • To modify an existing user, click the radio button for the user and click **Update Select ed User**; then, see the "Configuring the SNMP User" section on page 17-2. • To delete a user, click the radio button for the user and click **Delete Selected User**. The users that display vary depending on the security level that you configured for the notification destination.
Unified CM clusters only: Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box.

Deleting a Notification Destination for SNMP V3

To delete a notification destination, perform the following procedure:

Procedure

Step 1 Locate the SNMP notification destination, as described in the "Finding a Notification Destination for SNMP V3" section on page 17-5.

Step 2 From the list of matching records, check the check box next to the notification destination that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message asks you if you want to delete the notification destination. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

After the window refreshes, the notification destination that you deleted no longer displays in the search results window.

Additional Information

See the "Related Topics" section on page 17-9.

Where to Find More Information

Related Topics

- Understanding Simple Network Management Protocol, page 15-1
- Finding the SNMP User, page 17-1
- Configuring the SNMP User, page 17-2
- SNMP User Configuration Settings, page 17-3
- Deleting the SNMP User, page 17-4
- Finding a Notification Destination for SNMP V3, page 17-5
- Configuring a Notification Destination for SNMP V3, page 17-6
- Notification Destination Configuration Settings for SNMP V3, page 17-7
- Deleting a Notification Destination for SNMP V3, page 17-8
- Configuring SNMP V1/V2c, page 16-1
- Configuring SNMP System Group, page 18-1

CHAPTER 18

Configuring SNMP System Group

Cisco Unified Serviceability provides the MIB2 System Group Configuration window where you can configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location. This chapter contains information on the following topics:

Configuring the MIB2 System Group

Perform the following procedure to configure a system contact and system location for the MIB-II system group.

Tip This procedure supports SNMP v1, v2c, and v3 configuration.

Procedure

Step 1 Choose **Snmp > SystemGroup > MIB2 System Group**.

Step 2 Configure the settings, as described in Table 18-1.

Step 3 Click **Save**.

Step 4 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent service, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Note To clear the System Contact and System Location fields, click the **Clear All** button. To delete the system configuration, click the **Clear All** button and the **Save** button.

Additional Information

See the "Related Topics" section on page 18-2.

MIB2 System Group Configuration Settings

Table 18-1 describes the MIB2 System Group configuration settings. For related procedures, see the "Related Topics" section on page 18-2.

Table 18-1 MIB2 System Group Configuration Settings

Field	Description
Server	From the drop-down list box, choose the server for which you want to configure contacts; then, click **Go**.
System Contact	In the field, enter a person to notify when problems occur.
System Location	In the field, enter the location of the person that is identified as the system contact.
Unified CM clusters only: Apply To All Nodes	To apply the system configuration to all of the nodes in the cluster, check the check box.

Where to Find More Information

Related Topics

- Understanding Simple Network Management Protocol, page 15-1
- Configuring SNMP V1/V2c, page 16-1
- Configuring SNMP V3, page 17-1

CHAPTER 19

Configuring SNMP Trap/Inform Parameters

This section describes how to use CLI commands to set configurable trap settings. Table 15-3 provides the SNMP trap configuration parameters and recommended configuration for CISCO-SYSLOG-MIB, CISCO-CCM-MIB, and CISCO-UNITY-MIB.

This chapter provides information on the following topics:

Configuring CISCO-SYSLOG-MIB Trap Parameters

Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:

- Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to true from the linux command line using: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.41.1.1.2.0 i 1**

  You can also use any other SNMP management application for the SNMP Set operation.

- Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: **snmpset -c public -v2c** 1<*transmitter ipaddress*> **1.3.6.1.4.1.9.9.41.1.1.3.0 i** <*value*>

  Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.

  You can also use any other SNMP management application for the SNMP Set operation.

Note Before logging, Syslog truncates any trap message data that is larger than the specified Syslog buffer size. The Syslog trap message length limitation equals 255 bytes.

Configuring CISCO-CCM-MIB Trap Parameters

Unified CM and Unified CM BE 5000 only: Use these guidelines to configure CISCO-CCM-MIB trap settings on your system:

- Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.2 .0 i** <*value*>

  You can also use any other SNMP management application for the SNMP Set operation.

- Set ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

  You can also use any other SNMP management application for the SNMP Set operation.

Configuring CISCO-UNITY-MIB Trap Parameters

Connection only: The Connection SNMP Agent does not enable trap notifications, though traps can be triggered by Cisco Unity Connection alarms. You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability, on the Alarm > Definitions screen.

You can configure trap parameters by using the CISCO-SYSLOG-MIB. See the "Configuring CISCO-SYSLOG-MIB Trap Parameters" section on page 19-1.

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Configuring Services, page 11-1
- Configuring SNMP Trap/Inform Parameters, page 19-1
- Configuring SNMP V1/V2c, page 16-1
- Configuring SNMP V3, page 17-1
- Configuring SNMP System Group, page 18-1

Related Documentation

Command Line Interface Reference Guide for Cisco Unified Solutions

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V