Cisco Unified Serviceability Administration Guide for Cisco Unified Presence

Release 6.0(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-12729-01

CONTENTS

Preface

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

The preface covers these topics:

Purpose

The *Cisco Unified Presence Server Serviceability Administration Guide* provides information about the Cisco Unified Presence Serviceability program, including the Real-Time Monitoring Tool (RTMT).

Audience

The *Cisco Unified Presence Server Serviceability Administration Guide* provides information for network administrators responsible for managing and supporting the Cisco Unified Presence system. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, remote serviceability features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Chapter 1, "Introduction"	Provides an overview of the Cisco Unified Presence Serviceability application, remote serviceability applications, and reporting tools.
Chapter 2, "Managing Services"	Provides procedures for activating, deactivating, starting, and stopping Cisco Unified Presence services.
Chapter 3, "Alarm Configuration"	Provides procedures for configuring the Cisco Unified Presence alarms.
Chapter 4, "Alarm Definitions"	Provides procedures for searching and editing Cisco Unified Presence alarm definitions.
Chapter 5, "Trace Configuration"	Provides procedures for configuring trace parameters for Cisco Unified Presence services.
Chapter 6, "Troubleshooting Trace Setting Configuration"	Provides procedures for configuring the troubleshooting trace settings.
Chapter 7, "Real-Time Monitoring Configuration"	Provides procedures for configuring the real-time monitoring tool.
Chapter 8, "Alert Configuration in RTMT"	Provides procedures for working with alerts in the real-time monitoring tool, including setting alert properties, configuring alert actions, and configuring e-mails for alert notification.
Chapter 9, "Configuring and Using Performance Monitoring"	Provides procedures for working with performance monitors, including viewing performance counters and counter descriptions.
Chapter 10, "Trace Collection and Log Central in RTMT"	Provides information on configuring on-demand trace collection for Cisco Unified Presence services and crash dump files as well as on viewing the trace files in the appropriate viewer.
Chapter 11, "Using SysLog Viewer in RTMT"	Provides information on using the SysLog Viewer.
Chapter 12, "Using Plug-ins"	Provides information on installing and using plug-ins in the real-time monitoring tool.
Chapter 13, "Log Partition Monitoring Configuration"	Provides information on configuring Log Partition Monitoring to monitor the disk usage of the log partition on a server (or all servers in the cluster).
Chapter 14, "Serviceability Reports Archive Configuration"	Provides procedures for viewing reports generated by the Serviceability Reporter service.
Chapter 15, "SNMP V1/V2c Configuration"	Provides procedures for configuring SNMP versions 1 and 2c.
Chapter 16, "SNMP V3 Configuration"	Provides procedures for configuring SNMP version 3.
Chapter 17, "MIB2 System Group Configuration"	Provides procedures for configuring the system contact and system location objects for the MIB-II system group.

Related Documentation

Refer to the *Cisco Unified Presence Documentation Guide* for further information about related Cisco IP telephony applications and products. The following URL shows an example of the path to the documentation guide:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm

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.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

PART 1

Cisco Unified Presence Serviceability

CHAPTER 1

Introduction

This chapter comprises the following topics:

Cisco Unified Presence Serviceability Overview

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

- Saves Cisco Unified Presence services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Cisco Unified Presence services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Cisco Unified Presence cluster through the real-time monitoring tool (RTMT).
- 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.
- Archives reports that are associated with Cisco Unified Presence Serviceability tools.
- Allows Cisco Unified Presence to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster).

Accessing Cisco Unified Presence Serviceability

To access Cisco Unified Presence Serviceability, perform the following procedure:

Procedure

Step 1 By using Netscape 7.1 (or later) or Internet Explorer 6.0 (or later), browse into the Cisco Unified Presence where Cisco Unified Presence Serviceability service runs.

Tip In the supported browser, enter **https://<server name or IP address>:8443**, where server name or IP address equals the server where the Cisco Unified Presence 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 HTTPS. HTTP uses the port number, 8080.

Step 2 Click the **Cisco Unified Presence Administration** link.

Step 3 If the system prompts you about certificates, see the "Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)" section on page 1-2.

Step 4 The first time that the system prompts you for a user name and password, enter the application username and application user password that you specified during installation for the username and the password, respectively.

Tip Any user who has the Standard CCMUsers role assigned can access Cisco Unified Presence Serviceability. For information on how to assign this role to a user, refer to the *Cisco Unified Presence Administration Guide*.

Step 5 After Cisco Unified Presence Administration displays, choose **Serviceability** from the Navigation drop-down list box in the upper, right corner of the window.

Cisco Unified Presence Serviceability displays.

Tip To return to the Cisco Unified Presence Serviceability main window at any time during the configuration, click Home in the upper, right corner of the application window.

Additional Information

See the Related Topics, page 1-7.

Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

This section contains information on the following topics:

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 Cisco Unified Presence Serviceability. HTTPS also ensures that the user login password transports securely via the web.

HTTPS Overview for Internet Explorer

The first time that you (or a user) accesses Cisco Unified Presence Administration or other Cisco Unified Presence SSL-enabled virtual directories after the Cisco Unified Presence installation/upgrade, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must 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. To access the web application, you must click Yes or install the certificate via the View Certificate > Install Certificate options.

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 on the client.

Additional Information

See the Related Topics, page 1-7.

Saving the Certificate to the Trusted Folder in Internet Explorer

To save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application, perform the following procedure:

Procedure

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

Step 2 When the Security Alert dialog box displays, click **View Certificate**.

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

Step 4 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**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

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**.

Additional Information

See the Related Topics, page 1-7.

Using Netscape to Save the Certificate to the Trusted Folder

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.

Tip 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.

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

Procedure

Step 1 Browse to the application, for example, Cisco Unified Presence 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 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, page 1-7.

Using the Cisco Unified Presence Serviceability Interface

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

- To display documentation for a single window, choose **Help** > **This page** in Cisco Unified Presence Serviceability.
- To display a list of documents that are available with this release of Cisco Unified Presence (or to access the online help index), choose **Help** > **Contents** > **Contents and Index** in Cisco Unified Presence Serviceability.
- To go directly to the home page in Cisco Unified Presence Serviceability from a configuration window, click the **Home** link in the upper, right corner of the window.
- To access Cisco Unified Presence Administration or other applications, choose the appropriate application from the **Navigation** drop-down list box in the upper, right corner of the window.
- To use the icons in Cisco Unified Presence Serviceability, see Table 1-1.

Table 1-1 Icons in Cisco Unified Presence Serviceability

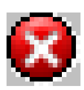
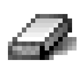
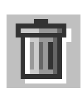
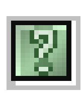
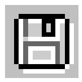
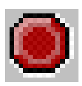
Icon	Purpose
 	Adds a new configuration
	Cancels the operation
	Clears the configuration that you specify
	Deletes the configuration that you choose
	Shows the online help for the configuration
	Refreshes the window to display the latest configuration

Table 1-1 Icons in Cisco Unified Presence Serviceability (continued)

Icon	Purpose
	Restarts the service that you choose
	Saves the information that you entered
	Sets the default for the configuration
	Starts the service that you choose
	Stops the service that you choose

Accessibility Features

Cisco Unified Presence Serviceability Administration 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 1-2 as a guide for navigating the interface by using keyboard shortcuts.

Table 1-2 Navigation Shortcuts for Cisco Unified Presence 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.
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

Table 1-2 Navigation Shortcuts for Cisco Unified Presence Serviceability

Keystroke	Action
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

- *Cisco Unified Presence Administration Guide*

Additional Information

See the Related Topics, page 1-7.

Related Topics

- Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), page 1-2
- HTTPS Overview for Internet Explorer, page 1-3
- Saving the Certificate to the Trusted Folder in Internet Explorer, page 1-3

Related Topics

PART 2

Service Management

CHAPTER 2

Managing Services

This chapter contains information on the following topics:

Activating and Deactivating Feature Services

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

Cisco Unified Presence allows you to activate and deactivate feature 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.

Perform the following procedure to activate or deactivate Cisco Unified Presence services in Cisco Unified Presence Serviceability.

Procedure

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

The Service Activation window displays.

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

The window displays the service names for the server that you chose and the activation status of the services.

Step 3 Click the **Set Default** button or activate the services that you want to use by checking the check box next to the service that you want to activate.

Step 4 After you finish making the appropriate changes, click **Save**.

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

Additional Information

See the Related Topics, page 2-3.

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

Control Center in Cisco Unified Presence Serviceability allows you to view status, refresh the status, and to start, stop, and restart Cisco Unified Presence services for a particular server in a cluster. Starting, stopping, or restarting a Cisco Presence service causes all gateways that are currently registered to that Cisco Presence service to fail over to their secondary Cisco Presence service. Devices and phones need to restart only if they cannot register with another Cisco Presence service. Starting, stopping, or restarting a Cisco Presence service causes other installed applications (such as Conference Bridge or Cisco Messaging Interface) that are homed to that Cisco Unified Presence to start and stop as well.

Note If you are upgrading Cisco Unified Presence, those services that were already started on your system will start after the upgrade.

Perform the following procedure to start, stop, restart, or view the status of services for a particular server in a cluster. You can start, stop, or refresh only one service at a time.

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 You can only start/stop/restart feature services that are activated. To activate a service, see the “Activating and Deactivating Feature Services” section on page 2-1.

- 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 service names for the server that you chose, the service type, and service status. The window also displays the status of the services (Started, Running or Stopped)

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 restart and click the **Restart** button.

  A message indicates that restarting may take a while. Click **OK**.

- 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.

- 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, page 2-3.

Using a Command Line Interface to Start and Stop Services

You can start and stop the following services by issuing a command in the command line interface (CLI):

- System NTP
- System SSH
- Service Manager
- A Cisco DB
- Cisco Tomcat
- Cisco Database Layer Monitor

To start a service, enter **utils service start <service name>**, where service name equals the entire name of the service.

To stop a service, enter **utils service stop <service name>**, where service name equals the entire name of the service.

Tip You must start and stop all other services from Control Center in Cisco Unified Presence Serviceability.

Additional Information

See the Related Topics, page 2-3.

Related Topics

- Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center, page 2-2
- Activating and Deactivating Feature Services, page 2-1

PART 3

Alarm Configuration

CHAPTER 3

Alarm Configuration

Cisco Unified Presence Serviceability Alarms assist system administrators and support personnel in troubleshooting Cisco Unified Presence problems by enabling administrators to configure alarms and events and by providing alarm message definitions. An administrator configures alarms and trace parameters and provides the information to a Cisco TAC engineer.

Administrators use alarms to provide runtime status and state of the system and to take corrective action for problem resolution; for example, to determine whether phones are registered and working. Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting for problems that are not on your local Cisco Unified Presence.

You can configure alarms for Cisco Unified Presence servers that are in a cluster and services for each server. You configure the alarm interface to send alarm information to multiple destinations, and each destination can have its own alarm event level (from debug to emergency). Then, you use the real-time monitoring tool to collect and view the alarms.

When a service issues an alarm, the alarm interface sends the alarm to the chosen monitors (for example, SDI trace, Cisco RIS Data Collector). The monitor forwards the alarm or writes it to its final destination (such as a log file).

This chapter contains the following topics:

Configuring or Updating an Alarm for a Service

This section describes how to configure an alarm for any Cisco Unified Presence service.

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

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 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, CUP, for which you want to configure the alarm; then, click **Go**.

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

Note The drop-down list box displays all services (active and inactive).

In the Alarm Configuration window, a list of alarm monitors with the event levels displays for the chosen service displays.

Step 5 Check the check box or boxes for the desired alarm destination as described in Table 3-1.

Step 6 In the Alarm Event Level selection box, choose the desired alarm event level as described in Table 3-2.

Step 7 To apply the current settings for selected services to all nodes in a cluster, check the **Apply to all Nodes** check box.

Step 8 To save your configuration, click the **Save** button.

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

Additional Information

See the Related Topics, page 3-4.

Alarm Destination Settings

Table 3-1 describes the alarm destination settings.

Table 3-1 Alarm Destinations

Name	Destination description
Enable Alarm for Local Syslogs	SysLog Viewer. The program logs Cisco Unified Presence 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 Serviceability Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, see the "Using SysLog Viewer in RTMT" section on page 11-1.
Enable Alarm for Remote Syslogs	Syslog file. 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 Presence does not send the Syslog messages. **Note** If you want to send the alarms to CiscoWorks 2000, specify the CiscoWorks 2000 server name.
Enable Alarm for SDI Trace	The SDI trace library. To log alarms in the SDI trace log file, check this check box, and check the Trace On check box in Trace Configuration window for the chosen service. For more information on by using the Trace Configuration window, see the "Configuring Trace Parameters" section on page 5-1.

Additional Information

See the Related Topics, page 3-4.

Alarm Event Level Settings

Table 3-2 describes the alarm event level settings.

Table 3-2 Alarm Event Levels

Name	Description
Emergency	This level designates system as unusable.
Alert	This level indicates that immediate action is needed.
Critical	Cisco Unified Presence 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.

Additional Information

See the Related Topics, page 3-4.

Related Topics

CHAPTER 4

Alarm Definitions

This chapter provides procedural information to search, view, and create user information for the Serviceability Alarm Definitions.

This chapter contains the following topics:

Alarm definitions describe alarm messages: what they mean and how to recover from them.

You search the alarm definitions database for alarm information. When you click on any service-specific alarm, a description of the alarm information and a recommended action display.

Cisco Unified Presence stores alarm definitions and recommended actions in a standard query language (SQL) server database. The system administrator can search the database for definitions of all the alarms. The definitions include the alarm name, description, explanation, recommended action, severity, parameters, and monitors. This information aids the administrator in process of troubleshooting problems that Cisco Unified Presence encounters.

Viewing Alarm Definitions and Adding User-Defined Descriptions

This section describes how to search for and view an alarm definition.

Procedure

Step 1 Choose **Alarm** > **Definitions**.

The Alarm Message Definitions window displays.

Step 2 From the Equals field, choose a catalog of alarm definitions or enter the alarm name in the Enter Alarm Name field.

Step 3 Click the **Find** button.

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

Note 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. 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 4 In the list, click the hyperlink alarm definition for which you want alarm details.

The Alarm Details window displays.

Step 5 If you want to add information to the alarm, enter text in the User Defined Text box, and click the **Update** button.

Step 6 To return to the Alarm Message Definitions window, choose **Back to Find/List Alarms** from the Related Links drop-down list box and click **Go**.

Additional Information

See the Related Topics, page 4-3.

Alarm Definition Catalog Descriptions

Table 4-1 contains the alarm definition catalog descriptions.

Table 4-1 Alarm Definition Catalogs

Name	Description
CiscoUPSConfigAgent	All configuration agent alarms
CiscoUPSPresenceEngine	All presence engine alarms
CiscoUPSSIPProxy	All SIP proxy alarms
CiscoUPSSoap	All Cisco Unified Personal Communicator change notified alarms
CiscoUPSSyncAgent	All sync agent alarms
DBAlarmCatalog	All Cisco database (aupair) alarm definitions
DRFAlarmsCatalog	All Disaster Recovery Framework alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Cisco CallManager Java Applications alarm definitions **Note** You cannot configure JavaApplications alarms by using the alarm configuration windows. You generally configure these alarms to go to the Event Logs and to generate SNMP traps to integrate with CiscoWorks2000. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
LpmTctCatalog	All Log Partition Monitor Trace Collection Tool alarms
SystemAccessCatalog	All process and thread monitoring alarms
TFTPAlarmCatalog	All Cisco TFTP alarm definitions

Related Topics

- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 4-1
- Alarm Definition Catalog Descriptions, page 4-2

PART 4

Trace Configuration

CHAPTER 5

Trace Configuration

The Trace Configuration window allows you to specify the parameters that you want to trace for troubleshooting Cisco Unified Presence 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, and size of file). You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

After you have configured which information 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 the Real-Time Monitoring Tool (RTMT). For more information on collecting traces, see the "Trace Collection and Log Central in RTMT" section on page 10-1.

Note Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC.

This chapter contains the following topics:

Configuring Trace Parameters

This section describes how to configure trace parameters for Cisco Presence services.

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**.

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

Note The drop-down list box displays all services (active and inactive).

The trace parameters display for the service that you chose.

Note If you configured Troubleshooting Trace for this service, a message displays at the top of the window that indicates that Troubleshooting Traces have been set. The system disables all fields on the window except the Output Settings. To configure the Output Settings, go to Step 10. To reset Troubleshooting trace, see the "Troubleshooting Trace Setting Configuration" section on page 6-1.

Step 5 If you want trace to apply to all Cisco Unified Presence servers in the cluster, check the **Apply to All Nodes** check box.

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

Step 7 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 5-3.

Step 8 Check the Trace Fields check box for the service that you chose; for example, Cisco UPS SIP Proxy Trace Fields.

Step 9 If the service that you chose has multiple trace fields, such as the Cisco UP SIP Proxy service, check the check boxes next the trace fields that you want to enable. For a description of the Cisco UP SIP Proxy service trace filter setting, see Table 5-1.

Step 10 To limit the number and size of the trace files, specify the trace output setting. See Table 5-3 for descriptions and default values.

Step 11 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. 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.

Table 5-1 Cisco UP SIP Proxy Service Parameter Trace Filter Settings

Parameter	Description
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable IPPM Trace	This parameter enables tracing for IP Phone Messenger.

Table 5-1 Cisco UP SIP Proxy Service Parameter Trace Filter Settings

Parameter	Description
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.

Additional Information

See the Related Topics, page 5-5.

Debug Trace Level Settings

Table 5-2 describes the debug trace level settings for services.

Table 5-2 Debug Trace Levels for Services

Level	Description
Arbitrary	Traces all Entry/Exit conditions plus low-level debugging information. **Note** Do not use this trace level with the Cisco UPS Presence Engine service or the Cisco IP Voice Media Streaming Application service during normal operation.
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. Trace level that turns on all logging
Detailed	Traces all Arbitrary conditions plus detailed debugging information. **Note** Do not use this trace level with the Cisco UPS Presence Engine service or the Cisco IP Voice Media Streaming Application service during normal operation.
Entry/Exit	Traces all Significant conditions plus entry and exit points of routines. Not all services use this trace level (for example, Cisco Presence does not).

Table 5-2 Debug Trace Levels for Services (continued)

Level	Description
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.
Fatal	Traces very severe error events that may cause the application to abort.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.
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.
Warn	Traces potentially harmful situations.

Additional Information

See the Related Topics, page 5-5.

Trace Output Settings Descriptions and Defaults

Table 5-3 contains the trace log file descriptions and defaults.

Caution When you change either the Maximum No. of Files or Maximum File Size parameter, the system deletes all the service log files except the current file if the service is running, or, if the service has not been activated, the system will delete the files when the service is initially activated. If you want to keep a record of the log files, make sure that you download and save the service log files to another server before changing the Maximum No. of Files parameter or the Maximum File Size parameter.

Table 5-3 Trace Output Settings

Field	Description
Maximum number of files	This field specifies the total number of trace files for a given service. Cisco Unified Presence automatically appends a sequence number to the file name to indicate which file it is; for example, esp000005. 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, page 5-5.

Related Topics

- Configuring Trace Parameters, page 5-1
- Trace Output Settings Descriptions and Defaults, page 5-4
- Debug Trace Level Settings, page 5-3

CHAPTER 6

Troubleshooting Trace Setting Configuration

The Troubleshooting Trace Setting window allows you to choose the services in Cisco Unified Presence for which you want to set predetermined troubleshooting trace settings. This chapter contains information on how to set and reset troubleshooting trace setting for specific services.

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 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 display. The services that are not activated on a Cisco Unified Presence node display as N/A.

Step 3 Perform one of the following tasks:

- To check specific services for the node 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 node 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 node that you chose in the Server drop-down list box.
  - **Check Selected Services on All Nodes—**Allows you to check specific service check boxes in the TroubleshootingTrace Setting window. This setting applies for all nodes in the cluster where the service is activated.
  - **Check All Services on All Nodes** —Automatically checks all check boxes for all services for all nodes 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 node that you chose in the Server drop-down list box; also displays as an icon that you can click.
- **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all nodes in the cluster.

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

Note The Reset Troubleshooting Traces button displays only if you have set troubleshooting trace for one or more services.

Additional Information

See the Related Topics, page 6-2.

Related Topics

- Trace Configuration, page 5-1

PART 5

Monitoring Tools Configuration

CHAPTER 7

Real-Time Monitoring Configuration

This chapter contains the following information for configuring the Cisco Unified Presence Real-Time Monitoring Tool (RTMT).

Tip Ensure that the RTMT version that you install is compatible with the Cisco Unified CallManager version that runs in your cluster; for example, the RTMT version that supports Cisco Unified CallManager 5.X does not support Cisco Unified CallManager 6.X. The RTMT version that supports Cisco Unified CallManager 5.0 supports Cisco Unified CallManager 5.1.To monitor clusters that are running different versions of Cisco Unified CallManager versions simultaneously, you must install multiple versions of RTMT (one version per Cisco Unified CallManager release). If you install multiple versions of the plug-in, you can install the versions on the same client as long as the versions exist in different folders. If the installation detects another version in the folder, a message displays. To continue the installation, install the version in a different folder.

Tip For information on alert, performance monitoring, trace collection, and syslog viewer configuration, see the “Where to Find More Information” section on page 7-10.

Installing the Real-Time Monitoring Tool (RTMT)

You can install RTMT, which works for resolutions 800*600 and above, on a Windows 98, Windows XP, Windows 2000, or Red Hat Linux with KDE and/or Gnome client.

Note If you have previously installed RTMT for use with a Cisco Unified CallManager server that is running Microsoft Windows, you must install RTMT for Cisco Unified Presence in a different folder on your local computer.

To install the tool, perform the following procedure:

Procedure

Step 1 From Cisco Unified Presence Administration, choose **Application** > **Plugins**.

Step 2 Click the **Find** button.

Step 3 If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Presence Real-Time Monitoring Tool-Windows. If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified Presence Real-Time Monitoring Tool-Linux.

Step 4 Download the executable to your preferred location.

Step 5 To install the Windows version, double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file. The extraction process begins.

To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**.

Step 6 In the RTMT welcome window, click **Next**.

Step 7 To accept the license agreement, click **Yes**.

Step 8 Choose the location where you want to install RTMT. If you do not want to use the default location, click Browse and navigate to a different location. Click **Next**.

Step 9 To begin the installation, click **Next**.

The Setup Status window displays. Do not click Cancel.

Step 10 To complete the installation, click **Finish**.

Additional Information

See the Related Topics, page 7-10.

Upgrading RTMT

When you use the tool (RTMT), it saves user preferences and downloaded module jar files locally on the client machine. The system saves profiles in the Cisco Unified Presence database, so you can access these items in RTMT after you upgrade the tool.

Tip To ensure compatibility, Cisco recommends that you upgrade RTMT after you complete the Cisco Unified Presence upgrade on all servers in the cluster.

To upgrade RTMT, perform the following procedure:

Procedure

Step 1 From Cisco Unified Presence Administration, choose **Application** > **Plugins**.

Step 2 Click the **Find** button.

Step 3 If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Windows. If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Linux.

Step 4 Download the executable to your preferred location.

Step 5 To install the Windows version, double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file. The extraction process begins.

To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**.

Step 6 In the RTMT welcome window, click **Next**.

Step 7 Because you cannot change the installation location for upgrades, click **Next**.

The Setup Status window displays; do not click **Cancel**.

Step 8 In the Maintenance Complete window, click **Finish**.

Additional Information

See the Related Topics, page 7-10.

Uninstalling RTMT

Tip When you use RTMT, it saves user preferences and the module jar files (the cache) locally on the client machine. The system also saves the cache in the server database. When you uninstall RTMT, you choose whether to delete or save the cache.

On a Windows client, you uninstall RTMT through **Add/Remove Programs** under the Control Panel. (Start > Settings > Control Panel >Add/Remove Programs)

To uninstall RTMT on a Red Hat Linux with KDE and/or Gnome client, choose **Start** > **Accessories** > **Uninstall Real-time Monitoring tool** from the task bar.

Additional Information

See the Related Topics, page 7-10.

Launching RTMT

Before You Begin

Before you can use RTMT, you must activate the Cisco AMC Service on each node in the cluster. From Cisco Unified Presence Serviceability, choose **Tools > Service Activation** and check the **Cisco AMC Service** check box. Click **Update**.

Procedure

Step 1 After you install the plug-in, perform one of the following tasks:

- From your Windows desktop, double-click the **Cisco Unified CallManager Real-Time Monitoring Tool** icon.
- Choose **Start** > **Programs** > **Cisco CallManager Serviceability** > **Real-Time Monitoring Tool** > **Real-Time Monitoring Tool**.

The Real-Time Monitoring Tool Login window displays.

Step 2 In the Host IP Address field, enter either the IP address or host name of the first node.

Step 3 In the User Name field, enter the CCMAdministrator application user username; for example, the default username for this user equals **CCMAdministrator**.

Step 4 In the Password field, enter the CCMAdministrator application user password that you established for the username.

Note If the authentication fails or if the server is unreachable, the tool prompts you to reenter the server and authentication details, or you can click the Cancel button to exit the application. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote node, when the local cache does not contain a monitoring module that matches the backend Cisco Unified Presence version.

Step 5 Enter the port that the application will use to listen to the server. The default setting equals 8443.

Step 6 Check the **Secure Connection** check box.

Step 7 Click **OK**.

Step 8 Add the certificate store by clicking **Yes**.

Additional Information

See the Related Topics, page 7-10.

Navigating RTMT

The RTMT window comprises the following main components:

- Menu Bar, which includes the following menu options:
  - File—Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified Serviceability, log off or exit RTMT.

   - System—Allows you to monitor system summary, monitor server resources, work with performance counters, and work with alerts, collect traces, and view syslog messages.
   - CUP—Allows you to view Cisco Unified CallManager summary information on the server.
   - Edit—Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.
   - Window—Allows you to close a single RTMT window or all RTMT windows.
   - Application—Allows you to browse the web pages for Administration and Serviceability.
   - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—Pane on the left side of RTMT window with tabs that you can click on to display information on the server or information on the applications. The tab contain groups of icons that you can click on to monitor various objects.
- Monitor pane—Pane where monitoring results display.

Additional Information

See the Related Topics, page 7-10.

Working with Configuration Profiles

This section provides information on the following topics:

Using the Default Configuration Profile

When you initially load RTMT, the system includes a default profile that is called CM-Default. The first time that you use RTMT, it will use the CM-Default profile and display the summary page in the monitor pane.

See the "Adding Configuration Profiles" section on page 7-5 for information on how to create your own configuration profile.

Additional Information

See the Related Topics, page 7-10.

Adding Configuration Profiles

After you open multiple monitoring windows in RTMT (such as CPU & Memory, and performance counters), you can create your own configuration profiles, so you can restore these monitoring windows in a single step rather than opening each window again. You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

The following procedure describes how to create a profile.

Procedure

Step 1 Choose **System** > **Profile**.

The Preferences dialog box displays.

Step 2 Click **Save**.

The Save Current Configuration dialog box displays.

Step 3 In the Configuration name field, enter a name for this particular configuration profile.

Step 4 In the Configuration description field, enter a description of this particular configuration profile.

Note You can enter whatever you want for the configuration profile name and description.

The system creates the new configuration profile.

Additional Information

See the Related Topics, page 7-10.

Restoring Profiles

Perform the following procedure to restore a profile that you configured:

Procedure

Step 1 Choose **System** > **Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to restore.

Step 3 Click **Restore**.

All windows with precanned settings and/or performance monitoring counters for the restored configuration open.

Additional Information

See the Related Topics, page 7-10.

Deleting Configuration Profiles

Perform the following procedure to delete a profile that you configured:

Procedure

Step 1 Choose **System** > **Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Close**.

Additional Information

See the Related Topics, page 7-10.

Working with Predefined Objects

The tool (RTMT) provides a set of default monitoring objects that monitor the health of the system. Default objects include performance counters or critical event status for services that are supported with Cisco Unified Presence.

This section provides information on the following topics:

Viewing/Monitoring a Predefined Object

The monitoring pane for a category, that is, a predefined object, displays the activities of predefined monitoring objects. The following procedure describes how to view information for a category.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the "**R**" key.

Procedure

Step 1 To view or monitor a category, click System or CUP in the Quick Launch Channel.

When you select System in the quick launch channel, RTMT displays information on predefined system objects, such as virtual memory usage. When you select CUP in the quick launch channel, RTMT displays information on predefined Cisco Unified Presense Server objects in the monitoring pane, such as PE Active Subscription. RTMT monitors the predefined objects on all nodes in the cluster.

Step 2 Click a category; for example, Summary or Server. If an icon displays for the category, click the icon to display the information that you want to monitor.

> **Note** Some options that are in in the current version of RTMT do not apply to Cisco Unified Presence.

Step 3 Depending on which category you want to display, choose one of the following options from Table 7-1:

Table 7-1 Monitoring Categories

Category	Data that Displays
CUP Summary	Displays information on PE Active Subscription, Proxy SIP Message Requests In, Proxy SIP Message Requests Out, Proxy SIP Register Requests In, Proxy SIP Subscribe Requests In, and JVM Memory. To display information on predefined system objects, choose **CUP > CUP Summary**.
System Summary	Displays information on Virtual Memory usage, CPU usage, Common Partition Usage, and the alert history log.To display information on predefined system objects, choose **System > System Summary**.
Server	• CPU and Memory—Displays information on CPU usage and Virtual memory usage for each server. To display information on CPU and Virtual memory usage, choose **System > Server > CPU and Memory**.To monitor CPU and memory usage for specific server, choose the server from the host drop-down list box. • Process—Displays information on the processes that are running on each server. To display information on processes running on the system, choose **System > Server > Process**. To monitor process usage for specific server, choose the server from the Host drop-down list box. • Disk Usage—Displays information on disk usage on each server.To display information on disk usage on the system, choose **System > Server > Disk Usage**. To monitor disk usage for specific server, choose the server from the host drop-down list box. • Critical Services—Displays information on the status of services that are running on the server. To display information on critical services, choose **System > Server > Critical Services**. To display system critical services, click the System tab. To display Cisco Unified Presense Server critical services, click on the CUP tab. To monitor Critical services for specific server, choose the server from the host drop-down list box.
Performance	Displays perfmon counters. To display perfmon counters, choose System > Performance > Performance. For more information on using perfmon counters, see the “Configuring and Using Performance Monitoring” section on page 9-1.

Additional Information

See the Related Topics, page 7-10.

Configuring Polling Rate Performance Monitoring Counters

Cisco Unified Presence polls counters to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance-monitoring counters.

Note High-frequency polling rate may adversely affect Cisco Unified Presence performance. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default value for both equals 10 seconds.

The default value for devices equals 10 minutes.

Perform the following procedure to update the polling rate:

Procedure

Step 1 Display the performance-monitoring counter in the RTMT monitoring pane.

Step 2 Click the device and choose **Edit > Polling Rate**.

Step 3 In the Polling Interval pane, specify the time that you want to use.

Step 4 Click **OK**.

Additional Information

See the Related Topics, page 7-10.

Working with Categories

Categories allow you to monitor performance-monitoring counters. For example, the category, Cisco UP SIP Proxy, allows you to monitor performance-monitoring counters in graph format for the SIP proxy. If you want to monitor more counters, you can configure a new category and display the data in table format.

Adding a Category

To add a category, perform the following procedure:

Procedure

Step 1 Display the Performance Monitoring tree hierarchy.

Step 2 Choose **Edit > New Category**.

Step 3 Enter the name of the category; click **OK**.

The category tab displays at the bottom of the window.

Additional Information

- See the Related Topics, page 7-10.

Renaming a Category

To rename a category, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Right-click the category tab that you want to rename and choose **Rename Category**.
- Click the category tab that you want to rename and choose **Edit > Rename Category**.

Step 2 Enter the new name and click **OK**.

The renamed category displays at the bottom of the window.

Additional Information

- See the Related Topics, page 7-10.

Deleting a Category

To delete a category, perform one of the following tasks:

- Right-click the category tab that you want to delete and choose **Remove Category**.
- Click the category tab that you want to delete and choose **Edit > Remove Category**.

Additional Information

See the Related Topics, page 7-10.

Where to Find More Information

- Alert Configuration in RTMT, page 8-1
- Configuring and Using Performance Monitoring, page 9-1
- Trace Collection and Log Central in RTMT, page 10-1

Additional Information

See the Related Topics, page 7-10.

Related Topics

- Adding a Category, page 7-9
- Renaming a Category, page 7-10
- Deleting a Category, page 7-10
- Configuring and Using Performance Monitoring, page 9-1
- Configuring Polling Rate Performance Monitoring Counters, page 7-8

- Configuring Polling Rate Performance Monitoring Counters, page 7-8
- Using the Default Configuration Profile, page 7-5
- Restoring Profiles, page 7-6
- Using the Default Configuration Profile, page 7-5
- Deleting Configuration Profiles, page 7-6
- Adding Configuration Profiles, page 7-5
- Working with Configuration Profiles, page 7-5
- Working with Predefined Objects, page 7-7
- Alert Configuration in RTMT, page 8-1
- Configuring and Using Performance Monitoring, page 9-1
- Using SysLog Viewer in RTMT, page 11-1
- Installing the Real-Time Monitoring Tool (RTMT), page 7-2
- Navigating RTMT, page 7-4
- Uninstalling RTMT, page 7-3
- Upgrading RTMT, page 7-2
- Launching RTMT, page 7-4

CHAPTER 8

Alert Configuration in RTMT

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under different tabs—System, CUP, and Custom. You can configure both kinds of alerts, but you cannot delete preconfigured alerts. You can disable both preconfigured and user-defined alerts in RTMT.

For information on preconfigured alerts, alert customization, and alert action fields in which you can configure alerts, refer to “Alerts” in the *Cisco Unified CallManager Serviceability System Guide*.

When an activated service goes from up to down, RTMT generates an alert. You use Alert Central to view the status and history of the alerts that RTMT generates.

This chapter provides information on the following topics:

Working with Alerts

By using the following procedure, you can perform tasks, such as access Alert Central, sort alert information, enable, disable, or remove an alert, clear an alert, or view alert details.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel:
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the Alert Central icon.
- Choose **System** > **Tools** > **Alert** > **Alert Central**.

The Alert Central monitoring window displays and shows the alert status and alert history of the alerts that the system has generated.

Step 2 Perform one of the following tasks:

- To set alert properties, see the "Setting Alert Properties" section on page 8-2.
- To suspend alerts on Cisco Unified Presence nodes, see the "Suspending Alerts on Cisco Unified Presence Nodes or the Cluster" section on page 8-5.
- To configure e-mails for alert notification, see the "Configuring E-mails for Alert Notification" section on page 8-5.
- To configure alert actions, see the "Configuring Alert Actions" section on page 8-6.
- To sort alert information in the Alert Status pane, click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or InSafeRange column.

  You can sort alert history information by clicking the up/down arrow in the columns in the Alert History pane. To see alert history that is out of view in the pane, use the scroll bar on the right side of the Alert History pane.
- To enable, disable, or remove an alert, perform one of the following tasks:
  - From the Alert Status window, right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
  - Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Disable/Enable** (or **Remove**) **Alert**.

Tip You can only remove user-defined alerts from RTMT. The Remove Alert option appears grayed out when you choose a preconfigured alert.

- To clear either individual or collective alerts after they get resolved, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Clear Alert** (or **Clear All Alerts**).
  - Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Clear Alert** (or **Clear All Alerts)**.

  After you clear an alert, it changes from red to black.
- To view alert details, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Alert Details**.
  - Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Alert Details**.

Tip After you have finished viewing the alert details, click **OK**.

Additional Information

See the Related Topics, page 8-6.

Setting Alert Properties

The following procedure describes how to set alert properties.

Procedure

Step 1 Display Alert Central, as described in the "Working with Alerts" section on page 8-1.

Step 2 From the Alert Status window, click the alert for which you want to set alert properties.

Step 3 Perform one of the following tasks:

- Right-click the alert and choose **Set Alert/Properties**.
- Choose **System** > **Tools** > **Alert** > **Set Alert/Properties**.

Note For Cisco Unified Presence clusterwide alerts, the Enable/Disable this alert on following server(s): box does not show up in the alert properties window. Clusterwide alerts include number of registered phones, gateways, media devices, route list exhausted, media list exhausted, MGCP D-channel out of service, malicious call trace, and excessive quality reports.

Step 4 To enable the alert, check the **Enable Alert** check box.

Step 5 From the Severity drop-down list box, choose the severity of the alert.

Step 6 From the Enable/Disable this alert on following server(s) pane, check the Enable check box of the servers on which you want this alert to be enabled.

For preconfigured alerts, the Description information pane displays a description of the alert.

Step 7 Click **Next**.

Step 8 In the Threshold pane, enter the conditions in which the system triggers the alert.

Step 9 In the Duration pane, click one of the following radio buttons:

- Trigger alert only when below or over.... radio button—If you want the alert to be triggered only when the value is constantly below or over the threshold for a specific number of seconds; then, enter the seconds.
- Trigger alert immediately—If you want the system to trigger an alert immediately.

Step 10 Click **Next**.

Step 11 In the Frequency pane, click one of the following radio buttons:

- trigger alert on every poll—If you want the alert to be triggered on every poll.
- trigger up to <numbers> of alerts within <number> of minutes—If you want a specific number of alerts to be triggered within a specific number of minutes. Enter the number of alerts and number of minutes.

Step 12 In the Schedule pane, click one of the following radio buttons:

- 24-hours daily—If you want the alert to be triggered 24 hours a day.
- Start time/Stop time—If you want the alert to be triggered within a specific start and stop time. Enter the start and stop times.

Step 13 Click **Next**.

Step 14 If you want to enable e-mail for this alert, check the Enable Email check box.

Step 15 To trigger an alert action with this alert, choose the alert action that you want to send from the drop-down list box.

Step 16 To configure a new alert action, or edit an existing one, click **Configure**.

Step 17 To add a new alert action, perform the following procedure:

a. Click **Add**.

b. In the Name field, enter a name for the alert action.

c. In the Description field, enter a description of the alert action.

d. To add an e-mail recipient, click **Add**.

e. In the Enter email/epage address field, enter an e-mail or e-page address of the recipient that you want to receive the alert action.

f. Click **OK**.

The Action Configuration window shows the recipient(s) that you added, and the Enable check box appears checked.

Tip To delete an e-mail recipient, highlight the recipient and click **Delete**. The recipient that you chose disappears from the recipient list.

g. When you finish adding all the recipients, click **OK**.

Step 18 To edit an existing alert action, perform the following procedure:

a. Highlight the alert action and click **Edit**.

The Action Configuration window of the alert action that you chose displays.

b. Update the configuration and click **OK**.

Step 19 After you finish alert action configuration, click **Close**.

Step 20 For alerts that do not allow trace download, click **Activate** in the Alert Properties: Email Notification window.

For alerts, such as CriticalServiceDown and CodeYellow, that allow trace download, perform the following procedure:

a. Click **Next.**

b. In the Alert Properties: TCT Download window, check the Enable TCT Download check box.

c. The SFTP Parameters Dialog window displays. Enter the IP address, a user name, password, port and download directory path where the trace will be saved. To ensure that you have connectivity with the SFTP server, click **Test Connection**. **If the connection test fails, your settings will not be saved.**

d. To save your configuration, click **OK.**

e. In the TCT Download Parameters window, enter the number and frequency of downloads. Setting the number and frequency of download will help you to limit the number of trace files that will be downloaded. The setting for polling provides the basis for the default setting for the frequency.

Caution Enabling TCT Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Note To delete an alert action, highlight the action, click **Delete**, and click **Close**.

Additional Information

See the Related Topics, page 8-6.

Suspending Alerts on Cisco Unified Presence Nodes or the Cluster

You may want to temporarily suspend some or all alerts, either on a particular Cisco Unified Presence node or the entire cluster. For example, if you are upgrading the Cisco Unified Presence to a newer release, you would probably want to suspend all alerts until the upgrade completes, so you do not receive e-mails and/or e-pages during the upgrade. The following procedure describes how to suspend alerts in Alert Central.

Procedure

Step 1 Choose **System** > **Tools** > **Alert** > **Suspend cluster/node Alerts**.

> **Note** Per server suspend states do not apply to Cisco Unified Presence clusterwide alerts.

Step 2 To suspend all alerts in the cluster, choose the Cluster Wide radio button and check the suspend all alerts check box.

Step 3 To suspend alerts per server, choose the Per Server radio button and check the Suspend check box of each server on which you want alerts to be suspended.

Step 4 Click **OK**.

> **Note** To resume alerts, choose **Alert** > **Suspend cluster/node Alerts** again and uncheck the suspend check boxes.

Additional Information

See the Related Topics, page 8-6.

Configuring E-mails for Alert Notification

Perform the following procedure to configure e-mail information for alert notification.

Procedure

Step 1 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

The Mail Server Configuration window displays.

Step 2 In the Mail Server field, enter the e-mail recipient information.

Step 3 In the Port field, enter the port number of the mail server.

Step 4 Click **OK**.

Additional Information

See the Related Topics, page 8-6.

Configuring Alert Actions

The following procedure describes how to configure new alert actions.

Procedure

Step 1 Display Alert Central, as described in the "Working with Alerts" section on page 8-1.

Step 2 Choose **Alert > Config Alert Action**.

Step 3 Perform Step 17 through Step 20 in the "Setting Alert Properties" section on page 8-2 to add, edit, or delete alert actions.

Additional Information

See the Related Topics, page 8-6.

Related Topics

- Working with Alerts, page 8-1
- Setting Alert Properties, page 8-2
- Suspending Alerts on Cisco Unified Presence Nodes or the Cluster, page 8-5
- Configuring E-mails for Alert Notification, page 8-5
- Configuring Alert Actions, page 8-6

CHAPTER 9

Configuring and Using Performance Monitoring

You can monitor the performance of Cisco Unified Presence by choosing the counters for any object by using RTMT. The counters for each object display when the folder expands.

You can log perfmon counters locally on the computer and use the performance log viewer in RTMT to display the perfmon CSV log files that you collected or the Alert Manager and Collector (AMC) perfmon logs and Realtime Information Server Data Collection (RISDC) perfmon logs.

You can also enable troubleshooting perfmon data logging to automatically collect statistics from a set of perfmon counters that will provide comprehensive information on the system state. Be aware that enabling troubleshooting perfmon data logging may impact system performance on the server.

This chapter contains information on the following topics:

Displaying Performance Counters

RTMT displays perfmon counters in chart or table format. The chart format displays the perfmon counter information by using line charts. For each category tab that you create, you can display up to six charts in the RTMT Perfmon Monitoring pane with up to three counters in one chart.

Tip You can display up to three counters in one chart in the RTMT Perfmon Monitoring pane. To add another counter in a chart, click the counter and drag it to the RTMT Perfmon Monitoring pane. Repeat again to add up to three counters.

By default, RTMT displays perfmon counters in a chart format. You can also choose to display the perfmon counters in a table format. To display the perfmon counters in table format, you need to check the **Present Data in Table View** check box when you create a new category.

You can organize the perfmon counters to display a set of feature-based counters and save it in a category. After you save your RTMT profile, you can quickly access the counters that you are interested in. After you create a category, you cannot change the display from a chart format to a table format, or vice versa.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel:
  - Click **System**.
  - In the tree hierarchy, double-click **Performance**.
  - Click the **Performance** icon.
- Choose **System** > **Performance** > **Open Performance Monitoring**.

Step 2 Click the name of the server where you want to add a counter to monitor.

The tree hierarchy expands and displays all the perfmon objects for the node.

Step 3 To monitor a counter in table format, see Step 4. To monitor a counter in chart format, see Step 5.

Step 4 To monitor a counter in table format, perform the following procedure.

a. Choose **Edit** > **New Category**.

b. In the Enter Name field, enter a name for the tab.

c. To display the perfmon counters in table format, check the **Present Data in Table View** check box.

d. Click **OK**.

A new tab with the name that you entered displays at the bottom of the pane.

e. Click the file icon next to the object name that lists the counters that you want to monitor.

Tip To display the counter in chart format after you display it in table format, right-click the category tab and choose **Remove Category**. The counter displays in chart format.

Step 5 To monitor a counter in chart format, perform the following tasks:

- Click the file icon next to the object name that lists the counters that you want to monitor.

  A list of counters displays.
- To display the counter information, either right-click the counter and click **Counter Monitoring**, double-click the counter, or drag and drop the counter into the RTMT Perfmon Monitoring pane.

The counter chart displays in the RTMT Perfmon Monitoring pane.

Additional Information

See the "Related Topics" section on page 9-11.

Removing a Counter from the RTMT Performance Monitoring Pane

You can remove counters from the RTMT Perfmon Monitoring pane when you no longer need them. This section describes how to remove a counter from the pane.

Perform one of the following tasks:

- Right-click the counter that you want to remove and choose **Remove**.
- Click the counter that you want to remove and choose **Perfmon** > **Remove Chart/Table Entry**.

The counter no longer displays in the RTMT Perfmon Monitoring pane.

Additional Information

See the "Related Topics" section on page 9-11.

Adding a Counter Instance

To add a counter instance, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counter, as described in the "Displaying Performance Counters" section on page 9-1.

Step 2 Perform one of the following tasks:

- Double-click the performance monitoring counter in the performance monitoring tree hierarchy.
- Click the performance monitoring counter in the performance monitoring tree hierarchy and choose **System** > **Performance** > **Counter Instances**.
- Right-click the performance monitoring counter in the performance monitoring tree hierarchy and choose **Counter Instances**.

Step 3 In the Select Instance window, click the instance; then, click **Add**.

The counter displays.

Additional Information

See the "Related Topics" section on page 9-11.

Configuring Alert Notification for a Counter

The following procedure describes how to configure alert notification for a counter.

Tip To remove the alert for the counter, right-click the counter and choose Remove Alert. The option appears gray after you remove the alert.

Procedure

Step 1 Display the performance counter, as described in the "Displaying Performance Counters" section on page 9-1.

Step 2 From the counter chart or table, right-click the counter for which you want to configure the alert notification, and choose **Set Alert/Properties**.

Step 3 Check the **Enable Alert** check box.

Step 4 In the Severity drop-down list box, choose the severity level at which you want to be notified.

Step 5 In the Description pane, enter a description of the alert.

Step 6 Click **Next**.

Step 7 Use Table 9-1 to configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes. After you enter the settings in the window, click **Next** to proceed to the next panes.

Table 9-1 Counter Alert Configuration Parameters

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	Check the check box and enter the value that applies. • Over—Check this check box to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress. • Under—Check this check box to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress. **Tip** Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.
Value Calculated As Pane	
Absolute, Delta, Delta Percentage	Click the radio button that applies. • Absolute—Because some counter values are accumulative (for example, CallsAttempted or CallsCompleted), choose Absolute to display the data at its current status. • Delta—Choose Delta to display the difference between the current counter value and the previous counter value. • Delta Percentage—Choose Delta Percentage to display the counter performance changes in percentage.
Duration Pane	
Trigger alert only when value constantly...; Trigger alert immediately	• Trigger alert only when value constantly...—If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent. • Trigger alert immediately—If you want the alert notification to be sent immediately, click this radio button.

Table 9-1 Counter Alert Configuration Parameters (continued)

Setting	Description
Frequency Pane	
Trigger alert on every poll; trigger up to...	Click the radio button that applies. • Trigger alert on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button. If the calls in progress continue to go over or under the threshold, the system does not send another alert notification. When the threshold is normal (between 50 and 100 calls in progress), the system deactivates the alert notification; however, if the threshold goes over or under the threshold value again, the system reactivates alert notification. • Trigger up to...—If you want the alert notification to activate at certain intervals, click this radio button and enter the number of alerts that you want sent and the number of minutes within which you want them sent.
Schedule Pane	
24-hours daily; start/stop	Click the radio button that applies: • 24-hours daily—If you want the alert to be triggered 24 hours a day, click this radio button. • Start/Stop—If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If the check box is checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.

Step 8 If you want the system to send an e-mail message for the alert, check the **Enable Email** check box.

Step 9 If you want to trigger an alert action that is already configured, choose the alert action that you want from the Trigger Alert Action drop-down list box.

Step 10 If you want to configure a new alert action for the alert, click **Configure**.

Note Whenever the specified alert is triggered, the system sends the alert action.

The Alert Action dialog box displays.

Step 11 To add a new alert action, click **Add**.

The Action Configuration dialog box displays.

Step 12 In the Name field, enter a name for the alert action.

Step 13 In the Description field, enter a description for the alert action.

Step 14 To add a new e-mail recipient for the alert action, click **Add**.

The Input dialog box displays.

Step 15 Enter either the e-mail or e-page address of the recipient that you want to receive the alert action notification.

Step 16 Click **OK**.

The recipient address displays in the Recipient list. The Enable check box gets checked.

Tip To disable the recipient address, uncheck the Enable check box. To delete a recipient address from the Recipient list, highlight the address and click **Delete**.

Step 17 Click **OK**.

Step 18 The alert action that you added displays in Action List.

Tip To delete an alert action from the action list, highlight the alert action and click **Delete**. You can also edit an existing alert action by clicking **Edit**.

Step 19 Click **Close**.

Step 20 In the User-defined email text box, enter the text that you want to display in the e-mail message.

Step 21 Click **Activate**.

Additional Information

See the "Related Topics" section on page 9-11.

Zooming a Counter

To get a closer look at perfmon counters, you can zoom the perfmon monitor counter in the RTMT Perfmon Monitoring pane.

Procedure

Step 1 Perform one of the following tasks:

- In the RTMT Performance Monitoring pane, double-click the counter that you want to zoom. The box with the counter appears highlighted, and the Zoom window automatically displays.
- In the RTMT Performance Monitoring pane, click the counter that you want to zoom. The box with the counter appears highlighted. Choose **System** > **Performance** > **Zoom Chart**. The Zoom window automatically displays.

The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

Step 2 To close the window, click **OK**.

Additional Information

See the "Related Topics" section on page 9-11.

Displaying a Counter Description

Use one of two methods to obtain a description of the counter:

Procedure

Step 1 Perform one of the following tasks:

- In the Perfmon tree hierarchy, right-click the counter for which you want property information and choose **Counter Description**.
- In the RTMT Performance Monitoring pane, click the counter and choose **System** > **Performance** > **Counter Description**.

Tip To display the counter description and to configure data-sampling parameters, see the "Configuring a Data Sample" section on page 9-7.

The Counter Property window displays the description of the counter. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

Step 2 To close the Counter Property window, click **OK**.

Additional Information

See the "Related Topics" section on page 9-11.

Configuring a Data Sample

The Counter Property window contains the option to configure data samples for a counter. The perfmon counters that display in the RTMT Perfmon Monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option. See the "Viewing Counter Data" section on page 9-8.

This section describes how to configure the number of data samples to collect for a counter.

Procedure

Step 1 Display the counter, as described in the "Displaying Performance Counters" section on page 9-1.

Step 2 Perform one of the following tasks:

- Right-click the counter for which you want data sample information and choose **Monitoring Properties** if you are using chart format and **Properties** if you are using table format.
- Click the counter for which you want data sample information and choose **System** > **Performance** > **Monitoring Properties**.

The Counter Property window displays the description of the counter, as well as the tab for configuring data samples. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

Step 3 To configure the number of data samples for the counter, click the **Data Sample** tab.

Step 4 From the No. of data samples drop-down list box, choose the number of samples (between 100 and 1000). The default specifies 100.

Step 5 From the No. of data points shown on chart drop-down list box, choose the number of data points to display on the chart (between 10 and 50). The default specifies 20.

Step 6 Click one parameter, as described in Table 9-2.

Table 9-2 Data Sample Parameters

Parameter	Description
Absolute	Because some counter values are cumulative (for example, CallsAttempted or CallsCompleted), choose Absolute to display the data at its current status.
Delta	Choose Delta to display the difference between the current counter value and the previous counter value.
Delta Percentage	Choose Delta Percentage to display the counter performance changes in percentage.

Step 7 To close the Counter Property window and return to the RTMT Perfmon Monitoring pane, click the **OK** button.

Additional Information

See Related Topics, page 9-11.

Viewing Counter Data

Perform the following procedure to view the data that is collected for a performance counter.

Procedure

Step 1 In the RTMT Perfmon Monitoring pane, right-click the counter chart for the counter for which you want to view data samples and choose **View All Data**.

The counter chart displays all data that has been sampled. The green dots display close together, almost forming a solid line.

Step 2 Right-click the counter that currently displays and choose **View Current**.

The counter chart displays the last configured data samples that were collected. See the "Configuring a Data Sample" section on page 9-7 procedure for configuring data samples.

Additional Information

See "Related Topics" section on page 9-11.

Local Logging of Data from Perfmon Counters

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer. See "Displaying Log Files on the Perfmon Log Viewer" section on page 9-10.

Starting the Counter Logs

To start logging perfmon counter data into a CSV log file, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counters, as described in the "Displaying Performance Counters" section on page 9-1.

Step 2 If you are displaying perfmon counters in the chart format, right-click the graph for which you want data sample information and choose **Start Counter(s) Logging**. If you want to log all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Start Counter(s) Logging.**

The Counter Logging Configuration dialog box displays.

Step 3 In the Logger File Name field, enter a file name and choose OK.

RTMT saves the CSV log files in the log folder in the .jrtmt directory under the user home directory. For example, in Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.

To limit the number and size of the files, specify the maximum file size and maximum number of files parameter in the trace output settings. See "Configuring Trace Parameters" section on page 5-1.

Stopping the Counter Logs

To stop logging perfmon counter data, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counters, as described in the "Displaying Performance Counters" section on page 9-1.

Step 2 If you are displaying perfmon counters in the chart format, right-click the graph for which counter logging is started and choose **Stop Counter(s) Logging.** If you want to stop logging of all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Stop Counter(s) Logging**.

Displaying Log Files on the Perfmon Log Viewer

The Performance Log Viewer displays data for counters from perfmon CSV log files in a graphical format. You can use the performance log viewer to display data from the local perfmon logs that you collected, or you can display the data from the Alert Manager and Collector (AMC) perfmon logs and Realtime Information Server Data Collection (RISDC) perfmon logs.

The local perfmon logs consist of data from counters that you choose and store locally on your computer. For more information on how to choose the counters and how to start and stop local logging, see "Local Logging of Data from Perfmon Counters" section on page 9-9.

When you enable AMC and RISDC perfmon logs, Cisco Unified Presence collects information for the system in logs that are written on the Cisco Unified Presence. You can enable or disable AMC and RISDC perfmon logs on Cisco Unified Presence Administration by choosing **System > Service Management**. By default, AMC perfmon logging is enabled and RISDC perfmon logging is disabled. RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects data that are used to troubleshoot problems. Because Cisco Unified Presence collects a large amount of data in a short period of time, you should limit the time that RISDC perfmon data logging (troubleshooting perfmon data logging) is enabled.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel:
  - Click **System**.
  - In the tree hierarchy, double-click **Performance**.
  - Click the **Performance Log Viewer** icon.
- Choose **System > Performance > Open Performance Log Viewer**.

Step 2 Choose the type of perfmon logs that you want to view:

- For AMC or RisDC Perfmon Logs, perform the following steps:
  a. Click on either AMC Perfmon Logs or Perfmon Logs and choose a node from the Select a node drop-down box.
  b. Click **Open**.

     The File Selection Dialog Box displays.
  c. Choose the file and Click **Open File**.

     The Select Counters Dialog Box displays.
  d. Choose the counters that you want to display by checking the check box next to the counter.
  e. Click **OK**.
- For locally stored data, perform the following steps:
  a. Click Local Perfmon Logs.
  b. Click **Open**.

     The File Selection Dialog Box displays. RTMT saves the perfmon CSV log files in the log folder in the .jrtmt directory under the user home directory. In Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.

c. Browse to the file directory.

d. Choose the file that you are interested in viewing or enter the file name in the filename field.

e. Click **Open**.

The Select Counters Dialog Box displays.

f. Choose the counters that you want to display by checking the check box next to the counter.

g. Click **OK**.

The performance log viewer displays a chart with the data from the selected counters. The bottom pane displays the selected counters, a color legend for those counters, display option, mean value, minimum value, and the maximum value.

Table 9-3 describes the functions of different buttons that are available on the performance log viewer.

Tip You can order each column by clicking on a column heading. The first time that you click on a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the records displays in the unsorted state.

Table 9-3 Performance Log Viewer

Button	Function
Select Counters	Allows you to add counters that you want to display in the performance log viewer. To not display a counter, uncheck the Display column next to the counter.
Reset View	Resets the performance log viewer to the initial default view.
Save Downloaded File	Allows you to save the log file to your local computer.

Zooming In and Out

The performance Log viewer includes a zoom feature that allows you to zoom in on an area in the chart. To zoom in, click and drag the left button of the mouse until you have the desired area selected.

To reset the chart to the initial default view, click **Reset View** or right-mouse click the chart and choose **Reset**.

Related Topics

- Displaying Performance Counters, page 9-1
- Removing a Counter from the RTMT Performance Monitoring Pane, page 9-3
- Configuring Alert Notification for a Counter, page 9-3
- Zooming a Counter, page 9-6
- Displaying a Counter Description, page 9-7

- Configuring a Data Sample, page 9-7
- Viewing Counter Data, page 9-8
- Local Logging of Data from Perfmon Counters, page 9-9
- Displaying Log Files on the Perfmon Log Viewer, page 9-10

CHAPTER 10

Trace Collection and Log Central in RTMT

The trace and log central feature in the Cisco Unified Presence real-time monitoring tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to an SFTP server on your network, or collect a crash dump file. After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool.

Note From RTMT, you can also edit the trace setting for the traces on the node that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.

Note To use the trace and log central feature in the RTMT, make sure that RTMT can access all of the nodes in the cluster directly without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the Cisco Unified Presence with a hostname instead of an IP address and make sure that the host names and their routable IP address are in the DNS server or host file.

Note For devices that support encryption, the SRTP keying material does not display in the trace file.

This chapter contains information on the following topics:

Importing Certificates

You can import the server authentication certificate that the certificate authority provides for each server in the cluster. Cisco recommends that you import the certificates before using the trace and log central option. If you do not import the certificates, the trace and log central option displays a security certificate for each node in the cluster each time that you log into RTMT and access the trace and log central option. You cannot change any data that displays for the certificate.

To import the certificate, choose **System** > **Tools** > **Trace** > **Import Certificate**.

A messages displays that states that the system completed the importing of server certificates. Click **OK**.

Displaying Trace & Log Central Options in RTMT

Before you begin, make sure that you have imported the security certificates as described in the "Importing Certificates" section on page 10-2.

To display the Trace & Log Central tree hierarchy, perform one of the following tasks:

- In the Quick Launch Channel, click **System**; in the tree hierarchy, double-click **Tools**; then, click the **Trace & Log Central** icon.
- Choose **System** > **Tools** > **Trace** > **Open Trace & Log Central**.

Tip From any option that displays in the tree hierarchy, you can specify the services/applications for which you want traces, specify the logs and servers that you want to use, schedule a collection time and date, configure the ability to download the files, configure zip files, and delete collected trace files.

After you display the Trace & Log Central options in the real-time monitoring tool, perform one of the following tasks:

- Collect traces for services, applications, and system logs on one or more servers in the cluster. See "Collecting Traces" section on page 10-3
- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use. See "Using the Query Wizard" section on page 10-5
- Schedule a recurring trace collection and download the trace files to an SFTP server on your network. See "Scheduling Trace Collection" section on page 10-9
- Collect a crash dump file for one or more servers on your network. See "Collecting a Crash Dump" section on page 10-12.
- View the trace files that you have collected. See the "Using Local Browse" section on page 10-14.
- View all of the trace files on the server. See the "Using Remote Browse" section on page 10-15.
- View the current trace file that is being written on the server for each application. You can perform a specified action when a search string appears in the trace file. See "Using Real Time Trace" section on page 10-18.

Collecting Traces

Use the Collect Traces option of the trace and log central feature to collect traces for services, applications, and system logs on one or more servers in the cluster. You specify date/time range for which you want to collect traces, the directory in which to download the trace files, whether to delete the collected files from the server, and so on. The following procedure describes how to collect traces by using the trace and log central feature.

Note The services that you have not activated also display, so you can collect traces for those services.

If you want to collect trace files that contain search criteria that you specify or you want to use trace collection criteria that you saved for later use, see the "Using the Query Wizard" section on page 10-5.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window. For more information, see the "Trace Configuration" section on page 5-1.
- If you want alarms to be sent to a trace file, choose an SDI trace file as the alarm destination in the Alarm Configuration window. For more information, see the "Alarm Configuration" section on page 3-1.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 In the tree hierarchy, double-click **Collect Files**.

The Select CUP Services/Applications tab displays.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Step 3 Perform one of the following tasks:

- To collect traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the trace collection wizard without collecting traces for services or applications, go to Step 4.

Note The services that you have not activated also display, so you can collect traces for those services.

> **Note** You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the server on which you have activated the service/application.

Step 4 Click **Next**.

The Select System Services/Applications tab displays.

Step 5 Perform one of the following tasks:

- To collect all system logs for all servers in the cluster, check the **Select All Logs on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.

  For example, to collect CSA logs, check the Cisco Security Agent check box in the Select System Logs tab. 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.
- To continue the trace collection wizard without collecting traces for system logs, go to Step 6.

Step 6 Click **Next**.

Step 7 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  The trace files that get modified in the date range (between the From date and the To date), get collected if the chosen time zone matches the time zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), but that server resides in a different time zone, then the trace files that get modified in the corresponding date range in Server 2 will get collected from Server 2.

  To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.
- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 8 From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

Cisco Unified Presence Serviceability stores logs for up to two Linux-based versions of Cisco Unified Presence. Cisco Unified Presence Serviceability stores the logs for the version of Cisco Unified Presence that you are logged in to in the active partition and stores the logs for the other version of Cisco Unified Presence (if installed) in the inactive directory.

So, when you upgrade from one version of Cisco Unified Presence that is running on the Linux platform to another and log in to the new version of Cisco Unified Presence that is running on the Linux platform, Cisco Unified Presence Serviceability moves the logs from the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version of

Cisco Unified Presence, Cisco Unified Presence Serviceability moves the logs for the newer version of Cisco Unified Presence to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Presence Serviceability does not retain logs from Cisco Unified Presence versions that ran on the Windows platform.

Step 9 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.

Step 10 To create a zip file of the trace files that you collect, choose the **Zip File** radio button. To download the trace files without zipping the files, choose the **Do Not Zip Files** radio button.

Step 11 To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.

Step 12 Click **Finish**.

The window shows the progress of the trace collection. If you want to stop the trace collection, click **Cancel**.

When the trace collection process is complete, the message "Completed downloading for node <IP address>" displays at the bottom of the window.

Step 13 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature. For more information, see the "Using Local Browse" section on page 10-14.

Additional Information

See the Related Topics, page 10-21.

Using the Query Wizard

The Trace Collection Query Wizard allows you to collect and download trace files that contain search criteria that you specify as well as to save trace collection criteria for later use. To use the Trace Collection Query Wizard, perform the following procedure.

Before You Begin

Perform one or more of the following tasks:

- From the Trace Configuration window, configure the information that you want to include in the trace files for the various services. For more information, see the "Trace Configuration" section on page 5-1.
- If you want alarms to be sent to a trace file, choose an SDI trace file as the alarm destination in the Alarm Configuration window. For more information, see the "Alarm Configuration" section on page 3-1.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 In the tree hierarchy, double-click **Query Wizard**.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Step 3 In the window that opens, click one of the following radio buttons:

- Saved Query

  Click the **Browse** button to navigate to the query that you want to use. Choose the query and click **Open**.

  If you chose a single node generic query, the node to which RTMT is connected displays with a checkmark next to the Browse button. You can run the query on additional nodes by placing a checkmark next to those servers.

  If you chose an all node generic query, all nodes display with a checkmark next to the Browse button. You can uncheck any server for which you do not want to run the query.

  If you chose a regular query, all of the nodes that you selected when you saved the query display with a checkmark. You can check or uncheck any of the servers in the list. If you choose new servers, you must use the wizard to choose the services for that node.

  To run the query without any modifications, click **Run Query** and go to Step 17. To modify the query, go to Step 4.

- Create Query

Step 4 Click **Next**.

The Select CUP Services/Applications tab displays.

Step 5 If you clicked the Saved Query radio button and chose a query, the criteria that you specified for query display. If necessary, modify the list of services/applications for which you want to collect traces. If you clicked the Create Query radio button, you must choose all services/applications for which you want to collect traces.

Tip To collect traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box. To collect traces for all services and applications on a particular server, check the check box next to the IP address of the server.

Note The services that you have not activated also display, so you can collect traces for those services.

Note You can install some listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the server on which you have activated the service/application.

Step 6 Click **Next**.

Step 7 In the Select System Services/Applications tab, check all check boxes that apply.

Tip To collect traces for all system logs for all servers in the cluster, check the **Select All Logs on All Servers** check box. To collect traces for all services and applications on a particular server, check the check box next to the IP address of the server.

Step 8 Click **Next**.

Step 9 In the Query Time Options group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **All Available Traces**—Choose this option to collect all the traces on the server for the service(s) that you chose.
- **Absolute Range—**Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  The trace files that get modified in the date range (between the From date and the To date), get collected if the chosen time zone matches the time zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), but that server is in a different time zone, then the trace files that get modified in the corresponding date range in Server 2 will get collected from Server 2.

  To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.
- **Relative Range—**Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 10 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. The tool searches for an exact match to the word or phrase that you enter.

Step 11 From the Call Procession Impact Options drop-down list box, specify the level of impact you want the string search activity to have on call processing. Available options include Low, Medium, and High. Low impact causes the least impact on call processing but yields slower results. High impact causes the most impact on call processing but yields faster results.

Step 12 Choose one of the following options:

- To execute the query, click **Run Query**.

  The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **OK** and continue with Step 17.
- To save the query, click the **Save Query** button and continue with Step 13.

Step 13 Check the check box next to the type of query that you want to create.

- **Generic Query—**Choose this option if you want to create a query that you can run on nodes other than the one on which it was created. You can only create a generic query if the services that you chose exist on a single node. If you chose services on more than one node, a message displays. You can either save the query as a regular query or choose services on a single node.

  Then, choose either the Single Node Query or All Node Query option. If you choose the Single Node Query, the trace collection tool by default chooses the server on which you created the query when you execute the query. If you choose the All Node Query option, the trace collection tool by default chooses all of the servers in the cluster when you execute the query.

Note You can choose servers other than the default before running the query.

- **Regular Query**—Choose this option if you only want to run the query on that node or cluster on which you created the query.

Step 14 Click **Finish**.

Step 15 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 16 Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with Step 17.
- To exit the query wizard without running the query that you created, click **Cancel**.

Step 17 After the query execution completes, perform one or more of the following tasks:

- To view a file that you collected, navigate to the file by double-clicking Query Results, double-clicking the <node> folder, where <node> equals the IP address or host name for the server that you specified in the wizard, and double-clicking the folder that contains the file that you want to view. After you have located the file, double-click that file. The file displays in the viewer that is designated for that file type.
- Download the trace files and the result file that contains a list of the trace files that your query collected by choosing the files that you want to download, clicking **Download**, specifying the criteria for the download, and clicking **Finish**.
  - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download all files field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 10-14.

- To save the query, click **Save Query** and complete Step 13 through Step 15.

Additional Information

See the Related Topics, page 10-21.

Scheduling Trace Collection

You can use the Schedule Collection option of the trace and log central feature to schedule recurring up to 6 concurrent trace collections and to download the trace files to an SFTP server on your network, run another saved query, or generate a syslog file. To change a scheduled collection after you have entered it in the system, you must delete the scheduled collection and add a new collection event. To schedule trace collection, perform the following procedure.

Note You can schedule up 10 trace collection jobs, but only 6 trace collection can be concurrent. That is, only 6 jobs can be in a running state at the same time.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window. For more information, see the "Trace Configuration" section on page 5-1.
- If you want alarms to be sent to a trace file, choose an SDI trace file as the alarm destination in the Alarm Configuration window. For more information, see the "Alarm Configuration" section on page 3-1.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 In the tree hierarchy, double-click **Schedule Collection**.

The Select CUP Services/Applications tab displays.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Step 3 Perform one of the following tasks:

- To collect traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the trace collection wizard without collecting traces for services or applications, go to Step 4.

Note The services that you have not activated also display, so you can collect traces for those services.

Note You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the server on which you have activated the service/application.

Step 4 Click **Next**.

The System Services/Applications tab displays.

Step 5 To collect traces on system logs, perform one of the following tasks:

- To collect all system logs for all servers in the cluster, check the **Select All Logs on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the trace collection wizard without collecting traces for system logs, go to Step 6.

Step 6 Click **Next**.

Step 7 Specify the server time zone and the time range for which you want to collect traces.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Step 8 To specify the date and time that you want to start the trace collection, click the down arrow button next to the Schedule Start Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

Step 9 To specify the date and time that you want to end the trace collection, click the down arrow button next to the Schedule End Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

Note The trace collection completes, even if the collection goes beyond the configured end time; however, the trace and log central feature deletes this collection from the schedule.

Step 10 From the Scheduler Frequency drop-down list box, choose how often you want to run the configured trace collection.

Step 11 From the **Collect Files generated in the last** drop-down list boxes, specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 12 To search by phrases or words that exist in the trace file, enter the word or phrase in the **Search String** field. The tool searches for an exact match to the word or phrase that you enter and only collects those files that match the search criteria.

Step 13 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 14 To delete collected log files from the server, check the **Delete Collected Log Files from the Server** check box.

Step 15 Choose one or more of the following actions:

- Download Files
- Run Another Query
- Generate Syslog

Step 16 Do one of the following:

- If you chose Download Files or Run Another Query, continue with Step 17.
- If you chose Generate Syslog, go to Step 19.

Step 17 In the SFTP Server Parameters group box, enter the server credentials for the server where the trace and log central feature downloads the results and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP server, click **OK**.

> **Note** The **Download Directory Path** field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP parameters fields: /home/<user>/Trace.

Step 18 If you chose the Run Another Query Option, click the **Browse** button to locate the query that you want to run and click **OK**.

> **Note** The trace and log central feature only executes the specified query if the first query generates results.

Step 19 Click **Finish**.

A message indicates that the system added the scheduled trace successfully.

> **Note** If the real-time monitoring tool cannot access the SFTP server, a message displays. Verify that you entered the correct IP address, user name, and password

Step 20 Click **OK**.

Step 21 To view a list of scheduled collections, click the **Job Status** icon in the Quick Launch Channel.

> **Tip** To delete a scheduled collection, choose the collection event and click **Delete**. A confirmation message displays. Click **OK**.

Additional Information

See the Related Topics, page 10-21.

Viewing Trace Collection Status and Deleting Scheduled Collections

To view trace collection event status and to delete scheduled trace collections, use the following procedure:

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 In the Quick Launch Channel, click the **Job Status** icon.

Step 3 From the Select a Node drop-down list box, choose the server for which you want to view or delete trace collection events.

This list of scheduled trace collections displays.

Possible job types include Scheduled Job, OnDemand, RealTimeFileMon, and RealTimeFileSearch.

Possible statuses include Pending, Terminated, Running, Cancel, and Terminated.

Step 4 To delete a scheduled collection, choose the event that you want to delete and click **Delete**.

Note You can only delete jobs with a status of "Pending" or "Running" and a job type of "ScheduleTask."

Additional Information

See the Related Topics, page 10-21.

Collecting a Crash Dump

Perform the following procedure to collect a core dump of trace files:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 Double-click **Collect Crash Dump**.

Note The services that you have not activated also display, so you can collect traces for those services.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Note You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the server on which you have activated the service/application.

Step 3 In the Select CUP Services/Applications tab, perform one of the following tasks:

- To collect traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting traces for services or applications, go to Step 4.

Step 4 Click **Next**.

Step 5 In the Select System Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the Select All Services on all Servers check box.
- To collect traces for all system logs on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting traces for system logs, go to Step 6.

Step 6 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  The crash files that get modified in the date range (between the From date and the to date, get collected if the chosen time zone matches the zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), that is in a different time zone, then the crash files that get modified in the corresponding date range in Server 2 will get collected from Server 2.

  To set the date range for which you want to collect crash files, choose the drop-down list box in the From Date/Time and To Date/Time fields.
- **Relative Range**—Specify the amount of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

Step 7 From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

Cisco Unified Presence Serviceability stores logs for up to two Linux-based versions of Cisco Unified Presence. Cisco Unified Presence Serviceability stores the logs for the version of Cisco Unified Presence that you are logged in to in the active partition and stores the logs for the other version of Cisco Unified Presence (if installed) in the inactive directory.

So, when you upgrade from one version of Cisco Unified Presence that is running on the Linux platform to another and log in to the new version of Cisco Unified Presence that is running on the Linux platform, Cisco Unified Presence Serviceability moves the logs from the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version of Cisco Unified Presence, Cisco Unified Presence Serviceability moves the logs for the newer version of Cisco Unified Presence to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Presence Serviceability does not retain logs from Cisco Unified Presence versions that ran on the Windows platform.

Step 8 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.

Step 9 To create a zip file of the crash dump files that you collect, choose the **Zip File** radio button. To download the crash dump files without zipping the files, choose the **Do Not Zip Files** radio button.

Note You cannot download a zipped crash dump file that exceeds 2 gigabytes.

Step 10 To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

Step 11 Click **Finish**.

A message displays that states that you want to collect core dumps. To continue, click **Yes**.

Note If you chose the **Zip File** radio button and the crash dump files exceed 2 gigabytes, the system displays a message that indicates that you cannot collect the crash dump file of that size with the **Zip File** radio button selected. Choose the **Do Not Zip Files** radio button, and try the collection again.

Additional Information

See the Related Topics, page 10-21.

Using Local Browse

After you have collected trace files and downloaded them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within the real-time monitoring tool.

Note Do not use NotePad to view collected trace files.

Perform the following procedure to display the log files that you have collected with the trace and log central feature. If you zipped the trace files when you downloaded them to your PC, you will need to unzip them to view them by using the viewers within the real-time monitoring tool.

Before You Begin

Collect traces files as described in one of the following sections:

- "Collecting Traces" section on page 10-3
- "Using the Query Wizard" section on page 10-5
- "Scheduling Trace Collection" section on page 10-9

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 Double-click **Local Browse**.

Step 3 Browse to the directory where you stored the log file and choose the file that you want to view.

Step 4 To display the results, double-click the file.

Step 5 Click on the program (viewer) that you would like to use to view the file. If the program is not on the list, choose another program by clicking on the **Other** button.If you wish to use this program as your default viewer, click the **Always use this program to open these files** checkboxThe real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

Additional Information

See the Related Topics, page 10-21.

Using Remote Browse

After the system has generated trace files, you can view them on the server by using the viewers within the real-time monitoring tool. You can also use the remote browse feature to download the traces to your PC.

Perform the following procedure to display and/or download the log files on the server with the trace and log central feature.

Before You Begin

Collect traces files as described in one of the following sections:

- "Collecting Traces" section on page 10-3
- "Using the Query Wizard" section on page 10-5
- "Scheduling Trace Collection" section on page 10-9

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 Double-click **Remote Browse**.

Step 3 Choose the appropriate radio button, and click **Next**. If you choose Trace Files, go to Step 4. If you choose Crash Dump, go to Step 9.

Note The services that you have not activated also display, so you can choose traces for those services.

Note You can install some listed services/applications only on a particular node in the cluster. To choose traces for those services/applications, make sure that you choose traces from the server on which you have activated the service/application.

Step 4 In the Select CUP Services/Applications tab, perform one of the following tasks:

- To choose traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
- To choose traces for all services and applications on a particular server, check the check box next to the IP address of the server.
- To choose traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the remote browse wizard without choosing traces for services or applications, go to Step 5.

Note The services that you have not activated also display, so you can choose traces for those services.

Note You can install some listed services/applications only on a particular node in the cluster. To choose traces for those services/applications, make sure that you choose traces from the server on which you have activated the service/application.

Step 5 Click **Next**.

The System Services/Applications tab displays.

Step 6 Perform one of the following tasks:

- To choose all system logs for all servers in the cluster, check the **Select All Logs on all Servers** check box.
- To choose traces for all system logs on a particular server, check the check box next to the IP address of the server.
- To choose traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the remote browse wizard without collecting traces for system logs, go to Step 13.

Step 7 Click **Next**.

Step 8 Go to Step 13.

Step 9 In the CUP Applications/Services tab, perform one of the following tasks:

- To choose crash dump files for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
- To choose crash dump files for all services and applications on a particular server, check the check box next to the IP address of the server.
- To choose crash dump files for particular services or applications on particular servers, check the check boxes that apply.

Step 10 Click **Next**.

Step 11 In the Select System Services/Application tab, perform one of the following tasks:

- To choose crash dump files for all servers, check the **Select All Services on all Servers** check box.

- To choose crash dump files for all system logs on a particular server, check the check box next to the IP address of the server.
- To choose crash dump files for particular system logs on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting crash dump files, go to Step 12.

Step 12 Click **Next**.

Step 13 Click **Finish**.

Step 14 After the traces become available, a message displays. Click **Close**.

Step 15 Perform one of the following tasks:

- To display the results, navigate to the file through the tree hierarchy. After the log file name displays in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer.

Tip To sort the files that displays in the pane, click a column header; for example, to sort the files by name, click the Name column header.

The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

- To download the trace files, choose the files that you want to download, click **Download**, specify the criteria for the download, and click **Finish**.
  - To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download all files field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Files on server** check box.
- To delete trace files from the node, click the file that displays in the pane on the right side of the window; then, click the **Delete** button.
- To refresh a specific service or node, click the server name or service; then, click the **Refresh** button. After a message states that the remote browse is ready, click **Close**.
- To refresh all services and nodes that display in the tree hierarchy, click the **Refresh All** button. After a message states that the remote browse is ready, click **Close**.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 10-14.

Additional Information

See the Related Topics, page 10-21.

Using Q931 Translator

Note Cisco Unified Presence does not support the Q931 Translator.

Displaying QRT Report Information

Note Cisco Unified Presence does not support QRT report information.

Using Real Time Trace

The real-time trace option of the trace and log central feature in the RTMT allows you to view the current trace file that is being written on the server for each application. If the system has begun writing a trace file, the real time trace starts reading the file from the point where you began monitoring rather than at the beginning of the trace file. You cannot read the previous content.

The real-time trace provides the following options:

- View Real Time Data, page 10-18
- Monitor User Event, page 10-19

View Real Time Data

The view real time data option of the trace and log central feature allows you to view a trace file as the system writes data to that file. You can view real-time trace data in the generic log viewer for up to 10 services, 5 of which can exist on a single node. The log viewer refreshes every 5 seconds. As the traces get rolled into a new file, the generic log viewer appends the content in the viewer.

Note Depending on the frequency of the traces that a service writes, the View Real Time Data option may experience a delay before being able to display the data in the generic log viewer.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 Double-click **Real Time Trace**.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Step 3 Double-click **View Real Time Data**.

The Real Time Data wizard displays.

Step 4 From the **Nodes** drop-down list box, choose the node for which you want to view real-time data and click **Next**.

Step 5 Choose the service and the trace file type for which you want to view real-time data and click **Finish**.

Note The services that you have not activated also display, so you can collect traces for those services.

The real-time data for the chosen service displays in the generic log viewer.

Step 6 Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear. Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.

Step 7 Repeat this procedure to view data for additional services. You can view data for up to 10 services, 5 of which can exist on a single node. A message displays if you attempt to view data for too many services or too many services on a single node.

Step 8 When you are done viewing the real time data, click **Close** on the generic log viewer.

Additional Information

See the Related Topics, page 10-21.

Monitor User Event

The monitor user event option of the trace and log central feature monitors real-time trace files and performs a specified action when a search string appears in the trace file. The system polls the trace file every 5 seconds. If the search string occurs more than once in one polling interval, the system only performs the action once. For each event, you can monitor one service on one node.

Before you Begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the TraceCollectionToolEvent alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 8-2.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace & Log Central Options in RTMT" section on page 10-2.

Step 2 Double-click **Real Time Trace**.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace & Log Central windows.

Step 3 Double-click **Monitor User Event**.

The Monitor User Event wizard displays.

Step 4 Perform one of the following tasks:

- To view the monitoring events that you have already set up, choose the **View Configured Events** radio button, choose a server from the drop-down list box, and click **Finish**.

  The events configured for the server that you choose display.

Note To delete an event, choose the event and click **Delete**.

- To configure new monitoring events, choose the **Create Events** radio button, click **Next**, and continue with Step 5.

Step 5 Choose the node that you want the system to monitor from the **Nodes** drop-down list box and click **Next**.

Step 6 Choose the service and the trace file type that you want the system to monitor and click **Next**.

Note The services that you have not activated also display, so you can collect traces for those services.

Step 7 In the **Search String** field, specify the phrases or words that you want the system to locate in the trace files. The tool searches for an exact match to the word or phrase that you enter.

Step 8 Specify the server time zone and the time range (start and end date and time) for which you want the system to monitor trace files.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

The trace files that get modified in the date range (between the From date and the To date), get monitored if the chosen time zone matches the time zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), but that server is in a different time zone, then the trace files that get modified in the corresponding date range in Server 2 will get monitored from Server 2.

To set the date range for which you want to monitor traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.

Step 9 Choose one or more of the following actions that you want the system to perform when it encounters the search string that you specified in the Search String field:

- Alert—Choose this option to generate an alarm when the system encounters the specified search string. For the system to generate the alarm, you must enable the enable the TraceCollectionToolEvent alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 8-2.
- Local Syslog—Choose this option if you want the system to log the errors in the application logs area in the SysLog Viewer. The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from RTMT.
- Remote Syslog—Choose this option to enable the system to store the syslog messages on a syslog server. In the **Server Name** field, specify the syslog server name.
- Download File—Choose this option to download the trace files that contain the specified search string. In the SFTP Server Parameters group box, enter the server credentials for the server where you want to download the trace files and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP server, click **OK**.

Note The Download Directory Path field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP parameters fields: /home/<user>/Trace.

Note The system polls the trace files every 5 seconds and performs the specified actions when it encounters the search string. If more than one occurrence of the search string occurs in a polling interval, the system performs the action only once.

Step 10 Click **Finish**.

Additional Information

See the Related Topics, page 10-21.

Updating the Trace Configuration Setting for RTMT

To edit trace settings for the Real-Time Monitoring plug-in, choose **Edit** > **Trace Settings**; then, click the radio button that applies. The system stores the rtmt.log file in the logs directory where you installed the RTMT plug-in; for example, C:\Program Files\Cisco\Presence Serviceability\jrtmt\log.

Tip The Error radio button equals the default setting.

Additional Information

See the Related Topics, page 10-21.

Related Topics

- Using the Query Wizard, page 10-5
- Using Local Browse, page 10-14
- Collecting Traces, page 10-3
- Scheduling Trace Collection, page 10-9
- Displaying Trace & Log Central Options in RTMT, page 10-2
- Collecting a Crash Dump, page 10-12
- Using Local Browse, page 10-14
- Trace Configuration, page 5-1
- Alert Configuration in RTMT, page 8-1

CHAPTER 11

Using SysLog Viewer in RTMT

To display messages in SysLog Viewer, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- In the Quick Launch Channel, click the **Tools** tab; then, click **SysLog Viewer** and the **SysLog Viewer** icon.
- Choose **System > Tools > SysLog Viewer> Open SysLog Viewer**.

Step 2 From the Select a Node drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Click the tab for the logs that you want to view.

Step 4 After the log displays, double-click the log icon to list the file names in the same window.

Step 5 To view the contents of the file at the bottom of the window, click the file name.

Step 6 Click the entry that you want to view.

Step 7 To view the complete syslog message, double-click the syslog message. You can also use the following buttons that are described in Table 11-1 to view the syslog messages:

Tip To make a column larger or smaller, drag the arrow that displays when your mouse hovers between two column headings.

Tip You can order the messages by clicking on a column heading. The first time that you click on a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the records displays in the unsorted state.

Tip You can filter the results by choosing an option in the Filter By drop-down list box. To remove the filter, click Clear Filter. All logs display after you clear the filter.

Table 11-1 Syslog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the syslog viewer. **Tip** You can enable the syslog viewer to automatically update the syslog messages by checking the Auto Refresh button.
Clear	Clears the display of the current log.
Filter	Limits the messages that displayed base on the set of options that you select.
Clear Filter	Removes the filter that limits the type of messages that display.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC

Additional Information

See the Related Topics, page 11-2.

Related Topics

- Real-Time Monitoring Configuration, page 7-1

CHAPTER 12

Using Plug-ins

You can expand the functionality of RTMT by installing an application plug-in, such as the Voice Log Translator (VLT) application. You can download the latest plug-ins for the RTMT viewer from Cisco.com. After installing the plug-in, you can access the application in the RTMT viewer.

To download the plug-in, perform the following procedure:

Procedure

Step 1 Choose **Application** > **CCO Webpage**.

Step 2 The Login Prompt displays. Enter your Cisco.com user name and password and click OK.

Step 3 Download the file to your PC.

Step 4 To begin the installation, double-click the download file.

Step 5 Follow the installation instruction.

To access the plug-in, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- In the Quick Launch Channel, click the **Tools** tab and then the **Plugins** tab; click the icon of the application in which you are interested.
- Choose the plug-in that you want to launch under **System** > **Tools** > **Plugin.**

The application displays in the plugin window.

Refer to the application document for usage information.

Related Topics

For more information on Cisco Voice Log Translator, refer to the *Cisco Voice Log Translator User Guide*.

CHAPTER 13

Log Partition Monitoring Configuration

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition on a server (or all servers in the cluster):

- LogPartitionLowWaterMarkExceeded (% disk space)—When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
- LogPartitionHighWaterMarkExceeded (% disk space)—When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central.

Enabling Log Partition Monitoring

To enable Log Partition Monitoring, perform the following procedure:

Procedure

Step 1 In Cisco Unified Presence Serviceability, choose **Tools** > **Control Center** > **Network Services**.

Step 2 From the Servers drop-down list box, choose the server where you want to monitor the disk usage; then, click **Go**.

Step 3 Under Performance and Monitoring Services, verify the status of the Cisco Log Partition Monitoring Tool (LPM).

Step 4 If the LPM is not running, click the radio button next to Cisco LPM and click the **Start** button.

Configuring Log Partition Monitoring

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central. See the “Setting Alert Properties” section on page 8-2.

Additional Information

See the Related Topics, page 13-2.

Related Topics

- Log Partition Monitoring, *Cisco Unified CallManager Serviceability Administration Guide*
- Alert Configuration in RTMT, *Cisco Unified Real-time Monitoring Tool Guide for Cisco Unified CallManager*
- Trace Collection and Log Central in RTMT, page 10-1

PART 6

Reporting Tools Configuration

CHAPTER 14

Serviceability Reports Archive Configuration

The Serviceability Reports Archive window allows you to view reports generated by the Serviceability Reporter service. The Serviceability Reporter service generates reports at the time the you specify in the Serviceability Reporter service parameters in Cisco Unified Presence Administration.

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

Before you Begin

Activate the Cisco Serviceability Report service. Because the Serviceability Reporter service is CPU intensive, 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 group box, choose the month for which you want to display reports.

The month and year that you chose displays.

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

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.

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

Note To view PDF reports, you must install Acrobat ® Reader on your machine. To download Acrobat Reader, click the link in the bottom, right corner of the window.

Additional Information

See the Related Topics, page 14-6.

Related Topics

- Real-Time Monitoring Configuration, page 7-1
- Real-Time Monitoring Tool, *Cisco Unified CallManager Serviceability System Guide*
- Serviceability Reports Archive, *Cisco Unified CallManager Serviceability System Guide*

PART 7

SNMP Configuration

CHAPTER 15

SNMP V1/V2c Configuration

This chapter, which describes how to configure SNMP versions 1 and 2c so the network management system can monitor Cisco Unified CallManager, contains the following topics:

Tip If you use SNMP version 3, see the "SNMP V3 Configuration" section on page 16-1.

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 want 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 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 15-2.

Additional Information

See the "Related Topics" section on page 15-8.

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 CallManager system. Change the community string to limit access to the Cisco Unified CallManager 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 15-1.

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 15-1; 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 for the community string.
- To delete a community string, see the "Deleting a Community String" section on page 15-4.

Step 3 Enter the configuration settings, as described in Table 15-1.

Tip If you are adding a new community string, you can click the **Clear All** button at any time to delete all information that you entered for all settings.

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 "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 2-2.

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 "Related Topics" section on page 15-8.

Community String Configuration Settings

Table 15-1 describes the community string configuration settings. For related procedures, see the "Related Topics" section on page 15-8.

Table 15-1 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 15-1. To change the server for the community string, perform the procedure in the "Finding a Community String" section on page 15-1.
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 15-1 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. • **None**—The community string cannot read, write, or send trap information. **Tip** To change the Cisco Unified Presence trap configuration parameters, you need to use a community with NotifyOnly or ReadWriteNotify privileges.
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 15-1.

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 2-2.

After the window refreshes, the string that you deleted no longer displays in the results.

Additional Information

See the "Related Topics" section on page 15-8.

Finding a Notification Destination

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 want 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 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 V1/V2c" section on page 15-5.

Additional Information

See the "Related Topics" section on page 15-8.

Configuring a Notification Destination for 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" section on page 15-5.

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" section on page 15-5; 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" section on page 15-7.

Step 3 Enter the configuration settings, as described in Table 15-2.

> **Tip** If you are adding a new notification destination, you can click the **Clear** button at any time to delete all information that you entered for all settings.

Step 4 Click **Insert** to save a notification destination 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 "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 2-2.

Additional Information

See the "Related Topics" section on page 15-8.

Notification Destination Configuration Settings for V1/V2c

Table 15-2 describes the notification destination configuration settings for V1/V2c. For related procedures, see the "Related Topics" section on page 15-8.

Table 15-2 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" section on page 15-5. To change the server for the notification destination, perform the procedure in the "Finding a Community String" section on page 15-1.
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 15-2.
Notification Type	From the drop-down list box, choose the appropriate notification type.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box.

Deleting a Notification Destination

To delete a notification destination, perform the following procedure:

Procedure

Step 1 Locate the notification destination, as described in the "Finding a Notification Destination" section on page 15-5.

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 "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 2-2.

After the window refreshes, the notification destination that you deleted no longer displays in the results.

Additional Information

See the "Related Topics" section on page 15-8.

Related Topics

- Configuring a Community String, page 15-2
- Configuring a Notification Destination for V1/V2c, page 15-5
- SNMP V3 Configuration, page 16-1
- MIB2 System Group Configuration, page 17-1

CHAPTER 16

SNMP V3 Configuration

This chapter, which describes how to configure SNMP v3, so the network management system can monitor Cisco Unified CallManager, contains the following topics:

Tip If you use SNMP v1 or v2c, see the "SNMP V1/V2c Configuration" section on page 15-1.

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 want 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.

Tip The Apply to All Nodes check box does not apply to Cisco Unified Communications Manager Business Edition systems.

Step 6 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 16-2.

Additional Information

See the "Related Topics" section on page 16-8.

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" section on page 16-5.

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" section on page 16-5; 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 16-4.

Step 3 Enter the configuration settings, as described in Table 16-1.

Tip You can click the **Clear All** button at any time to delete all information that you entered for all settings.

Step 4 Click **Insert** to add a new user, 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 "Managing Services" section on page 2-1.

> **Note** To access this Cisco Unified CallManager 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 16-8.

SNMP User Configuration Settings

Table 16-1 describes the SNMP user configuration settings for V3. For related procedures, see the "Related Topics" section on page 16-8.

Table 16-1 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" section on page 16-5. To change the server where you want to provide access, perform the procedure in the "Finding the SNMP User" section on page 16-1.
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.

Table 16-1 SNMP User Configuration Settings for V3

Field	Description
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.
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 a trap and inform messages. • **None**—The user cannot read, write, or send trap information. To change the trap configuration parameters, you need to configure a user with NotifyOnly or ReadWriteNotify privileges.
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 16-1.

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 "Managing Services" section on page 2-1.

After the window refreshes, the user that you deleted no longer displays in the results.

Additional Information

See the "Related Topics" section on page 16-8.

Finding a Notification Destination

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 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 16-5.

Additional Information

See the "Related Topics" section on page 16-8.

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" 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 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 16-7.

Step 3 Configure the settings, as described in Table 16-2.

> **Tip** You can click the **Clear** button at any time to delete all information that you entered for the settings.

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 "Managing Services" section on page 2-1.

Additional Information

See the "Related Topics" section on page 16-8.

Notification Destination Configuration Settings for SNMP V3

Table 16-2 describes the notification destination configuration settings for V3. For related procedures, see the "Related Topics" section on page 16-8.

Table 16-2 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" section on page 16-5. To change the server for the notification destination, perform the procedure in the "Finding a Notification Destination" section on page 16-5.
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.

Table 16-2 Notification Destination Configuration Settings for V3

Field	Description
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.
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 16-2. • 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 16-2. • 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.
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" 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 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 "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 2-2.

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 16-8.

Related Topics

- SNMP V1/V2c Configuration, page 15-1
- Configuring the SNMP User, page 16-2
- MIB2 System Group Configuration, page 17-1
- Configuring a Notification Destination for SNMP V3, page 16-5

CHAPTER 17

MIB2 System Group Configuration

Cisco Unified Presence 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 17-1.

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 17-2.

MIB2 System Group Configuration Settings

Table 17-1 describes the MIB2 System Group configuration settings. For related procedures, see the "Related Topics" section on page 17-2.

Table 17-1 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.
Apply To All Nodes	To apply the system configuration to all of the nodes in the cluster, check the check box.

Related Topics

- SNMP V1/V2c Configuration, page 15-1
- SNMP V3 Configuration, page 16-1

INDEX

A

C

S

T

U

Z