Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor

Release 7.6(1)

May 2009

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

Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor

CONTENTS

Preface

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

Note This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL: http://www.cisco.com/go/ea

The preface covers these topics:

Purpose

The *Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor* provides information about the Real-Time Monitoring Tool (RTMT) for the Cisco Unified Expert Advisor.

All documents provide instructions for administering Cisco Unified Expert Advisor and include descriptions of procedural tasks that you complete by using Cisco Unified Expert Advisor operations console.

Audience

The *Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor* provides information for network administrators responsible for managing and supporting the Cisco Unified Expert Advisor operations console. 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, "Understanding Cisco Unified Expert Advisor Real-Time Monitoring Tool"	Provides a brief description of the Cisco Unified Expert Advisor Real-Time Monitoring Tool (RTMT).
Chapter 2, "Installing and Configuring Real-Time Monitoring Tool"	Provides procedures for installing, upgrading, and uninstalling RTMT. Also provides information on how to navigate within RTMT and how to configure profiles.
Chapter 3, "Monitoring Predefined Objects"	Provides an overview of the predefined objects that are monitored by RTMT.
Chapter 4, "Understanding Performance Monitoring"	Provides an overview of performance counters.
Chapter 5, "Configuring and Displaying Performance Counters"	Provides procedures for working with performance monitors, including viewing performance counters and counter descriptions.
Chapter 6, "Alerts"	Provides an overview of alerts, including a description of preconfigured alerts. Describes fields that you use to configure alerts and alert actions.
Chapter 7, "Working with Alerts"	Provides procedures for working with Alerts.
Chapter 8, "Configuring Trace & Log Central in RTMT"	Provides information on configuring on-demand trace collection and crash dump files for system services as well as on viewing the trace files in the appropriate viewer.
Chapter 9, "Using SysLog Viewer in RTMT"	Provides information on using the SysLog Viewer.
Appendix A, "Performance Objects and Counters for the System"	Provides a list of performance objects and their associated counters for the system
Appendix B, "Performance Objects and Counters for the Cisco Unified Expert Advisor"	Provides a list of performance objects and their associated counters for the Cisco Unified Expert Advisor.

Related Documentation

For additional Cisco Unified Expert Advisor documentation, refer to the following URL:
http://www.cisco.com/en/US/products/ps9675/tsd_products_support_series_home.html

Conventions

This document uses the following conventions:

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

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address:
ccbu_docfeedback@cisco.com.

CHAPTER 1

Understanding Cisco Unified Expert Advisor Real-Time Monitoring Tool

The Real-Time Monitoring Tool (RTMT) for Cisco Unified Expert Advisor, which runs as a client-side application, uses HTTPS and TCP to monitor system performance and device status for Cisco Unified Expert Advisor. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

Note Even when RTMT is not running as an application on your desktop, tasks such as alarm and performance monitoring updates continue to take place on the server in the background.

Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter)

RTMT Collector, a component that automatically gets installed with the application, logs preconfigured monitoring objects information while Alert Manager, also automatically installed, logs alert histories into log files. Each preconfigured object belongs to one of several categories: devices, services, and servers. Each category has a separate log file, and alert details get logged in a separate file.

The system also records important perfmon object values in performance log files.

Tip Although they require no configuration tasks to run, RTMT Collector and Alert Manager support redundancy. If the primary collector or manager fails for any reason, the secondary collector and manager perform the tasks until primary support becomes available. RTMT Collector, Alert Manager, and RTMT Reporter run on the first node (primary runtime server).

Note The term node and server are used interchangeably in this document and refers to a computer that provides services or resources to other computers (called clients) connected to it through a network.

The locally written log files appear in the primary collector server at /common/log/taos-log-a/cm/log/amc. Because the primary collector changes because of failover and fallback scenarios, the log files can exist on more than one server in the Cisco Unified Expert Advisor cluster.

You can display log files, except an alert log file, by using the Performance log viewer in RTMT or by using the native Microsoft Performance viewer. For more information on using the Performance log viewer in RTMT, refer to "Viewing Perfmon Log Files" section on page 5-10. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace & Log Central in RTMT. For more information on downloading log files by using the collect files option, refer to "Collecting Trace Files" section on page 8-3.

Alternatively, from the Command Line Interface (CLI), you can use the file list command to display a list of files and the file get command to download files by SFTP. For more information on using CLI commands, refer to the *Administration and Configuration Guide for Cisco Unified Expert Advisor*.

Log files exist in csv format. New log files get created every day at 00:00 hours on the local system (based on the log file size). New logs for devices, services, servers, and calls get created when the time zone changes, when a new node is added to the cluster, or during failover/fallback scenarios. The first column of all these logs comprises the time zone information and the number of minutes from the Greenwich Meridian Time (GMT). RTMT Reporter uses these log files as a data source to generate daily summary reports. The report, which is based on the default monitoring objects, generates every 24 hours for the following information:

- Server Status—% CPU load,% memory used,% disk space used per server.
- Alert Status—Number of alert per severity level for the cluster, including the top 10 alerts in the cluster.

Tip The RTMT reports only display in English.

Caution The service parameters that apply to RTMT report generation (for serviceability reports) are preconfigured and cannot be changed using the Cisco Unified Expert Advisor.

For more information on the Serviceability reports, see the "Serviceability Reports" chapter in *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.

Additional Information

See the "Related Topics" section on page 1-3.

Understanding Server Logs

Every 5 minutes, the server data gets logged into the file as a single record. The system logs the data every 5 minutes for the following counters, based on the following calculation:

- cpuUsage—Average of all the values that were collected in the last 5 minutes
- MemoryInUse—Average of all the values that were collected in the last 5 minutes
- DiskSpaceInUse—Average of all the values that were collected in the last 5 minutes for the active partition

The Cisco AMC service logs the server data in csv format. The header of the log comprises the time zone information and a set of columns with the previous counters for a Cisco Unified Expert Advisor node. These sets of columns repeat for every node.

The following file name format of the server log applies: ServerLog_MM_DD_YYYY_hh_mm.csv. The first line of each log file comprises the header.

To download the server logs for viewing on your local computer, refer to Configuring Trace & Log Central in RTMT, page 8-1.

Additional Information

See the "Related Topics" section on page 1-3.

Related Topics

- Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter), page 1-1
- Understanding Server Logs, page 1-2

CHAPTER 2

Installing and Configuring Real-Time Monitoring Tool

You can install the Real-Time Monitoring Tool (RTMT) on a computer that is compatible with the Cisco Unified Expert Advisor software.

Tip See the *Hardware and System Software Specification (Bill of Materials)* at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

This chapter contains information on the following topics:

Installing RTMT

To install the tool, perform the following procedure:

Note While installing RTMT on a Windows Vista machine, you will see a User Account Control pop-up message that says, “An unidentified program wants to access your computer.” Click **Allow** to continue working with RTMT.

Tip See the *Hardware and System Software Specification (Bill of Materials)* at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Procedure

Step 1 From Cisco Unified Expert Advisor operations console, choose **Tools > RTMT Plugin Download**.

Step 2 To install the RTMT tool on a client that is running the Microsoft Windows operating system, select the **Windows** radio button.

To install the RTMT tool on a client that is running the Linux operating system, select the **Linux** radio button.

Step 3 Click on the **Download** link.

Step 4 Download the executable to the preferred location on your client.

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.

Step 6 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 7 After the RTMT welcome window displays, click **Next**.

Step 8 To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.

Tip Only the first node in the cluster displays the number of licenses. The other nodes in the cluster do not display any licensing information. During a failover, the primary (publisher) node continues to retain the license information.

Step 9 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 10 To begin the installation, click **Next**.

The Setup Status window displays. Do not click Cancel.

Step 11 To complete the installation, click **Finish**.

Additional Information

See the "Related Topics" section on page 2-10.

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 user-created profiles in the 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 Expert Advisor operations console upgrade on all servers in the cluster.

Before you upgrade to a newer version of RTMT, Cisco recommends that you uninstall the previous version of RTMT. See "Uninstalling RTMT" section on page 2-4.

To upgrade to a newer version of RTMT, perform the following procedure:

Procedure

Step 1 From Cisco Unified Expert Advisor operations console, choose **Tools > RTMT Plugin Download**.

Step 2 To install the RTMT tool on a client that is running the Microsoft Windows operating system, select the **Windows** radio button.

To install the RTMT tool on a client that is running the Linux operating system, select the **Linux** radio button.

Step 3 Click on the **Download** link.

Step 4 Download the executable to your preferred location.

Step 5 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.

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" section on page 2-10.

Installing Multiple Copies of RTMT

A single version of RTMT can only monitor one cluster for one product (based on compatibility with the product).

To monitor a product on a server or node in a different cluster, you must first log off the server or node before you can log on to the other server.

Multiple copies of RTMT that are installed on your computer (for different Cisco Unified Expert Advisor clusters) allow you to simultaneously monitor multiple Cisco Unified Expert Advisor products that are installed on different servers.

Tip To monitor another Cisco Unified Communication product (other than Cisco Unified Expert Advisor), ensure to empty the RTMT cache before launching RTMT for the new product. The RTMT cache generally exists in your %TEMP%/.jrtmt directory for a Window's client, and in your $HOME/.jrtmt directory for a Linux client. You must delete all the files in this .jrtmt directory after exiting one product's RTMT and before logging on to another product's RTMT.

When you install multiple copies of RTMT on a single computer, you must install RTMT in different folders.

Tip Cisco recommends installing no more than four copies of RTMT on a computer.

After installing another copy of RTMT, complete the following tasks:

1. The shortcut icon gets overwritten and points to only the latest RTMT installation. Create another icon by creating a shortcut to jrtmt.exe in the folder with the previous installation.
2. Rename the icon accordingly.

If the installation detects another version in the selected folder, a message displays. To continue the installation, install the version in a different folder.

Note Your computer stores the user preferences, such as the IP address and RTMT frame size, from the RTMT client that last exits.

Uninstalling RTMT

Tip When you use RTMT, it saves user preferences and the module jar files (the cache) locally on the client machine. 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. (Choose **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.

Note While uninstalling RTMT on a Windows Vista machine, you will a see a User Account Control pop-up message that says, "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Tip See the *Hardware and System Software Specification (Bill of Materials)* at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Additional Information

See the "Related Topics" section on page 2-10.

Launching RTMT

Note While using RTMT on a Windows Vista machine, you will a see a User Account Control pop-up message that says, "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Tip See the *Hardware and System Software Specification (Bill of Materials)* at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Procedure

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

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

Step 3 In the User Name field, enter the Administrator username for the application.

Step 4 In the Password field, enter the Administrator 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 server, when the local cache does not contain a monitoring module that matches the backend 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 When prompted, add the certificate store by clicking **Yes**.

Cisco Unified Expert Advisor Real-Time Monitoring Tool starts.

Launching RTMT on Linux

Tip To install a RTMT plugin on a Linux machine, you must have root privileges. Before launching the RTMT installer, use the **chmod +x** command to execute permissions on the installer.

Procedure

Step 1 Navigate to the directory in which you have installed RTMT.

Step 2 Launch RTMT on your Linux machine by running the JRtmt file.

```
run: ./JRtmt
```

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, work with alerts, collect traces, view syslog messages, and go to the Cisco Unified Reporting application.
  - Cisco Unified Expert Advisor—Allows you to view Cisco Unified Expert Advisor summary information on the server, view performance information, and monitor services.
  - 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 Cisco Unified Expert Advisor operations console and Cisco Unified Serviceabilty for Cisco Unified Expert Advisor. Allows you to browse the web pages for Cisco Unified Expert Advisor and its related applications.
  - 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 to display information on the server or information on the applications. The tab contains groups of icons on which you can click the monitor various objects.
- Monitor pane—Pane where monitoring results display.

Additional Information

See the "Related Topics" section on page 2-10.

Working with Configuration Profiles

You can use RTMT to connect to a server. After you log in, RTMT launches the monitoring module from the local cache or from a remote server when the local cache does not contain a monitoring module that matches the backend version.

RTMT includes a default configuration that is called Default. The first time that you use RTMT, it uses the Default profile and displays the system summary page in the monitor pane.

You can configure RTMT to display the information that interests you, such as different performance counters for different features, in the monitor pane of RTMT and save the framework of your configuration in a profile. You can then restore the profile at a later time during the same session or the next time that you log in to RTMT. By creating multiple profiles, so each profile displays unique information, you can quickly display different information by switching 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 Default. The first time that you use RTMT, it will use the Default profile and display the system summary page in the monitor pane.

Adding Configuration Profiles

With RTMT, you can customize your monitoring window by monitoring different performance counters, then 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.

Note Profiles apply to all nodes within a cluster, but the profile cannot be saved and applied to a different cluster.

The system creates the new configuration profile.

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.

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" section on page 2-10.

Working with Categories

Categories allow you to organize objects in RTMT, such as performance monitoring counters and devices. For example, the default category under performance monitoring, RTMT allows you to monitor six performance monitoring counters in graph format. 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 Performance Monitoring under the system tab in the Search window.

Step 2 Choose **Edit > Add 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" section on page 2-10.

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" section on page 2-10.

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" section on page 2-10.

Related Topics

- Installing RTMT, page 2-1
- Upgrading RTMT, page 2-2
- Uninstalling RTMT, page 2-4
- Launching RTMT, page 2-5
- Navigating RTMT, page 2-6
- Working with Configuration Profiles, page 2-7
- Working with Categories, page 2-9

CHAPTER 3

Monitoring Predefined Objects

RTMT provides a set of default monitoring objects that assist you in monitoring the health of the system. Default objects include performance counters or critical event status for the system and other supported services.

This chapter contains information on the following topics:

Viewing the System Summary

The system summary in RTMT allows you to monitor important common information in a single monitoring pane. In system summary, you can view information on the following predefined object:

- Virtual memory usage
- CPU usage
- Common partition usage
- Alert history log

Additional Information

See the "Related Topics" section on page 3-4.

Monitoring Server Status

The Servers category monitors CPU and memory usage, processes, disk space usage, and critical services for the different applications on the server.

The CPU and Memory monitor provide information about the CPU usage and virtual memory usage on each server. For each CPU on a server, the information includes the percentage of time that each processor spends executing processes in different modes and operations (User, Nice, System, Idle, IRQ, SoftIRQ, and IOWait). The percentage of CPU equals the total time that is spent executing in all the different modes and operations excluding the Idle time. For memory, the information includes the Total, Used, Free, Shared, Buffers, Cached, Total Swap, Used Swap, and Free Swap memory in Kbytes, and the percentage of Virtual Memory in Use.

The Processes monitor provides information about the processes that are running on the system. RTMT displays the following information for each process—process ID (PID), CPU percentage, Status, Shared Memory (KB), Nice (level), VmRSS (KB), VmSize (KB), VmData (KB), Thread Count, Page Fault Count, and Data Stack Size (KB).

The disk usage monitoring category charts the percentage of disk usage for the common and swap partitions. It also displays the percentage of disk usage for each partition (Active, Boot, Common, Inactive, Swap, SharedMemory) in each host.

The Critical Services monitoring category provides the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services are up and running on the system.

The **Systems** tab lists all critical services related to the system and the **Expert Advisor** tab defines all critical services related to the Cisco Unified Expert Advisor. These critical services are activated when VOS starts.

For a specific description of each states, see Table 3-1.

Table 3-1 Status of Critical Services

Status of Critical Service	Description
starting	The service currently exists in start mode, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability operations console.
up	The service currently runs, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability operations console.
stopping	The service currently remains stopped, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability operations console.
down	The service stopped running unexpectedly; that is, you did not perform a task that stopped the service. The Critical Services pane indicates that the service is down. The CriticalServiceDown alert gets generated when the service status equals down.
stopped by Admin	You performed a task that intentionally stopped the service; for example, the service stopped because you backed up or restored Cisco Unified Expert Advisor performed an upgrade, stopped the service in Cisco Unified Serviceability operations console or the CLI, and so on. The Critical Services pane indicates the status.
not activated	The service does not exist in a currently activated status, as indicated in the Critical Services pane and in Service Activation in Cisco Unified Serviceability operations console.
unknown state	The system cannot determine the state of the service, as indicated in the Critical Services pane.

Additional Information

See the "Related Topics" section on page 3-4.

Viewing/Monitoring Predefined System Objects

RTMT displays information on predefined system objects in the monitoring pane when you select System in the quick launch channel.

Table 3-2 provides information on the predefined object that RTMT monitors.

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.

Table 3-2 System Categories

Category	Description
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 the 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 the 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 the 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 the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for a particular Cisco Unified Communications node. To display information on critical services, choose **System > Server > Critical Services.** To display system critical services, click on the system tab. – To display Cisco Unified Expert Advisor critical services, click the Expert Advisor tab. – To monitor critical services for specific server, choose the server from the host drop-down list box and click the critical services tab in which you are interested. If the critical service status indicates that the administrator stopped the service, the administrator performed a task that intentionally stopped the service; for example, the service stopped because the administrator backed up or restored Cisco Unified Expert Advisor, performed an upgrade, stopped the service in Cisco Unified Serviceability operations console or the CLI, and so on. If the critical service status displays as unknown state, the system cannot determine the state of the service. For more information on the critical service states, refer to Monitoring Server Status, page 3-1.

Related Topics

- Viewing the System Summary, page 3-1
- Monitoring Server Status, page 3-1
- Viewing/Monitoring Predefined System Objects, page 3-3

CHAPTER 4

Understanding Performance Monitoring

Cisco Unified Expert Advisor directly updates Performance Monitoring counters (called Perfmon counters). The counters contain simple, useful information on the system and devices on the system, such as the number of Cisco Unified Expert Advisor Perfmon counters.

Single object contains most of the Cisco Unified Expert Advisor performance counters, and these counters have only one instance. The instance-based counters that belong to the other objects can have zero or more instances.

You can monitor the performance of the components of the system and the components for the application on the system 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 Realtime Information Server Data Collection (RISDC) Perfmon logs.

This chapter contains information on the following topics:

Using RTMT for Perfmon

.RTMT integrates with the administration and serviceability software for Cisco Unified Expert Advisor. RTMT displays performance information for all Cisco Unified Expert Advisor components. RTMT provides alert notification for troubleshooting performance. It also periodically polls performance counter to display data for that counter. Refer to "Displaying a Counter Description" section on page 5-7 for examples on displaying Perfmon counters in a chart or table format.

Perfmon allows you to perform the following tasks:

- Monitor performance counters including all the Cisco Unified Expert Advisor nodes in a cluster.
- Monitor Cisco Unified Expert Advisor servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an e-mail message.
- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.
- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.

- Display up to six Perfmon counters in one chart for performance comparisons.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. Up to six charts display in the RTMT Perfmon pane for each category tab that you create. You can display a particular counter by double clicking the counter in the Perfmon pane. Because chart view represents the default, you configure the performance counters to display in table format when you create a category.

See the following sections for configuration options in the RTMT Perfmon pane:

- Category Tabs, page 4-2
- Sample Rate, page 4-2
- Using RTMT for Perfmon, page 4-1
- Displaying a Counter Description, page 5-7

Category Tabs

A category comprises a group of monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

You can create custom categories in the RTMT monitoring pane to view information that helps you troubleshoot specific performance, system, or device problems. If your system is experiencing performance problems with specific objects, create custom categories to monitor the performance of the counters within the object. If the system is experiencing problems with specific devices, create custom categories to monitor the devices in your system. In addition, you can create alert notifications for counters and gateways in these custom categories. To create custom categories, you add a new category tab. When the tab is created, you specify the specific performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

Sample Rate

Note The application polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance counters, devices, and gateway ports for each category tab that you create. High-frequency polling rate affects the performance on the server. 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 3 seconds. The default for both specifies 10 seconds.

Adding Counters to Monitor

To troubleshoot system performance problems, you add the counter that is associated with the Perfmon object to the RTMT Perfmon pane, which displays a chart for the counter. Before you add counters, see the "Category Tabs" section on page 4-2.

Category tabs contain up to six Perfmon counter charts.

Alert Notification for Counters

Using the alert notification feature, the application notifies you of system problems. Perform the following configuration setup to activate alert notifications for a system counter:

- From the RTMT Perfmon pane, choose the system Perfmon counter.
- Set up an e-mail or a message popup window for alert notification.
- Determine the threshold for the alert (for example, an alert activates when the number of active calls exceed the threshold of over 100 calls or under 50 calls).
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

Zoom Counter

To get a closer look at a Perfmon chart, zoom the monitor counter in the RTMT Perfmon monitoring pane by highlighting the counter chart and choosing **System > Performance > Zoom Chart**.

Counter Properties

Counter properties allow you to display a description of the counter and configure data-sampling parameters.

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the RTMT performance 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 to view all the data that a Perfmon counter collected.

Additional Information

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

Troubleshooting Perfmon Data Logging

The troubleshooting Perfmon data logging feature assists Cisco TAC in identifying system problems. When you enable troubleshooting perfmon data logging, you initiate the collection of a set of Cisco Unified Expert Advisor and operating system performance statistics on the selected node. When you enable troubleshooting Perfmon data logging, you initiate the collection of a set of Cisco Unified Expert Advisor, and operating system performance statistics on the selected server. The statistics that are collected include comprehensive information that can be used for system diagnosis.

The system automatically enables troubleshooting Perfmon data logging to collect statistics from a set of Perfmon counters that provides comprehensive information on the system state. When Troubleshooting Perfmon Data Logging is enabled, Cisco estimates that the system experiences a less than 5-percent increase in CPU utilization and an insignificant increase in the amount of memory that is being used, and it writes approximately 50 MB of information to the log files daily.

You can perform the following administrative tasks with the troubleshooting Perfmon data logging feature:

- Enable and disable the trace filter for Troubleshooting Perfmon data logging.
- Monitor a set of predefined System and Cisco Unified Expert Advisor performance objects and counters on each server.
- Monitor a set of predefined System/Cisco Unified Expert Advisor objects and counters on each server.
- Log the monitored performance data in CSV file format on the server in the active log partition in the var/log/active/cm/log/ris/csv directory. The log file uses the following naming convention: PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv. Specify the polling rate. This rate specifies the rate at which performance data gets gathered and logged. You can configure the polling rate down to 5 seconds. Default polling rate equals 15 seconds.
- View the log file in graphical format by using the Microsoft Windows performance tool or by using the Performance Log viewer in RTMT.
- Displays the maximum number of log files that will be stored on disk. Serviceability log files exceeding this limit get purged automatically by removal of the oldest log file. The default specifies 50 files (cannot be changed).
- Displays the rollover criteria of the serviceability log file based on the maximum size of the file in megabytes. The default value specifies 2 MB.
- Collect the Cisco RISDC PerfMonLog log file by using the Trace & Log Central feature of the Real-Time Monitoring Tool or CLI.

For more information on the following objects and classes, see the related sections:

- Cisco Unified Expert Advisor serviceability solutions for single objects. See Table B-1.
  - General Information Section
  - License Information Section
  - Expert Advisor JVM Statistics
  - Thread Pool Section
- Cisco Unified Expert Advisor serviceability solutions for instance-based objects: See Table B-1.
  - System Condition Table
  - Services Table
  - BRE Table
  - Contact Manager Table
  - ICMGW Table
  - MPA Table
  - Reporting Adapter Table
  - RDA Table
  - Resource Manager Table
  - Reporting Subsystem Table
  - Work Assigner Table
- IP Object. See Table A-8.

- Memory Object. See Table A-9
- Network Interface Object. See Table A-10.
- Replication Counters. See Table A-11.
- Partition Object. See Table A-12.
- Process Object See Table A-13.
- Processor Object. See Table A-14.
- System Object. See Table A-15.
- TCP Object. See Table A-16.
- Thread Object. See Table A-17.

Related Topics

- Using RTMT for Perfmon, page 4-1
- Troubleshooting Perfmon Data Logging, page 5-13
- Appendix A, “Performance Objects and Counters for the System”
- Appendix B, “Performance Objects and Counters for the Cisco Unified Expert Advisor”

CHAPTER 5

Configuring and Displaying Performance Counters

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 in which you are interested. 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.

Step 3 To monitor a counter in table format, continue to Step 4. To monitor a counter in chart format, skip to Step 9.

Step 4 Choose **Edit > New Category**.

Step 5 In the Enter Name field, enter a name for the tab.

Step 6 To display the perfmon counters in table format, check the **Present Data in Table View** check box.

Step 7 Click **OK**.

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

Step 8 Perform one of the following tasks to select one or more counters with one or more instances for monitoring in table format (skip the remaining step in this procedure):

- Double click a single counter and select a single instance from the pop-up window; then, click **Add**.
- Double click a single counter and select multiple instances from the pop-up window; then, click **Add**.
- Drag a single counter to the monitoring window and select a single instance from the pop-up window; then click **Add**.
- Drag a single counter to the monitoring window and select multiple instances from the pop-up window; then, click **Add**.
- Select multiple counters and drag them onto the monitoring window. Select a single instance from the pop-up window; then, click **Add**.
- Select multiple counters and drag them onto the monitoring window. Select multiple instances from the pop-up window; then, click **Add**.

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 9 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, page 5-14.

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, page 5-14.

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 "Using RTMT for Perfmon" section on page 4-1.

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, page 5-14.

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 "Using RTMT for Perfmon" section on page 4-1.

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 5-1 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 5-1 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. • 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. **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—Choose Absolute to display the data at its current status. These counter values are cumulative. • 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	

Table 5-1 Counter Alert Configuration Parameters (continued)

Setting	Description
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.
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. For example, if the active calls 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 active calls), 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, page 5-14.

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, page 5-14.

Displaying a Counter Description

All system conditions for the Cisco Unified Expert Advisor system are visible as individual RTMT alerts. These alerts appear in the Alert Central tool in RTMT under the Expert Advisor Tab. Each alert description explains the system condition and possible resolution actions.

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** from the menu bar.

Tip To display the counter description and to configure data-sampling parameters, see the "Configuring a Data Sample" section on page 5-8.

Note To view the description of the service, click on the Service Type in the Service Table perfmon counter and right-click to select the corresponding description.

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, page 5-14.

See Appendix C, "System Condition Descriptions for the Cisco Unified Expert Advisor"

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 5-9.

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 "Using RTMT for Perfmon" section on page 4-1.

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 5-2.

Table 5-2 Data Sample Parameters

Parameter	Description
Absolute	Because some counter values are accumulative, 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 the Related Topics, page 5-14.

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 5-8 procedure for configuring data samples.

Additional Information

See the Related Topics, page 5-14.

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 "Viewing Log Files on the Performance Log Viewer" section on page 5-10.

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 "Using RTMT for Perfmon" section on page 4-1.

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 click **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, configure the maximum file size and maximum number of files parameter in the trace output setting for the specific service in the Trace Configuration window of Cisco Unified Serviceability. See the *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.

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 "Using RTMT for Perfmon" section on page 4-1.

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**.

Additional Information

See the Related Topics, page 5-14.

Viewing Perfmon Log Files

You can view data from the perfmon CSV log by using the Performance Log Viewer in RTMT or by using the Microsoft Performance tool.

Viewing Log Files on the Performance 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 RISDC perfmon logs.

The local perfmon logs comprise 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 5-9.

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 RISDC Perfmon Logs, perform the following steps:
  a. Click on RISDC 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.

Caution If you have changed this default path during installation, be sure to use the path you specified.

  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 5-3 describes the functions of different buttons that are available on the performance log viewer.

Table 5-3 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.

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.

Additional Information

See the Related Topics, page 5-14.

Viewing All Log Files

You can use the Remote Browse feature to view all the local perfmon logs that you collected.

The local perfmon logs comprise 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 5-9.

Procedure

Step 1 Click on Trace & Log Central.

Step 2 Double-click on Remote Browse.

Step 3 Select the **Trace Files** radio button.

Step 4 Select the logs specific to Cisco Unified Expert Advisor from the displayed table of logs. Alternately, click Next to select the logs of all other services in the subsequent table.

Step 5 Click Finish.

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 selected desired area.

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

Additional Information

See the Related Topics, page 5-14.

Viewing the Perfmon Log Files with the Microsoft Performance Tool

To view the log files by using the Microsoft Performance tool, follow these steps:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Performance.**

Step 2 In the application window, click the right mouse button and choose **Properties**.

Step 3 Click the Source tab in the System Monitor Properties dialog box.

Step 4 Browse to the directory where you downloaded the perfmon log file and choose the perfmon csv file. The log file includes the following naming convention: PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv.

Step 5 Click **Apply.**

Step 6 Click the **Time Range** button. To specify the time range in the perfmon log file that you want to view, drag the bar to the appropriate starting and ending times.

Step 7 To open the Add Counters dialog box, click the Data tab and click **Add**.

Step 8 From the Performance Object drop-down box, choose the perfmon object. If an object has multiple instances, you may choose **All instances** or select only the instances that you are interested in viewing.

Step 9 You can choose **All Counters** or select only the counters that you are interested in viewing.

Step 10 To add the selected counters, click **Add**.

Step 11 When you finish selecting counters, click **Close**.

Additional Information

See the Related Topics, page 5-14.

Troubleshooting Perfmon Data Logging

Cisco Unified Expert Advisor collects system performance information that is written on the Cisco Unified Expert Advisor server. You can use this performance data to troubleshoot problems. By default, RISDC perfmon logging gets enabled. Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging.

You can collect the log files for Cisco RISDC service on the server by using RTMT to download the log files. If you want to download the log files by using the CLI, refer to *Cisco Unified Expert Advisor Option OAMP Configuration Guide*. After you collect the log files, you can view the log file by using the Performance Log Viewer in RTMT or by using the Microsoft Windows performance tool. See "Viewing Log Files on the Performance Log Viewer" section on page 5-10 or "Viewing the Perfmon Log Files with the Microsoft Performance Tool" section on page 5-12.

Tip In Cisco Unified Expert Advisor, the Troubleshooting Perfmon Data logging parameters cannot be changed. The default values are as follows:
- Maximum file size = 2MB
- Maximum number of files = 50

Related Topics

- Displaying Performance Counters, page 5-1
- Removing a Counter from the RTMT Performance Monitoring Pane, page 5-3
- Adding a Counter Instance, page 5-3
- Configuring Alert Notification for a Counter, page 5-4
- Zooming a Counter, page 5-6
- Displaying a Counter Description, page 5-7
- Configuring a Data Sample, page 5-8
- Viewing Counter Data, page 5-9
- Local Logging of Data from Perfmon Counters, page 5-9
- Viewing Log Files on the Performance Log Viewer, page 5-10
- Understanding Performance Monitoring, page 4-1
- Performance Objects and Counters for the System, page A-1
- Performance Objects and Counters for the Cisco Unified Expert Advisor, page B-1

CHAPTER 6

Alerts

This chapter contains information on the following topics:

Understanding Alerts

The system generate alert messages to notify administrator when a predefined condition is met, such as when an activated service goes from up to down. Alerts can be sent out as e-mail/epage.

RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts). The Alert menu comprises the following menu options:

- Alert Central—This option comprises the history and current status of every alert in the system.

Note You can also access Alert Central by clicking the Alert Central icon in the hierarchy tree in the system drawer.

- Set Alert/Properties—This menu option allows you to set alerts and alert properties.
- Remove Alert—This menu category allows you to remove an alert.
- Enable Alert—With this menu category, you can enable alerts.
- Disable Alert—You can disable an alert with this category.
- Suspend cluster/node Alerts—This menu category allows you to temporarily suspend alerts on a particular Cisco Unified Expert Advisor operations console node or on the entire cluster.
- Clear Alerts—This menu category allows you to reset an alert (change the color of an alert item from to black) to signal that an alert has been taken care of. After an alert has been raised, its color will automatically change to in RTMT and will stay that way until you manually clear the alert.
- Clear All Alerts—This menu category allows you to clear all alerts.
- Alert Detail—This menu category provides detailed information on alert events.

- Config Email Server—In this category, you can configure your e-mail server to enable alerts.
- Config Alert Action—This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired e-mail recipients.

In RTMT, you configure alert notification for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on.

You can locate Alert Central under the Tools hierarchy tree in the quick launch. Alert Central provides both the current status and the history of all the alerts in the system.

Additional Information

See the Related Topics, page 6-7.

Viewing Alerts

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under different tabs—System, Cisco Unified Expert Advisor, and Custom.

You can enable or disable preconfigured and custom alerts in Alert Central; however, you cannot delete preconfigured alerts.

The following list comprises the preconfigured alerts for the system:

- AuthenticationFailed
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown

Note The CriticalServiceDown alert only gets generated when the service status equals down (not for other states).

- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown

Note The ServerDown alert gets generated when the currently “active” AMC (primary AMC or the backup AMC, when the primary is not available) cannot reach another node in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

- SyslogSeverityMatchFound

- SyslogStringMatchFound
- SystemVersionMismatched
- ThreadCounterUpdateStopped

Table 6-1 displays the preconfigured alerts for Cisco Unified Expert Advisor (in addition to the current VOS CPU, memory, disk, and other alerts).

Table 6-1 Preconfigured Alerts for Cisco Unified Expert Advisor

Alert Name	Counter	Description	Raise	Clear
[1]System Condition Status Warning	SystemConditionStatus	The overall system condition is abnormal (warn or critical).	>1	<2
System Condition Status Critical	SystemConditionStatus	The overall system condition is critical.	>2	<3
Excessive Tasks Queued for Execution	TPoolRtTaskQSize	The number of tasks currently queued for execution waiting for a thread has exceeded the threshold.	>10	<10

1. All system conditions for the Cisco Unified Expert Advisor system are visible as individual RTMT alerts. These alerts appear in the Alert Central tool in RTMT under the Expert Advisor Tab. Each alert description explains the system condition and possible resolution actions.

Additional Information

See the Related Topics, page 6-7.

Alert Fields

You can configure and disable both preconfigured and user-defined alerts in RTMT. You can add and delete user-defined alerts in the performance-monitoring window; however, you cannot delete preconfigured alerts.

Table 6-2 provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 6-2 Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which RTMT associates an alert	Descriptive name. For preconfigured alerts, you cannot change this field. For a list of preconfigured alerts, see the "Viewing Alerts" section on page 6-2.
Description	Description of the alert	You cannot edit this field for preconfigured alerts. For a list of preconfigured alerts, see the "Viewing Alerts" section on page 6-2.
Performance Counter(s)	Source of the performance counter	You cannot change this field.
Threshold	Condition to raise alert	The value can be one or more of the following: up < - > down, less than #, %, rate greater than #, %, rate.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta.

Table 6-2 Alert Customization (continued)

Field	Description	Comment
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sending the alert immediately or after a specified time that the alert has persisted.
Number of Events Threshold	Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes).	For ExcessiveVoiceQualityReports, the default thresholds equal 10 to 60 minutes. For RouteListExhausted and MediaListExhausted, the defaults equal 0 to 60 minutes.
Server IDs	Cluster or list of servers to monitor	All servers in the cluster or just the selected server(s). **Note** When you deactivate all servers in the cluster, the system considers that server as removed from the currently monitored server list. When you reactivate the cluster, that server gets added back, and its settings get restored to default values.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action gets defined first (see the "Additional Information" section on page 6-4). If this field is blank, that indicates that e-mail is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disabled.
Clear Alert	Resets alert (change the color of an alert item from to black) to signal that the alert has been resolved	After an alert has been raised, its color will automatically change to and stay that way until you manually clear the alert. Use Clear All to clear all alerts.
Alert Details	Displays the detail of an alert (not configurable)	N/A
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Raise alert once every X minutes if condition persists.) Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	N/A
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts.

Additional Information

See the Related Topics, page 6-7.

Alert Action Configuration

In RTMT, you can configure alert actions for every alert that is generated and have the alert action sent to e-mail recipients that you specify in the alert action list.

Table 6-3 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 6-3 Alert Action Configuration

Field	Description	Comment
Alert Action ID	ID of alert action to take	Specify descriptive name.
Mail Recipients	List of e-mail addresses. You can selectively enable/disable an individual e-mail in the list.	N/A

Additional Information

See the Related Topics, page 6-7.

Enabling Trace Download

Some preconfigured alerts will allow you to initiate a trace download based on the occurrence of an event. You can automatically capture traces when a particular event occurs by checking the Enable Trace Download check box in Set Alert/Properties for the following alerts:

- CriticalServiceDown
- CoreDumpFileFound

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

Additional Information

See the Related Topics, page 6-7.

Understanding Alert Logs

The alert log stores the alert, which is also stored in memory. The memory gets cleared at a constant interval, leaving the last few minutes (30 minutes or longer) of data in the memory. When the service starts/restarts, the last few minutes of the alert data load into the memory by the system reading from the alert logs that exist in all servers in the cluster. The alert data in the memory gets sent to the RTMT clients on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last few minutes in the Alert Central log history. Alert log periodically gets updated, and new logs get inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

The following file name format for the alert log applies: AlertLog_MM_DD_YYYY_hh_mm.csv.

The alert log includes the following attributes:

- Time Stamp—Time when RTMT logs the data
- Alert Name—Descriptive name of the alert
- Node—Node name for where RTMT raised the alert

- Alert Message—Detailed description about the alert
- Description—Description of the monitored object
- Severity—Severity of the alert
- PollValue—Value of the monitored object where the alert condition occurred
- Action—Alert action taken
- Group ID—Identifies the source of the alert

The first line of each log file comprises the header. Details of each alert get written in a single line, separated by a comma.

Additional Information

See the Related Topics, page 6-7.

Log Partition Monitoring

Log Partition Monitoring, which is installed automatically with the system, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partitioning Monitoring Tool service starts automatically after installation of Cisco Unified Expert Advisor.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition on a server:

- 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 & 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.

In addition, Cisco Log Partitioning Monitoring Tool service checks the server every 5 seconds for newly created core dump files. If there are new core dump files, Cisco Log Partitioning Monitoring Tool service sends a CoreDumpFileFound alarm and an alert to Alert Central with information on each new core file.

To utilize log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on each node in the cluster on Cisco Unified Serviceability. Stopping the service causes a loss of feature functionality.

When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends a alarm message to syslog and generates a corresponding alert in RTMT Alert central.

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central. For more information, see "Setting Alert Properties" section on page 7-2.

To offload the log files and regain disk space on the server, you should collect the traces that you are interested in saving by using the Real-Time Monitoring tool.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

Note Log Partition Monitoring automatically identifies the common partition that contains an active directory and inactive directory. The active directory contains the log files for the current version of Cisco Unified Expert Advisor, and the inactive directory contains the log files for the previous installed version of Cisco Unified Expert Advisor. If necessary, the service deletes log files in the inactive directory first. The service then deletes log files in the active directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low water mark. The service does not send an e-mail when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5 minute intervals.

Related Topics

- Understanding Alerts, page 6-1
- Viewing Alerts, page 6-2
- Alert Fields, page 6-3
- Alert Action Configuration, page 6-4
- Enabling Trace Download, page 6-5
- Understanding Alert Logs, page 6-5
- Working with Alerts, page 7-1
- Setting Alert Properties, page 7-2
- Configuring E-mails for Alert Notification, page 7-4
- Configuring Alert Actions, page 7-5

CHAPTER 7

Working with Alerts

This chapter contains 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 7-2.
- To configure e-mails for alert notification, see the "Configuring E-mails for Alert Notification" section on page 7-4.
- To configure alert actions, see the "Configuring Alert Actions" section on page 7-5.
- 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 In Safe Range 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" section on page 7-5.

Setting Alert Properties

The following procedure describes how to set alert properties.g

Procedure

Step 1 Display Alert Central, as described in the "Working with Alerts" section on page 7-1.

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**.

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, continue to Step 18. To edit an existing alert action, skip to Step 25.

Step 18 Click **Add**.

Step 19 In the Name field, enter a name for the alert action.

Step 20 In the Description field, enter a description of the alert action.

Step 21 To add an e-mail recipient, click **Add**.

Step 22 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.

Step 23 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.

Step 24 When you finish adding all the recipients, click **OK**. Skip to Step 27.

Step 25 To edit an existing alert action, highlight the alert action and click **Edit**.

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

Step 26 Update the configuration and click **OK**. Continue to Step 27.

Step 27 After you finish alert action configuration, click **Close**.

Step 28 For alerts that do not allow trace download, click **Activate** in the Alert Properties: Email Notification window.

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

a. Click **Next**.

b. In the Alert Properties: Trace Download window, check the Enable Trace 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 get saved.

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

e. In the Trace 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 Trace 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" section on page 7-5.

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" section on page 7-5.

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 7-1.

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

Step 3 Perform Step 17 through Step 28 in the "Setting Alert Properties" section on page 7-2 to add, edit, or delete alert actions.

Additional Information

See the "Related Topics" section on page 7-5.

Related Topics

- Working with Alerts, page 7-1
- Setting Alert Properties, page 7-2
- Configuring E-mails for Alert Notification, page 7-4
- Configuring Alert Actions, page 7-5
- Configuring Alert Notification for a Counter, page 5-4
- Alerts, page 6-1

CHAPTER 8

Configuring Trace & Log Central in RTMT

The Trace & Log Central feature in the Cisco Unified Expert Advisor 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 a SFTP or FTP 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. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Note To use the Trace & 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 Expert Advisor 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.

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 & Log Central option. If you do not import the certificates, the Trace & Log Central option displays a security certificate for each node in the cluster each time that you log into RTMT and access the Trace & Log Central option. You cannot change any data that displays for the certificate.

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

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

Additional Information

See the Related Topics, page 8-24.

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 8-2.

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

- In the Quick Launch Channel, click **System**; then, click the **Trace & Log Central** icon.
- Choose **Tools > Trace > 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 Trace Files" section on page 8-3
- 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 8-6
- Schedule a recurring trace collection and download the trace files to a SFTP or FTP server on your network. See "Scheduling Trace Collection" section on page 8-10
- Collect a crash dump file for one or more servers on your network. See "Collecting a Crash Dump" section on page 8-13.
- View the trace files that you have collected. See the "Using Local Browse" section on page 8-16.
- View all of the trace files on the server. See the "Using Remote Browse" section on page 8-17.
- View the current trace file 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 8-20.

Additional Information

- See Related Topics, page 8-24.

Collecting Trace Files

Use the Collect Files option in Trace & Log Central 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 & 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 8-6.

RTMT Trace & Log Central Disk IO and CPU Throttling

Caution In Cisco Unified Expert Advisor, throttling is turned on by default, and cannot be configured.

RTMT supports the throttling of critical Trace & Log Central operations and jobs, whether they are running on demand, scheduled, or automatic. The throttling slows the operations when IO utilization is in high demand for call processing, so call processing can take precedence.

When you make a request for an on-demand operation when the active node is running under high IO conditions, the system displays a warning which gives you the opportunity to abort the operation. Be aware that the IO rate threshold values that control when the warning displays are configurable with the following service parameters (Cisco RISDC service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The values of these parameters get compared to the actual system CPU and IOWait values. If the goal (the value of the service parameter) is lower than the actual value, the system displays the warning.

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 in Cisco Unified Serviceability. For more information, refer to *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.
- Configure the throttling of critical Trace & Log Central operations and jobs by setting the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RISDC service). For more information on configuring service parameters, refer to the *Administration and Configuration Guide for Cisco Unified Expert Advisor*.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

The Trace Collection wizard displays.

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 CUEA Services/Applications tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- To collect traces for all services and applications for all servers, 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 trace collection 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:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- 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 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 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.

Trace & Log Central downloads the file with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

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.

In the Download File option group box, specify the options you want for downloading 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 Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory.

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 <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

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 <Server name or 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 8-16.

Note You will see an error message if the service parameter values are exceeded.

Additional Information

- For information about setting the values of service parameters, see the Service Parameters Configuration chapter in the *Cisco Expert Advisor Administration Guide*.
- Also see Related Topics, page 8-24.

Collecting Installation Logs

The following procedure describes how to collect installation and upgrade logs in Trace & Log Central.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - Click the **Trace & Log Central** icon.
- Choose **Tools > Trace > Trace & Log Central**.

The Trace & Log Central window displays.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Install Logs**.

The Collect Install Logs wizard displays

Step 3 In the Select Servers Options box, specify from which server you would like to collect the install logs. To collect the install logs for a particular server, check the check box next to the server. To collect the install logs for all servers, check the Select All Servers check box.

Step 4 In the Download File Options, specify the directory where you want to download the log file. To specify the directory in which you want to download the log files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 5 Click **Finish**.

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.

Note You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

From the Trace Configuration window in Cisco Unified Serviceability, configure the information that you want to include in the trace files for the various services. For more information, refer to *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Query Wizard**.

The Query wizard displays.

Step 3 In the Query Wizard Options window, 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 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 19. To modify the query, go to Step 4.

- Create Query

Step 4 Click **Next**.

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 server name or server IP address.

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 6 In the Select CUEA Services/Applications tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 7 Click **Next**.

Step 8 In the Select System Logs tab, choose the logs in which you are interested by checking all check boxes that apply.

Step 9 Click **Next**.

Step 10 In the Query Time Options 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.

Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

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 11 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box.

Step 12 Click **Next**.

Step 13 In the Action Options window, choose one of the following actions:

- Trace Browse
- On Demand Trace Collection
  - 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 selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - 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.
- Schedule Download

  Included a start date and time and an end date and time. To configure the trace server, click the Configure Trace Server checkbox. The SFTP Parameters dialog box displays. In the dialog box, you can configure the following parameters:
  - Host IP Address
  - User Name
  - Password
  - Port
  - Download Directory Path

Step 14 Choose one of the following options:

- To execute the query, click **Run Query**. This option is only available if you selected Trace Browse from the Action Options window.

  The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **Close** and continue with Step 19.
- To save the query, click the **Save Query** button and continue with Step 15.

- To download the trace, click the **Download Trace** button. This option is only available if you selected On Demand Trace Collection or Schedule Download from the Action Options window.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the Trace & Log Central feature. For more information, see the "Using Local Browse" section on page 8-16.

Step 15 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.

  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 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 16 Click **Finish**.

Step 17 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 18 Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with Step 19.
- To exit the query wizard without running the query that you created, click **Cancel**.

Step 19 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, 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. 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.

- 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 the **Download** button, 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 selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - 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 & Log Central feature. For more information, see the "Using Local Browse" section on page 8-16.

- To save the query, click **Save Query** button and complete Step 15 through Step 17.

Note You will see an error message if the service parameter values are exceeded.

Additional Information

See the Related Topics, page 8-24.

Scheduling Trace Collection

You can use the Schedule Collection option of the Trace & Log Central feature to schedule up to six concurrent trace collections and to download the trace files to a SFTP or FTP 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 six trace collection can be concurrent. That is, only six 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 of Cisco Unified Serviceability. For more information, refer to the *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.
- 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, refer to the *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Schedule Collection**.

The Schedule Collection wizard displays.

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 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 CUEA Services/Applications tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- To collect traces for all services and applications for all servers, 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 schedule collection 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:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- 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 server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the schedule 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 & 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 a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box

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. If you chose Download Files or Run Another Query, continue with Step 16.
- Run Another Query
- Generate Syslog. If you chose Generate Syslog, go to Step 18.

Step 16 In the SFTP/FTP Server Parameters group box, enter the server credentials for the server where the Trace & Log Central feature downloads the results and click **Test Connection**. After the Trace & Log Central feature verifies the connection to the SFTP or FTP server, click **OK**.

Note The **Download Directory Path** field specifies the directory in which the Trace & 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 or FTP parameters fields: /home/<user>/Trace.

Step 17 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 & Log Central feature only executes the specified query if the first query generates results.

Step 18 Click **Finish**.

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

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

Step 19 Click **OK**.

Step 20 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of 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 8-24.

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 tree hierarchy, as described in "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

Step 2 Double-click **Job Status**.

The Job Status Window displays.

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, 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 delete jobs with a status of "Pending" or "Running" and a job type of "Schedule Task" or job type of "RealTimeFileSearch."

Additional Information

See the Related Topics, page 8-24.

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 8-2.

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

The Collect Crash Dump wizard displays.

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 CUEA Services/Applications tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- To collect traces for all services and applications for all servers, 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:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- 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 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 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.

  Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

  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 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 Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory.

Note Cisco Unified Serviceability does not retain logs from Cisco Unified Expert Advisor 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 <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 10 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 11 To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

Step 12 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 8-24.

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 & 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.

Note You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

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

- "Collecting Trace Files" section on page 8-3
- "Using the Query Wizard" section on page 8-6
- "Scheduling Trace Collection" section on page 8-10

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

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 If the file type has a viewer already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box displays. Click the program (viewer) that you would like to use to view the file. If your preferred program is not on the list, choose another program by clicking the **Other** button.

If you want to use this program as your default viewer, click the **Always use this program to open these files** check box

The real-time monitoring tool displays the file in the appropriate viewer for the file type.

Additional Information

See the Related Topics, page 8-24.

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 & Log Central feature.

Note You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

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

- "Collecting Trace Files" section on page 8-3
- "Using the Query Wizard" section on page 8-6
- "Scheduling Trace Collection" section on page 8-10

Procedure

Step 1 Display the Trace & Log Central options, as described in the "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

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 10.

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

Note If you choose Crash Dump, the wizard only displays the services that may cause a crash dump. If you do not see the service in which you are interested, click **Back** and choose Trace Files.

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 CUEA Services/Applications tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- To collect traces for all services and applications for all servers, 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 Remote Browse wizard without collecting traces for services or applications, go to Step 5.

Step 5 Click **Next**.

Step 6 In the Select System Services/Application tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- 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 server.
- To collect 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 10.

Step 7 In the Select CUEA Services/Applications tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- To choose crash dump files for all services and applications for all servers, 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 server.
- To choose crash dump files for particular services or applications on particular servers, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting crash dump files, go to Step 8.

Step 8 Click **Next**.

Step 9 In the Select System Services/Application tab, perform one of the following tasks:

Note When you check the **Select All Services on All Servers** check box, Trace & Log Central will collect traces from all servers in the cluster.

- 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 server.
- To choose crash dump files for particular system logs on particular servers, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting crash dump files, go to Step 10.

Step 10 Click **Finish**.

Step 11 After the traces become available, a message displays. Click **Close**.

Step 12 To display log files, navigate to the file through the tree hierarchy.

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.

Step 13 After the log file name displays in the pane on the right side of the window, use one of the following methods to display the selected log file:

- For .log and/or .out files—Use one of the following methods:
  - Right-click the required file and select **Open** to view it in the Cisco Default Viewer.
  - Alternately, you can also right-click on the required file and select **Open with** to view all available programs with which to open these files.

Caution The Cisco QRT Viewer program is not supported by Cisco Unified Expert Advisor as an option to view files.

- Using .zip files: Some files may use the ZIP format and in these cases, you will need to use the .zip file viewer to view these files.

Caution Cisco Unified Expert Advisor provides some log files in a ZIP format. The Trace & Log Central Remote Browse feature in Cisco Unified Communications RTMT does not display .zip files by default. You can choose to add the appropriate application program or download/save the .zip file and view it directly from the downloaded location.

To add the appropriate application program to view .zip files (for example, Winzip.exe, or other similar programs) to the list of programs, follow this procedure:

a. right-click the required .zip file and select **Open with**.

   The Open with window opens to display the available programs.

b. If the required program is not listed, click the **Other** button at the bottom of this window.

   In the resulting browse window, navigate to the location of the required program file and select it to be added to the RTMT list.

c. Click OK to add it to the RTMT list.

d. The selected program is now added to the RTMT list. You can now use this program to open .zip files.

Step 14 To download 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 <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
- 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 server, 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 & Log Central feature. For more information, see the "Using Local Browse" section on page 8-16.

Additional Information

See the Related Topics, page 8-24.

Using Real-Time Trace

The real-time trace option of the Trace & 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 8-20
- Monitor User Event, page 8-21

View Real-Time Data

The view real-time data option of the Trace & 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, with a limit of 3 concurrent sessions on a single server. 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 8-2.

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 View Real Time Data wizard displays.

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

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

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

Note The following warning message displays at the bottom of this window: If trace compression is enabled, the data seen in this window can be bursty due to buffering of data.

Step 6 Click **Finish**. The real-time data for the chosen service displays in the generic log viewer.

Step 7 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 8 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 9 When you are done viewing the real-time data, click **Close** on the generic log viewer.

Tip To search by phrases or words in the Log Viewer, enter the word or phrase in the Search String field. If you want to do a case sensitive search for a word or phrase, check the Match Case check box.

Additional Information

See the Related Topics, page 8-24.

Monitor User Event

The monitor user event option of the Trace & 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 LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 7-2.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace & Log Central Options in RTMT" section on page 8-2.

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 server that you want the system to monitor from the **Nodes** drop-down list box and click **Next**.

Step 6 Choose the product, 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.

Trace & Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

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 LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 7-2.
- 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/FTP Server Parameters group box, choose either FTP or SFTP, enter the server credentials for the server where you want to download the trace files, and click **Test Connection**. After the Trace & Log Central feature verifies the connection to the SFTP or FTP server, click **OK**.

Note The Download Directory Path field specifies the directory in which the Trace & 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/FTP 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.

Note The following warning message displays at the bottom of this window: If trace compression is enabled, there might be a delay in catching the event after it occurs, due to buffering of data.

Step 10 Click **Finish**.

Additional Information

See the Related Topics, page 8-24.

Updating the Trace Configuration Settings

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 Documents and Settings directory for the user; for example, on a Windows machine, the log gets stored in C:\Documents and Settings\<userid>\.jrtmt\log.

Tip The Error radio button equals the default setting.

Additional Information

See the Related Topics, page 8-24.

Related Topics

- Using the Query Wizard, page 8-6
- Using Local Browse, page 8-16
- Collecting Trace Files, page 8-3
- Scheduling Trace Collection, page 8-10
- Displaying Trace & Log Central Options in RTMT, page 8-2
- Collecting a Crash Dump, page 8-13
- Using Local Browse, page 8-16
- *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*

CHAPTER 9

Using SysLog Viewer in RTMT

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

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 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 9-1 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 a column heading. The first time that you click 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 9-1 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 every 5 seconds by checking the Auto Refresh check box.
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.

Related Topics

Chapter 2, “Installing and Configuring Real-Time Monitoring Tool”

APPENDIX A

Performance Objects and Counters for the System

This appendix provides information on system-related objects and counters. For information on specific counters, click the blue text in the following list to go to the object:

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for for system monitoring, access the performance monitoring counters in the Real-Time Monitoring Tool. In RTMT, you can review a counter description, as described in the "Displaying Performance Counters" section on page 5-1.

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP)/HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related web pages are accessed. The Secure Socket Layer (SSL) status of the URLs for web applications provides the basis for the instance name for each Tomcat HTTP Connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL. Table A-1 contains information on the Tomcat HTTP connector counters.

Table A-1 Cisco Tomcat Connector

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that the connector encountered. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesReceived	This counter represents the amount of data that the connector received. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector.For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesSent	This counter represents the amount of data that the connector sent. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Requests	This counter represents the total number of request that the connector handled. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsTotal	This counter represents the current total number of request processing threads, including available and in-use threads, for the connector. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Table A-1 Cisco Tomcat Connector (continued)

Counters	Counter Description
ThreadsMax	This counter represents the maximum number of request processing threads for the connector. Each incoming request on a Cisco Unified Expert Advisor related window requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads will be created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests will receive connection refused messages until resources are available to process them. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The Connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Expert Advisor related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsBusy	This counter represents the current number of busy/in-use request processing threads for the connector. A Tomcat Connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when web pages that are related to Cisco Unified Expert Advisor are accessed. The Secure Sockets Layer (SSL) status of the URLs for the web application provides the basis for the instance name for each Tomcat connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the Tomcat JVM, which represents, among other things, a pool of common resource memory that Cisco Unified Expert Advisor related web applications such as Cisco Unified Expert Advisor, Cisco Unified Serviceability, and more use. Table A-2 contains information on the Tomcat JVM counters.

Table A-2 Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified Expert Advisor operations console and Cisco Unified Serviceability create. When the amount of free dynamic memory is low, more memory gets automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
KBytesMemoryMax	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Expert Advisor Administration and Cisco Unified Serviceability create.
KBytesMemoryTotal	This counter represents the current total dynamic memory block size, including free and in-use memory, of Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Expert Advisor Administration and Cisco Unified Serviceability create.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to run Cisco Unified Expert Advisor web applications. The URLs for the web application provide basis for the instance name for each Tomcat Web Application. For example, Cisco Expert Advisor Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified Serviceability gets identified by ccmservice, Cisco Unified Expert Advisor User Options gets identified by ccmuser, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root. Table A-3 contains information on the Tomcat Web Application counters.

Table A-3 Tomcat Web Application

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that a Cisco Unified Expert Advisor related web application encountered. The URLs for the web application provide the basis instance name for each Tomcat Web Application.
Requests	This counter represents the total number of requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly. The URLs for the web application provide the basis instance name for each Tomcat Web Application.
SessionsActive	This counter represents the number of sessions that the web application currently has active (in use). The URLs for the web application provide the basis instance name for each Tomcat Web Application.

Database Change Notification Client

The Database Change Notification Client object provides information on change notification clients. Table A-4 contains information on the Database Change Notification Client counters.

Table A-4 Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	This counter represents the number of database change notifications that have been processed. This counter refreshes every 15 seconds.
MessagesProcessing	This counter represents the number of change notification messages that are currently being processed or are waiting to be processed in the change notification queue for this client. This counter refreshes every 15 seconds.
QueueHeadPointer	This counter represents the head pointer to the change notification queue. The head pointer acts as the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds.
QueueMax	This counter represents the largest number of change notification messages that will be processed for this client. This counter remains cumulative since the last restart of the Cisco Database Layer Monitor service.

Table A-4 Database Change Notification Client (continued)

Counters	Counter Descriptions
QueueTailPointer	This counter represents the tail pointer to the change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds
TablesSubscribed	This counter represents the number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information on different change-notification-related statistics. Table A-5 contains information on the Database Change Notification Server counters.

Table A-5 Database Change Notification Server

Counter	Counter Descriptions
Clients	This counter represents the number of change notification clients (services/servlets) that have subscribed for change notification.
QueuedRequestsInDB	This counter represents the number of change notification records that are in the DBCNQueue (Database Change Notification Queue) table via direct TCP/IP connection (not queued in shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	This counter represents the number of change notification requests that are queued in shared memory.

Database Change Notification Subscription

The Database Change Notification Subscription object displays the names of tables where the client will receive Change Notifications.

The SubscribedTable object displays the table with the service or servlet that will receive change notifications. Because the counter does not increment, this display occurs for informational purposes only

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. Table A-6 contains information on the Database local DSN.

Table A-6 Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	This counter represents the amount of CcmDbSpace that is being consumed
CcmtempDbSpace_Used	This counter represents the amount of CcmtempDbSpace that is being consumed.

Table A-6 Database Local Data Source Name (continued)

Counters	Counter Descriptions
LocalDSN	This counter represents the data source name (DSN) that is being referenced from the local machine.
RootDbSpace_Used	This counter represents the amount of RootDbSpace that is being consumed.

DB User Host Information Counters

The DB User Host Information object provides information on DB User Host.

The DB:User:Host Instance object displays the number of connections that are present for each instance of DB:User:Host.

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces. Table A-7 contains information on the enterprise replication DB monitors.

Table A-7 Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	This counter represents the amount of enterprise replication DbSpace that was consumed.
ERSBDbSpace_Used	This counter represents the amount of ERDbSpace that was consumed.

Enterprise Replication Perfmon Counters

The Enterprise Replication Perfmon Counter object provides information on the various replication counters.

The ServerName:ReplicationQueueDepth counter displays the server name followed by the replication queue depth.

IP

The IP object provides information on the IP statistics on your system. Table A-8 contains information on the IP counters.

Table A-8 IP

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated at this entity.
Frag Fails	This counter represents the number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that were successfully fragmented at this entity.

Table A-8 IP (continued)

Counters	Counter Descriptions
In Delivers	This counter represents the number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).
In Discards	This counter represents the number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	This counter represents the number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	This counter represents the total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.
Reasm Fails	This counter represents the number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that required reassembly at this entity.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. Table A-9 contains information on memory counters.

Table A-9 Memory

Counters	Counter Descriptions
% Mem Used	This counter displays the system physical memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes) / Total KBytes, which also corresponds to the Used KBytes/Total KBytes.
% Page Usage	This counter represents the percentage of active pages.
% VM Used	This counter displays the system virtual memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes) / (Total KBytes + Total Swap KBytes), which also corresponds to Used VM KBytes/Total VM KBytes.

Table A-9 Memory (continued)

Counters	Counter Descriptions
Buffered KBytes	This counter represents the capacity of buffers in your system in kilobytes.
Cached KBytes	This counter represents the amount of cached memory in kilobytes.
Free KBytes	This counter represents the total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	This counter represents the amount of free swap space that is available in your system in kilobytes.
Pages	This counter represents the number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	This counter represents the number of pages that the system paged in from the disk.
Pages Output	This counter represents the number of pages that the system paged out to the disk.
Shared KBytes	This counter represents the amount of shared memory in your system in kilobytes.
Total KBytes	This counter represents the total amount of memory in your system in kilobytes.
Total Swap KBytes	This counter represents the total amount of swap space in your system in kilobytes.
Total VM KBytes	This counter represents the total amount of system physical and memory and swap space (Total Kbytes + Total Swap Kbytes) that is in use in your system in kilobytes.
Used KBytes	This counter represents the amount of system physical memory that is in use on the system in kilobytes. The value of the Used KBytes counter equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes. The Used KBytes value differs from the Linux term that displays in the top or free command output. The Used value that displays in the top or free command output equals the difference in Total KBytes - Free KBytes and also includes the sum of Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your system in kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swap space that is in use on your system in kilobytes. The value equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes. This corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. Table A-10 contains information on network interface counters.

Table A-10 Network Interface

Counters	Counter Descriptions
Rx Bytes	This counter represents the number of bytes, including framing characters, that were received on the interface.
Rx Dropped	This counter represents the number of inbound packets that were chosen to be discarded even though no errors had been detected. This prevents the packet from being delivered to a higher layer protocol. Discarding packets to free up buffer space provides one reason.
Rx Errors	This counter represents the number of inbound packets (packet-oriented interfaces) and the number of inbound transmission units (character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.

Table A-10 Network Interface (continued)

Counters	Counter Descriptions
Rx Multicast	This counter represents the number of multicast packets that were received on this interface.
Rx Packets	This counter represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This counter represents the total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	This counter represents the total number of Rx packets and Tx packets.
Tx Bytes	This counter represents the total number of octets, including framing characters, that were transmitted out from the interface.
Tx Dropped	This counter represents the number of outbound packets that were chosen to be discarded even though no errors were detected. This action prevents the packet from being delivered to a higher layer protocol. Discarding a packet to free up buffer space represents one reason.
Tx Errors	This counter represents the number of outbound packets (packet-oriented interfaces) and the number of outbound transmission units (character-oriented or fixed-length interfaces) that could not be transmitted because of errors.
Tx Packets	This counter represents the total number of packets that the higher level protocols requested for transmission, including those that were discarded or not sent. This does not include packets that were addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	This counter represents the length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides information about the replication state on the system. Table A-11 contains information on replication counters.

Table A-11 Number of Replicates Created and State of Replication

Counters	Counter Descriptions
Number of Replicates Created	This counter displays the number of replicates that were created by Informix for the DB tables. This counter displays information during Replication Setup.
Replicate_State	This counter represents the state of replication. The following list provides possible values: • 0—Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed. • 1—The system created replicates of some tables but not all tables. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 2—Good Replication. • 3—Bad Replication. When the counter displays a value of 3, consider replication in the cluster as bad. It does not mean that replication failed on a particular node. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 4—Replication setup did not succeed.

Partition

The partition object provides information about the file system and its usage in the system. Table A-12 contains information on partition counters.

Table A-12 Partition

Counters	Counter Descriptions
% CPU Time	This counter represents the percentage of CPU time that is dedicated to handling I/O requests that were issued to the disk.
% Used	This counter represents the percentage of disk space that is in use on this file system.
Await Read Time	This counter represents the average time, measured in milliseconds, for Read requests that are issued to the device to be served.
Await Time	This counter represents the average time, measured in milliseconds, for I/O requests that were issued to the device to be served. This includes the time spent by the requests in queue and the time spent servicing them.
Await Write Time	This counter represents the average time, measured in milliseconds, for write requests that are issued to the device to be served.
Queue Length	This counter represents the average queue length for the requests that were issued to the disk.
Read Bytes Per Sec	This counter represents the amount of data in bytes per second that was read from the disk.
Total Mbytes	This counter represents the amount of total disk space that is on this file system in megabytes.
Used Mbytes	This counter represents the amount of disk space that is in use on this file system in megabytes.
Write Bytes Per Sec	This counter represents the amount of data that was written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. Table A-13 contains information on process counters.

Table A-13 Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total CPU time, represents the tasks share of the elapsed CPU time since the last update.
% MemoryUsage	This counter represents the percentage of physical memory that a task is currently using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task encountered that required the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically wraps, but the value will never equal zero.

Table A-13 Process (continued)

Counters	Counter Descriptions
Process Status	This counter displays the process status: • 0—Running • 1—Sleeping • 2—Uninterruptible disk sleep • 3—Zombie • 4—Stopped • 5— Paging • 6—Unknown
Shared Memory Size	This counter displays the amount of shared memory (KB) that a task is using. Other processes could potentially share the same memory.
STime	This counter displays amount of system time (STime), measured in jiffies, that this process has scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second consists of 100 jiffies.
Thread Count	This counter displays the number of threads that are currently grouped with a task. A negative value (-1) indicates that this counter is currently not available. This happens when thread statistics (which includes all performance counters in the Thread object as well as the Thread Count counter in the Process object) are turned off because the system total processes and threads exceeded the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user mode and kernel mode since the start of the task. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second consists of 100 jiffies.
UTime	This counter displays the time, measured in jiffies, that a task has scheduled in user mode.
VmData	This counter displays the virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB) This includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in kilobytes (KB). It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

Processor

The processor object provides information on different processor time usage in percentages. Table A-14 contains information on processor counters.

Table A-14 Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed CPU time, excluding idle time, since the last update. This share gets expressed as a percentage of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idle state and did not have an outstanding disk I/O request.

Table A-14 Processor (continued)

Counters	Counter Descriptions
IOwait Percentage	This counter represents the percentage of time that the processor is in the idle state while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends executing the interrupt request that is assigned to devices, including the time that the processor spends sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends executing at the user level with nice priority.
Softirq Percentage	This counter represents the percentage of time that the processor spends executing the soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is executing processes in system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is executing normal processes in user (application) level.

System

The System object provides information on file descriptors on your system. Table A-15 contains information on system counters

Table A-15 System

Counters	Counter Descriptions
Allocated FDs	This counter represents the total number of allocated file descriptors.
Being Used FDs	This counter represents the number of file descriptors that are currently in use in the system.
Freed FDs	This counter represents the total number of allocated file descriptors on the system that are freed.
Max FDs	This counter represents the maximum number of file descriptors that are allowed on the system.
Total CPU Time	This counter represents the total time in jiffies that the system has been up and running.
Total Processes	This counter represents the total number of processes on the system.
Total Threads	This counter represents the total number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system. Table A-16 contains information on the TCP counters.

Table A-16 TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED stated from either the SYN-RCVD state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state.
Curr Estab	This counter displays the number of TCP connections where the current state is either ESTABLISHED or CLOSE- WAIT.
Estab Resets	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
In Segs	This counter displays the total number of segments that were received, including those received in error. This count only includes segments that are received on currently established connections.
InOut Segs	This counter displays the total number of segments that were sent and the total number of segments that were received.
Out Segs	This counter displays the total number of segments that were sent. This count only includes segments that are sent on currently established connections, but excludes retransmitted octets.
Passive Opens	This counter displays the number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that were retransmitted because the segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system. Table A-17 contains information on the Thread counters.

Table A-17 Thread

Counters	Counter Description
% CPU Time	This counter displays the threads share of the elapsed CPU time since the last update. This counter expresses the share as a percentage of the total CPU time.
PID	This counter displays the threads leader process ID.

Related Topics

- Chapter 4, “Understanding Performance Monitoring”
- Chapter 5, “Configuring and Displaying Performance Counters”

APPENDIX B

Performance Objects and Counters for the Cisco Unified Expert Advisor

This appendix provides information on system-related objects and counters. All Cisco Unified Expert Advisor's perfmon counters are logged in RTMT by default.

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for for system monitoring, access the performance monitoring counters in RTMT. In RTMT, you can review a counter description, as described in the "Displaying Performance Counters" section on page 5-1.

The class object provides information on different processor time usage in percentages. Table B-1 contains information on processor counters.

Table B-1 Class Objects

Counters	Counter Descriptions
Class: Expert Advisor General Information section	
LocalDeviceType	This object specifies the type of Cisco Unified Expert Advisor device: • runtime server (1) • reporting server (2) • other (3) • A value of 0 indicates that the Cisco Unified Expert Advisor application is not running (terminated) and hence RTMT is unable to contact it.
SystemConditionStatus	This object provides an overall summary of Cisco Unified Expert Advisor system conditions. It specifies the health of the Cisco Unified Expert Advisor: • statusNormal=1 (green) • statusWarn=2 (yellow) • statusCritical=3 (red) • A value of 0 indicates that the Cisco Unified Expert Advisor application is not running (terminated) and hence RTMT is unable to contact it. A management station can use this status along with specific conditions raised, that are in the Cisco Unified Expert Advisor system condition counter to learn about the health of the Cisco Unified Expert Advisor.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
SystemStatus	The SystemStatus object is the last known status of the Cisco Unified Expert Advisor application. It summarizes the overall status of all services in Cisco Unified Expert Advisor. It can have the following values: • terminated (0): The process is terminated and RTMT is not able to contact it. • inService (3): The service is up and running optimally, accepting connections at full QoS (if applicable). • partialService (6): The service is no longer accepting new calls but finishes processing active calls (may be due to a loss of a dependency connectivity, or a shutdown request). • stopped (9): The service has shut down and is not processing any more calls. The process itself is terminating (performing memory cleanup, saving settings, shutting down threads, etc.).
Class: Expert Advisor License Information section	
LicRtTotalExpertAdvisorsConfigurable	The total number of Cisco Unified Expert Advisor licenses configured on this device.
Class: Expert Advisor Thread Pool section	
TPoolRtIdleThreads	The real-time idle threads object is a real-time snapshot metric indicating the number of idle threads in the pool waiting for work. The thread pool is a cache of threads used (by Cisco Unified Expert Advisor components only) for the processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.
TPoolRtRunningThreads	The real-time running threads object is a real-time snapshot metric indicating the number of running threads in the pool currently processing work. The thread pool is a cache of threads used (by Cisco Unified Expert Advisor components only) for the processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.
TPoolRtCoreThreads	The real-time core threads object is a real-time snapshot metric indicating the number of threads in the pool that will never be destroyed no matter how long they remain idle. The thread pool is a cache of threads used (by Cisco Unified Expert Advisor components only) for the processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.
TPoolRTMaxThreadsAvail	The real-time maximum threads available object is a real-time snapshot metric indicating the maximum number of threads in the pool that can exist simultaneously. The thread pool is a cache of threads used (by Cisco Unified Expert Advisor services only) for the processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
TPoolRtMaxThreadsUsed	The real-time maximum threads used object is a real-time snapshot metric indicating the peak number of threads in the pool that are simultaneously tasked with work to process. The thread pool is a cache of threads used (by Cisco Unified Expert Advisor components only) for the processing of relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.
TPoolRtTaskQSize	The real-time task queue size object is a real-time snapshot metric indicating the number of tasks in queue.
Class: Expert Advisor JVM Statistics	
EnvRtMaxMemUsed	The real-time maximum memory used object is a real-time snapshot metric indicating the peak memory allocated to the runtime environment. The object value is expressed in MegaBytes (MB) and indicates the high water mark of memory that can be used by the runtime environment
EnvRtCurrMemUsed	The real-time current memory used object is a real-time snapshot metric indicating the current memory usage by the runtime environment. The object value is expressed in MB and indicates the current amount of memory used by this runtime environment.
EnvRtCommitMemUsed	The real-time current memory used object is a real-time snapshot metric indicating the memory committed by the runtime environment. This memory is guaranteed to be available to the runtime environment and can change dynamically over time but is never less than EnvRtCurrMemUsed. The object value is expressed in MB.
EnvRtMaxMemAvail	The real-time maximum memory available object is a real-time snapshot metric indicating the maximum amount of System memory available. The object value is expressed in MB.
EnvRtCurrMemAvail	The real-time current memory available object is a real-time snapshot metric indicating the amount of system memory not being used. The object value is expressed in MB and indicates the amount of current system memory that is currently not being used.
EnvRtCurrThreadsInUse	The real-time current threads in use object is a real-time snapshot metric indicating a count of threads that are in use in the runtime environment. The number of threads in use by the runtime environment include all of the Cisco Unified Expert Advisor standalone and thread pool threads as well as those threads created by the web application server running within the same runtime environment.
EnvMaxThreadsUsed	The real-time maximum threads used object is a real-time snapshot metric indicating the peak amount of threads used simultaneously in the runtime environment since startup. The maximum number of threads used by the runtime environment includes all Cisco Unified Expert Advisor standalone and thread pool threads as well as threads created by the web application server running within the same runtime environment.
EnvRtUpTime	The real-time up time object is a real-time snapshot metric indicating how long the Cisco Unified Expert Advisor application has been running. The object value is expressed as a count of milliseconds that have elapsed since the application began executing.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
RtMsgQMemPercentUsage	The percentage of available message bus memory in use. The object value is expressed as a count of MB.
MaxMsgQMemAvail	The actual amount of available message bus memory for use.
Class: Expert Advisor Services Table	
ServiceType	The service type object identifies the type of Cisco Unified Expert Advisor functional service: • cm(1) Contact Manager • rm(2) Resource Manager • wa(3) Work Assigner • mpa(4) Media Platform Adapter • bre(5) Business Rule Engine • icmgw(6) ICMGW • rda(7), -- Resource Desktop Adapter • ra(8) Reporting Adapter • rs(9) Reporting Subsystem
ServiceStatus	The service status object is the last known status of the Cisco Unified Expert Advisor application service. The various values are: • disabled(1) • starting(2) • inService(3) • inServiceWarning(4 • inServiceCritical(5) • partialService(6) • outOfService(7) • stopping(8) • stopped(9) • unknown(10)
ServiceIntPeriod	The interval period object defines the number of minutes of accumulated values for the interval and aggregate statistic objects in an instrumentation group. Once this period elapses, each Cisco Unified Expert Advisor service reports the next group of accumulated interval and aggregate statistical values.
RtMessageThroughput	The average message throughput in messages/sec per subsystem (service).
RtUptime	The number of seconds the subsystem (service) has been up.
RtMsgReceived	The number of messages received by the subsystem (service).
MaxThreadsAvailable	Maximum number of threads available for this service.
RtThreadsInUse	Number of currently running threads for this service.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
Class: Expert Advisor Resource Manager Table	
RmRtAgentsLoggedIn	The real-time indicator of the number of agents currently logged in.
RmRtAgentsOnCalls	The real-time indicator of the number of agents currently on calls.
RmRtAgentsReserved	The real-time indicator of the number of agents currently in the reserved state.
RmRtAgentsWrapUp	The real-time indicator of the number of agents currently wrapping up a call.
RmRtAgentsReady	The real-time indicator of the number of agents currently in the ready state.
RmRtAgentsNoQueue	The real-time indicator of the number of agents currently unallocated in any queue (most likely a configuration error).
RmAggNumOffersAccept	The number of offers accepted since Boot time.
RmIntNumOffersAccept	The number of offers accepted over the last interval.
RmAggNumOffersReject	The number of offers rejected since boot time.
RmIntNumOffersReject	The number of offers rejected over the last interval.
RmAggNumOffersTimedOut	The number of offers that timed out since boot time.
RmIntNumOffersTimedOut	The number of offers that timed out over the last interval.
Class: Expert Advisor Contact Manager Table	
CmRtNumActiveCalls	The real-time indicator of the number of active calls.
CmRtNumCallTrying	The real-time indicator of the number of calls where a contact is created; BRE script is started.
CmRtNumCallRingBack	The real-time indicator of the number of calls which currently receive ringback.
CmRtNumCallConnecting	The real-time indicator of the number of calls where a resource has been identified and selected, and the call is in the process of being connected.
CmRtNumCallConnected	The real-time indicator of the number of calls in which a contact is connected to one or more participants (e.g., self-service, agents, conference).
CmRtNumCallInitial	The real-time indicator of the number of calls in which a contact is Initial state.
CmRtNumCallTerminated	The aggregate count of contacts since boot time, that have completed processing (and thus deleted).
CmIntNumCallTerminated	The number of contacts that terminated over the last interval.
CmAggNumCallArrivals	Number of new calls which arrived at the Contact Manager since boot time.
CmIntNumCallArrivals	Number of new calls which arrived at the Contact Manager over the last interval.
CmRtNumCallRejecting	The real-time indicator of the number of calls which could not be accepted and processed (for example, due to invalid call, lack of system resources or licenses, or no agent available) and are currently in the process of being rejected.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
CmRtNumCallTransferring	The real-time indicator of the number of calls in which Participant changes are currently in progress (for example, participant adds/removes like conferencing, redirecting or transferring).
CmRtNumCallTerminating	The real-time indicator of the number of calls which are currently terminating because all parties but one have disconnected.
CmAggAvgCallDurationTime	The average call handling time since boot time in seconds.
CmIntAvgCallDurationTime	The average call handling time over the last interval in seconds.
CmAggMaxCallDurationTime	The maximum call handling time since boot time in seconds.
CmIntMaxCallDurationTime	The maximum call handling time over the last interval in seconds.
CmAggAvgCallInQueueTime	The average call time in queue since boot time in seconds.
CmIntAvgCallInQueueTime	The average call time in queue over the last interval in seconds.
CmAggMaxCallInQueueTime	The maximum call time in queue since boot time in seconds.
CmIntMaxCallInQueueTime	The maximum call time in queue over the last interval calls per minute.
CmAggAvgCallArrivalRate	The average call arrival rate since boot time calls per minute.
CmIntAvgCallArrivalRate	The average call arrival rate over the last interval in calls per minute.
CmAggMaxCallArrivalRate	The maximum of interval average call arrival rate since boot time in calls per minute.
Class: Expert Advisor RDA Table	
RdaAggNumMsgProc	The number of messages processed since boot time.
RdaIntNumMsgProc	The number of messages processed over the last interval.
RdaAggNumSuccessPresenceNotifications	The number of success Presence notifications since boot time.
RdaIntNumSuccessPresenceNotifications	The number of success Presence notifications over the last interval.
RdaAggNumUnSuccessPresenceNotifications	The number of unsuccessful presence notification since boot time.
RdaIntNumUnSuccessPresenceNotifications	The number of unsuccessful presence notification over the last interval.
RdaRtNumActiveClients	The real-time number of active end-user devices that has capability to perform instant message operation.
RdaRtNumInActiveClients	The real-time number of inactive client.
RdaRtNumOutstandingOfferTasks	The real-time number of outstanding offer tasks that has processed.
Class: Expert Advisor BRE Table	
BreAggLoadedScripts	The total number of scripts loaded by the BRE.
BreAggDistinctScripts	The total number of distinct scripts loaded by the BRE (not including different versions of the same script).
BreRtActiveScripts	The number of loaded BRE scripts that are active.
BreRtCurrentInstances	The current number of script instances existing at this moment in time.
BreAggMaxConcurrentInstances	The maximum number of script instances that existed since boot time.
BreIntMaxConcurrentInstances	The maximum number of script instances that existed over the last interval.
BreAggAvgConcurrentInstances	The average number of instances being worked on by the BRE since boot time.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
BreIntAvgConcurrentInstances	The average number of instances being worked on by the BRE over the last interval.
BreAggTotalInstanceInitiations	The total number of script instances created since boot time.
BreIntTotalInstanceInitiations	The total number of script instances created over the last interval.
BreAggTotalContactInstanceInitiations	The total number of contact script instances created since boot time.
BreIntTotalContactInstanceInitiations	The total number of contact script instances created over the last interval.
BreAggTotalResourceInstanceInitiations	The total number of resource script instances created since boot time.
BreIntTotalResourceInstanceInitiations	The total number of resource script instances created over the last interval.
BreAggTotalInstanceTerminations	The total number of script instances terminated since boot time.
BreIntTotalInstanceTerminations	The total number of script instances terminated over the last interval.
BreAggTotalContactInstanceTerminations	The total number of contact script instances terminated since boot time.
BreIntTotalContactInstanceTerminations	The total number of contact script instances terminated over the last interval.
BreAggTotalResourceInstanceTerminations	The total number of resource script instances terminated since boot time.
BreIntTotalResourceInstanceTerminations	The total number of resource script instances terminated over the last interval.
BreAggTotalAbnormalEndings	The total number of script instances that ended abnormally since boot time.
BreIntTotalAbnormalEndings	The total number of script instances that ended abnormally over the last interval.
BreAggTotalAbnormalContactEndings	The total number of contact script instances that ended abnormally since boot time.
BreIntTotalAbnormalContactEndings	The total number of contact script instances that ended abnormally over the last interval.
BreAggTotalAbnormalResourceEndings	The total number of resource script instances that ended abnormally since boot time.
BreIntTotalAbnormalResourceEndings	The total number of resource script instances that ended abnormally over the last interval.
Class: Expert Advisor Assigner Table	
WaAggResourceRequestReceived	Total number of Resource Request received since boot time.
WaAggResourceResponseSent	Total number of Resource Response sent since boot time.
WaAggOfferTaskAcceptedSent	Total number of OfferTaskAccepted sent since boot time.
WaAggOfferTaskCancelledSent	Total number of OfferTaskCancelled sent since boot time.
WaAggOfferTaskResponseReceived	Total number of OfferTaskResponse received since boot time.
WaAggOfferTaskSent	Total number of OfferTask Sent since boot time.
WaAggWorkRequestReceived	Total number of WorkRequestReceived since boot time.
WaAggWorkRequestCanceledSent	Total number of WorkRequestCanceled messages sent since boot time.
WaAggMessageSentError	Total number of times messages could not be sent since boot time.
WaRtTotalResourceCount	Total number of known resources.
WaRtTotalContactCount	Total number of known contacts.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
WaRtTotalResourceManagerCount	Total number of known resource manager subsystems.
WaRtTotalContactManagerCount	Total number of known contact manager subsystems.
Class: Expert Advisor MPA Table	
MpaAggNewCalls	Counter showing number of New Calls requests received by Cisco Unified Expert Advisor.
MpaAggConnectsRcv	Counter showing number of connect attempts made by Cisco Unified Expert Advisor.
MpaAggAvgLatency	Average time in milliseconds required to complete a connection made by Cisco Unified Expert Advisor.
MpaAggFailedInvites	Number of failed invitation attempts made by Cisco Unified Expert Advisor.
MpaAggFailedReinvites	Number of failed re-invitation attempts made by Cisco Unified Expert Advisor.
MpaAggTotalCalls	Current number of calls into and originating from Cisco Unified Expert Advisor.
MpaRtIncomingCalls	Current number of calls into Cisco Unified Expert Advisor.
MpaRtOutgoingCalls	Current number of calls originating from Cisco Unified Expert Advisor
MpaRtActiveClientSessions	Number of currently registered Client Sessions.
MpaAggTotalClientsRegistered	Number of client sessions opened (Including disconnected clients).
MpaAggInstantMessagesSent	Number of instant messages sent.
MpaAggInstantMessagesReceived	Number of instant messages received.
MpaAggPresenceUpdatesReceived	Number of presence documents received.
MpaAggPresenceUpdatesBytesRcv	Total number of bytes received in presence updates.
MpaRtActiveRegisteredSipAddresses	Number of SIP current registrations to SIP Registrar.
MpaRtActiveSipControlAddresses	Number of SIP addresses currently registered with Stack.
MpaRtActiveIMAddresses	Number of IM addresses currently registered with Stack.
MpaRtActiveMonitoredPresenceAddresses	Number of Presentities currently registered with presence server.
MpaRtActiveInteractions	Number of Interactions that currently exist.
MpaRtActivePublishAddresses	Number of Publishers currently registered with presence server.
MpaRtTotalPublishAddressesRegistered	Number of Publishers registered with presence server (including deregistered ones).
MpaAggTotalRegisteredSipAddresses	The number of SIP registrations to SIP registrar (including deregistered ones) since boot time.
MpaAggTotalSipControlAddressesRegistered	The number of SIP addresses registered with stack (including deregistered ones) since boot time.
MpaAggTotalIMAddressesRegistered	The number of IM addresses registered with stack (including deregistered ones) since boot time.
MpaAggTotalMonitoredPresenceAddressesRegistered	The number of presence entities (for example, CUP server users) registered with presence server (including deregistered ones) since boot time.
Class: Expert Advisor Reporting Adapter Table	

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
RaAggMsgReceived	Total number of messages received.
RaAggMsgSent	Total number of messages dispatched.
RaAggContactDetailMesgDispatched	Total number of contact detail messages received.
RaAggContactDetailMesgReceived	Total number of contact detail messages dispatched.
RaAggContactDetailAttribMsgDispatched	Total number of contact detail attributes messages dispatched.
RaAggContactSegDetailMsgReceived	Total number of contact segment detail messages received.
RaAggContactSegDetailMesgDispatched	Total number of contact segment detail messages dispatched.
RaAggContactSegMediaDetailMsgDispatched	Total number of contact segment media detail messages dispatched.
RaAggResourceTaskDetailMsgReceived	Total number of resource task detail messages received.
RaAggResourceTaskDetailMsgDispatched	Total number of resource task detail messages dispatched.
RaAggTaskStateChangeMsgReceived	Total number of task state change messages received.
RaAggResourceStateChngMesgReceived	Total number of resource state change messages received.
RaAggResourceStateChngMsgDispatched	Total number of version response messages received.
RaAggVersionResponseRecieved	Total number of version request messages dispatched.
RaAggVersionRequestDispatched	Total number of version request messages dispatched.
RaAggNodeSyncDispatched	Total number of node synchronization messages dispatched.
Class: Expert Advisor Reporting Subsystem Table	
RsAggTotalContactDetailRecords	Total number of Contact Detail Records written to the database since the Reporting Server Subsystem started. For each ContactDetail Record written this metric will be incremental by one.
RsAggTotalContactDetailAttributeRecords	Total number of ContactDetailAttribute Records written to the database since the Reporting Server Subsystem started. For each ContactDetailAttribute record written this metric will be incremental by one.
RsAggTotalContactSegmentDetailRecords	Total number of Contact Segment Detail Records written to the database since the Reporting Server Subsystem started. For each ContactSegmentDetail Record written this metric will be incremented by one.
RsAggTotalResourceTaskDetailRecords	Total number of ResourceTaskDetail Records written to the database since the Reporting Server Subsystem started. For each ResourceTaskDetail Record written this metric will be incremented by one.
RsAggTotalResourceEventDetailRecords	Total number of ResourceEventDetail Records written to the database since the Reporting Server Subsystem started. For each ResourceEventDetail Record written this metric will be incremented by one.
RsAggTotalContactSegmentMediaDetailRecords	Total number of Contact Segment Media Detail Records written to the database since the Reporting Server Subsystem started. For each ContactSegment media Detail Record written this metric will be incremented by one.
RsAggTotalDBWrites	Total number of writes to the database by the Reporting Server since startup. For each write to the database by the Reporting Server, this metric will be increased by one.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
RsIntContactDetailRecords	Total number of ContactDetailRecords written to the database by the Reporting Server during the last interval. For each ContactDetail Record written, this metric will be incremented by one.
RsIntContactDetailAttribRecords	Total number of ContactDetailAttribute Records written to the database by the Reporting Server during the last interval. For each ContactDetailAttribute Record written, this metric will be incremented by one.
RsIntContactSegmentDetailRecords	Total number of ContactSegmentDetail Records written to the database by the Reporting Server during the last interval. For each ContactSegmentDetail Record written, this metric will be incremented by one.
RsIntResourceTaskDetailRecords	Total number of ResourceTaskDetail Records written to the database by the Reporting Server during the last interval. For each ResourceTaskDetail Record written, this metric will be incremented by one.
RsIntResourceEventDetailRecords	Total number of ResourceEventDetail Records written to the database by the Reporting Server during the last interval. For each ResourceEventDetail Record written, this metric will be incremented by one.
RsIntContactSegmentMediaDetailRecords	Total number of Contact Segment Media Detail Records written to the database by the Reporting Server during the last interval. For each Contact Segment media detail Record written, this metric will be incremented by one.
RsIntDBWrites	IntervalDBWrites is an interval metric indicating the total number of writes to the database made by the Reporting Server during the last interval. For each write to the database by the Reporting Server, this metric is increased by one.
RsRtNumberActiveDBUsers	Current number of active Reporting Database User sessions.
RsDBSizeAllocated	Allocated size (bytes) of the Reporting Server Database.
RsRtDBSpaceUsed	Number of bytes of Used DB.
RsRtDBSpaceFree	Number of bytes of Free DB space.
RsRtDBPercentUsed	Percentage of Used DB space.
RsRtDBPercentFree	Percentage of Free DB space.
RsRtTransactionLogSize	Size in bytes of the TransactionLog.
Class: Expert Advisor ICMGW (ICM Gateway) Table	
IcmgwAggSocketConnects	Number of socket connections since boot time.
IcmgwAggSocketDisconnects	Number of socket disconnections since boot time.
IcmgwAggACMIBytesSent	Number of bytes sent to the PIM since boot time.
IcmgwAggACMIBytesRcvd	Number of bytes received from the PIM since boot time.
IcmgwAggACMIMsgsSent	Number of messages sent to the PIM since boot time.
IcmgwAggACMIMsgsRcvd	Number of messages received from the PIM since boot time.
IcmgwRtACMIOutQueueDepth	Current ACMI output queue depth.
IcmgwRtACMIOutQueueWait	Queuing time of the message in the ACMI output queue in milliseconds.

Table B-1 Class Objects (continued)

Counters	Counter Descriptions
IcmgwRtAgentsMonitored	Number of agents being monitored.
IcmgwRtAqsMonitored	Number of Assignment Queues being monitored.
IcmgwRtRoutesMonitored	Number of DNIS being monitored.
IcmgwRtPendingQueryAgentStateDlgs	Number of pending QueryAgentState dialogues.
IcmgwRtPendingGetContactDetailDlgs	Number of pending GetContactDetail dialogues.
IcmgwAggQueryAgentStateTimeouts	Number of QueryAgentState timeouts.
IcmgwAggGetContactDetailTimeouts	Number of GetContactDetail timeouts.
IcmgwRtQueryAgentStateDelay	QueryAgentState response delay (ms).
IcmgwRtGetContactDetailDelay	GetContactDetail response delay (ms).
IcmgwRtPendingCallTermEvents	Number of pending CallTerminationEvent messages.
Class: Expert Advisor System Condition Table	
SystemConditionId	An unique Id of the System Condition, assigned by Cisco Unified Expert Advisor, used to identify a specific System Condition.
SystemConditionSeverity	This counter is used to specify the severity of a specific System Condition raised by the Cisco Unified Expert Advisor application or services in it. The Cisco Unified Expert Advisor application can run with certain conditions raised. The values are: • conditionWarn (1): This severity level indicates a warning that something is not right, however Cisco Unified Expert Advisor is still functioning, but the condition may be indicative of problem that may become more serious later. • ConditionCritical(2): This severity indicates a condition where the system is not functioning properly. • terminated(0):The Cisco Unified Expert Advisor application is terminated and RTMT is not able to contact the system to obtain the system Condition severity.

GLOSSARY

The *Glossary for the Cisco Unified Expert Advisor* document is specific to the Cisco Unified Expert Advisor documentation set and explains the commonly-used terms in the context of this product.

Note This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL: http://www.cisco.com/go/ea

A

ACD

Automatic Call Distributor. A feature that automatically routes incoming calls to an agent or attendant in accordance with a set of configurable rules such as longest idle agent.

ACL

Access Control List. In the incoming ACL, you can configure patterns that control which hosts and domains can access Cisco Unified Presence.

Active Directory

Active Directory. For expert(s) to be able to search the directory for other users, add users to their contact lists, and place calls to other users from Cisco Unified Personal Communicator, you must configure an LDAP server, or Active Directory server that supports LDAP. The Active Directory implementation is also used to authenticate Cisco Unified Expert Advisor administrators.

active server

The active server makes global decisions for the cluster and keeps track of calls, expert states, and historical detail records. The active server provides all system services and resources. Only one server in the cluster can be the active server at any given time. Which server is active is determined by which of the two servers has an active connection to the Unified Gateway. If the active server fails, the system automatically fails over to the standby server. Both servers are synchronized when administrative changes are made on the active server.

administrator

During the Cisco Unified Expert Advisor installation, you specify two administrator accounts (user name/password):

- The super user (or application administrator): can access the serviceability web pages and perform daily management functions (such as adding and maintaining assignment queues, agents, skill groups, message sets, and attributes).
- The platform administrator: can access OS administration and DRS web pages, as well as the CLI. You can create additional platform administrators from the CLI.

See the *Installation Guide for Cisco Unified Expert Advisor* for more information.

agent

An agent generally refers to the formal contact center agent who initially handled an incoming customer call and transfers it to the expert(s).

In the reporting context, an agent interchangeably refers to the expert(s).

alarm

Signals that declare the run-time status and state of the Cisco Unified Expert Advisor system and provide information for troubleshooting. Alarms can be forwarded to a syslog server, to an SNMP agent, or to a log file for an event.

alarm catalog

A file that contains alarms definitions.

alarm definition

A list of alarms and their properties. The definition for each alarm includes the alarm name, a description, an explanation, recommended actions, and related information.

alarm message

An alarm name followed by the reason for the alarm or the module name.

alarm service

A service that receives alarms from the Cisco Unified Expert Advisor and its subsystems.

AMC

Alert Manager and Collector (AMC). The Cisco AMC service logs the server data in CSV format. The header of the log comprises the time zone information and a set of columns with the previous counters for a Cisco Unified Expert Advisor node. These sets of columns repeat for every node.

The ServerDown alert is generated when the currently "active" AMC (primary AMC or the backup AMC, when the primary is not available) cannot reach another node in a cluster. This alert identifies network connectivity issues in addition to a ServerDown condition.

application

In general, an application is a program that helps you accomplish a specific task; for example, a word processing program, a spreadsheet program, or an FTP client. On a Cisco Unified Expert Advisor runtime or reporting server, the Cisco Unified Expert Advisor application runs on the Cisco Unified Operating System.

In Cisco Unified Expert Advisor, application is an internal object that is created every time an assignment queue is created. The name of each application is autogenerated and is prepended with APP_. A separate instance of each application is created for each assignment queue, as the script values may differ.

application user

During the installation, an application user is created on the Application User Configuration screen. The installation passes the user name and password for this application user to the User Management screen in the Cisco Unified Expert Advisor operations console. This user becomes the default Cisco Unified Expert Advisor super user.

assignment queue

Assignment queues handle the assignment of contacts to resources. Assignment queues are used to match expert(s) with incoming contact requests. Assignment queues have a one-to-one relationship with skill groups. When an assignment queue is created on the Cisco Unified Expert Advisor system, a skill group is also created and tied to the assignment queue.

A skill group is the Unified ICM concept (and object) that corresponds to an assignment queue in Cisco Unified Expert Advisor.

attributes

Attributes are customizeable variables associated with expert(s) and contacts. You can create resource attributes and associate them with expert(s), then use those attributes to match expert(s) with assignment queues. You can also map contact attributes from Unified ICM ECC variables, Unified ICM call variables, or SIP header variables to attributes in Cisco Unified Expert Advisor.

auto-configuration

Auto-configuration occurs when certain data are pulled from the EADB and uploaded to the Unified ICM database. This is a function of the Unified Gateway, which also tracks configuration changes on the Cisco Unified Expert Advisor and uploads those changes to keep the databases synchronized.

Automatic Call Distribution

See ACD.

Automatic failover

If the active server fails, the Cisco Unified Expert Advisor application provides automatic failover to the standby server. After a failover the high availability runtime server becomes the active server, and the primary (when it comes up again) becomes the standby server. Both servers are synchronized when administrative changes are made on the active server. The system uses database replication to copy the data automatically from the active server to the standby server.

B

broadcast notice

A broadcast notice is a request sent to one or more expert(s) (based on the configuration in the assignment queue). When a broadcast notice is sent, the system sends the call to the first expert who accepts the request. The system then sends a *Task Cancelled* message to all other broadcast experts. No action is required by the expert(s) receiving a task cancellation message.

BRE

Business Rules Engine. The application object (assignment queue) maps the incoming address to a BRE script to be executed.

C

CA

Certificate Authority (CA). You can import the server authentication certificate that the CA provides for each server in the cluster. Cisco recommends that you import the certificates before using the Trace & Log Central option. You cannot change any data that displays for the certificate.

call control

The Cisco Unified Expert Advisor system uses SIP for call control. A call control feature refers to any new call, transferred call, or call that is placed on hold.

category

Categories allow you to organize objects in RTMT, such as performance monitoring counters and devices. For example, the default category under performance monitoring, RTMT allows you to monitor six performance monitoring counters in graph format. If you want to monitor more counters, you can configure a new category and display the data in table format.

CDP

Cisco Discovery Protocol (CDP). Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP runs on all media that support SNMP, including LANs, Frame Relay, and ATM media.

Cisco Security Agent

Cisco Security Agent (CSA). This application detects and prevents security intrusion. It integrates with various Cisco products to provide a collaborative network and endpoint solution.

Cisco Unified Expert Advisor

Cisco Unified Expert Advisor is a product option within a unified contact center. It extends the contact center by allowing an "expert(s)" to handle certain incoming contacts. For example, there might be a situation where the contact center customer requires a discussion or advice from a specialist or expert(s). This expert is not a member of the formal contact center but agrees to be "on call" to provide consultation services.

Cisco Unified Expert Advisor Database

See EADB.

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise (Unified CCE), an integral component of the Cisco Unified Communications system, delivers a comprehensive solution that provides intelligent routing and call treatment with blending of multiple communication channels. It handles traditional ACD calls and functions as a virtual ACD. Capabilities of Unified CCE include intelligent multichannel contact routing, ACD functionality, network-to-desktop CTI, IVR integration, call queuing, and consolidated reporting.

Cisco Unified Communications Manager

TheCisco Unified Communications Manager (Unified CM) software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco Unified Intelligent Contact Management

See Unified ICM

Cisco Unified Operating System

You can perform many common system administration functions through the Cisco Unified Operating System. The Cisco Unified Operating System administration console for the Cisco Unified Expert Advisor application allows you to configure and manage the Cisco Unified Operating System.

For more information, see the *Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor.*

CLI

Command Line Interface. The platform CLI provides a limited set of commands accessible from any of the server consoles or through a SSH session. These commands allow basic maintenance and failure recovery and also enable some system administration when the Cisco Unified Expert Advisor operations console online interface is unavailable. The Cisco Unified Expert Advisor operations console is enabled for login at the completion of the installation and is the primary interface for administering, configuring, and maintaining Cisco Unified Expert Advisor.

cluster

A Cisco Unified Expert Advisor cluster deployment consists of two required (primary and high availability) servers and one optional (reporting) server running Cisco Unified Expert Advisor. The first server you install is always the primary, or publisher, and all additional servers in the same cluster are considered subscribers.

components

Core components of the Cisco Unified Expert Advisor system include:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Presence Server
- Cisco Unified Contact Center Enterprise
- Cisco Unified Customer Voice Portal
- Microsoft Active Directory Server (Active Directory)
- Optional LDAP Server (LDAP)
- IM client
  - Cisco Unified Personal Communicator
  - IP Phone Messenger (IPPM)
  - Microsoft Office Communicator (MOC)

contacts

A person needing help from a resource.

contact manager subsystem

The component (subsystem) responsible for handling contacts. This subsystem orchestrates the interaction of a contact from the time the contact begins interacting with Cisco Unified Expert Advisor until the interaction has completed.

CSA

See Cisco Security Agent.

CSV

Comma-Separated Values (CSV).

D

DHCP
Dynamic Host Configuration Protocol (DHCP). The IP Settings window indicates whether DHCP is active and provides the related Ethernet IP addresses, as well as the IP address for the network gateway.

DNS

Domain Name System (DNS) is an internet directory service which translates domain names into IP addresses. The DNS service is defined during the Cisco Unified Expert Advisor installation.

drawer

The left panel of the Cisco Unified Expert Advisor operations console uses the visual concept of a drawer as a container for related system functions. Similar to a menu, a drawer allows access to one or more utilities that have similar purposes or similar user permissions.

DRF

Disaster Recovery Framework (DRF) which provides the customer interface for the disaster recovery process. DRF itself, does not backup or restore any data—it merely provides a user interface and set of tools/utilities to perform different disaster recovery tasks

DRS

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Expert Advisor operations console, provides full data backup and restore capabilities for all servers in the cluster. The DRS allows you to perform regularly scheduled, automatic or user-invoked data backups.

The DRS performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Expert Advisor cluster to a central location and archives the backup data to physical storage device.

E

EADB

Cisco Unified Expert Advisor database (EADB), which stores configuration information for the entire system. This database is installed on all servers in the Cisco Unified Expert Advisor cluster.

ECC

Extended Call Contact (ECC). ECC variables are specific to Unified ICM. The Contact Attribute Sources page in the Cisco Unified Expert Advisor operations console allows you to map external call variables, such as Unified ICM ECC variables, to the Cisco Unified Expert Advisor system attributes.

event

An occurrence that is significant to an application and that may call for a response from the application.

Excel (XLS) format

Format of data in the Microsoft Excel spreadsheet application.

expert(s)

Cisco Unified Expert Advisor is an optional feature for Cisco Unified Contact Center. It extends the contact center to allow an *expert advisor* to handle certain incoming calls. An expert advisor is a specialist who is not employed by the contact center—but who agrees to be 'on call' to provide services as a consultant.

Experts establish their presence and availability to take a contact by the state of their IM client.

F

firewall

A firewall is a set of related programs that protect the resources of a network by examining (screening) each network packet to determine whether to forward it toward its destination. For Cisco Unified Expert Advisor, only ports and protocols that are specifically named will be allowed by the firewall.

fault tolerance

Fault tolerance differs based on the server in question:

- **active server failure:** When a failure condition is encountered, whether in a subsystem of the active server, in the Unified Gateway, or in the communication path between servers, the standby server assumes control. This should result in little or no disruption to the call center expert advisor operation.
- **standby server failure:** There is no effect on call center operations, except that the standby server will not be able to take control if the active server has also failed.
- **reporting server failure:** When the reporting server fails, you will not be able to run Historical reports. Like the runtime server, the reporting server is also integrated in the DRF for backup and restore functions.

field

A field is an item in a database record and is also referred to as a database field. For example, name, city, or zip code. A group of fields make up a record.

H

high availability

With high availability, if an active server becomes unavailable, the standby server immediately and automatically becomes the active server. Both runtime servers must be in the same location as the corresponding Unified Gateway on a connected LAN.

high availability runtime server

The high availability server (also referred to as a runtime server or standby server or secondary server) is one of the servers installed in the cluster.

HRDB

Historical database (HRDB), which stores data used in the historical reporting templates as well as system tables for the reporting server. This database is installed on the reporting server only.

I

IM

Instant Messaging (IM) is used to notify expert(s) about an incoming task request. The expert(s) respond to the IM by accepting or rejecting the request (if configured with the required permissions); the expert can also provide an alternate phone number at which to be called.

IM client

The IM client effectively serves as the "desktop" for expert(s), who establish their willingness to take a contact by responding to an IM contact request from the Cisco Unified Expert Advisor system.

Informix

Informix is a relational database management system used by the CUEA databases.

L

LDAP

Lightweight Directory Access Protocol. An application protocol for querying and modifying directory services running over TCP/IP.

For expert(s) to be able to search the directory for other users, add users to their contact lists, and place calls to other users from Cisco Unified Personal Communicator, you must configure an LDAP server, or Active Directory server that supports LDAP.

license

The Cisco Unified Expert Advisor includes five free seats. These five seats are referred to as the default license. When completing the initial configuration, you can optionally upload the license that you additionally purchase. If you do not upload any additional purchased license, the five free seats are used by default.

localization

Localization is the process of adapting a product or service to a particular language and culture. This includes idiomatic language translation and details as time zones and currency. Cisco Unified Expert Advisor has been localized for more than a dozen languages.

log file

A file that keeps track of the activity of a computer or an application.

LPM

Log Partition Monitor (LPM). The LPM monitors the current log file partition disk usage and purges files when the log partition high water mark is exceeded.

local agent

The server has a local agent to perform backup and restore functions. Each server in a Cisco Unified Expert Advisor cluster, including the server that contains the master agent, must have its own local agent to perform backup and restore functions for its server. By default, a local agent automatically gets activated on each server in the cluster. The local agent runs backup and restore scripts on each server in the cluster.

M

master agent

The master agent stores backup data on a locally attached tape drive or a remote network location. The master agent maintains a complete set of scheduled tasks in the database. When it receives updates from the user interface, the master agent sends executable tasks to the applicable local agents, as scheduled (local agents execute immediate-backup tasks without delay). You access the master agent through the DRS user interface to perform activities such as configuring storage locations, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.

message set

A group of messages by language and client format type. Messages from message sets are sent to and/or received from expert(s).

MIB

Management Information Base (MIB). Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MOC

Microsoft Office Communicator (MOC). Microsoft's instant messaging and presence client. It can be used with Unified Expert Advisor as an IM client. Unified Expert Advisor supports either Cisco Unified Personal Communicator clients or MOC clients, but not both in the same installation.

MTU

Maximum Transmission Unit (MTU). All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The MTU on Eth0 defaults to 1500.

N

NAT

Network Access Translation (NAT). To use the Trace & Log Central feature in the RTMT, make sure that RTMT can access the server directly without NAT. If you have set up a NAT to access devices, configure the Cisco Unified Expert Advisor with a host name 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.

NIC

Network Interface Card (NIC). Each server in the cluster is required to have a NIC. The NIC is configured during installation for two connection settings: speed and duplex.

node

See server.

The term node and server are used interchangeably in this document and refer to a computer that provides services or resources to other computers (called clients) connected to it through a network.

NTP

Network Time Protocol (NTP). You can only configure the NTP server settings on the first Cisco Unified Expert Advisor publisher. After deleting, modifying, or adding a NTP server, you must restart all the other nodes in the cluster for the changes to take affect.

O

OAMP tasks

Operations, Administration, Maintenance, and Provisioning tasks

OCS

Microsoft Office Communication Server (OCS).

operations console

The web-based user interface that runs on the primary runtime server and allows you to perform OAMP tasks on multiple servers in a Cisco Unified Expert Advisor cluster.

P

pane

A part of a window that is devoted to a specific function.

partition

Cisco Unified Expert Advisor software creates three partitions during each installation: an active bootable partition, an inactive bootable partition, and a common partition. A fresh (first-time) installation places the new Cisco Unified Expert Advisor software and operating system on the active partition. The system boots up and operates on the active partition.

PG

Peripheral Gateways (PG). The Unified ICM central controller communicates with each peripheral through a monitoring node referred to as the PG. Unified ICM software has a unique PG for each device it supports. Unified ICM treats Cisco Unified Expert Advisor as a peripheral. The primary runtime server and the high availability runtime server each connect with Unified CM with a dedicated Unified Gateway.

ports

In a communications network, a logical channel is identified by its unique port number.

post-routing

Process of making a routing decision after a call reaches a termination point.

pre-routing

Process of making a routing decision before a call reaches a termination point.

primary runtime server

The primary server (also referred to as a runtime server or a publisher or active server) in the Cisco Unified Expert Advisor cluster. This is the first runtime server installed in a cluster.

After a failover the high availability runtime server becomes the active server, and the primary (when it comes up again) becomes the standby server.

prompts

A message from a computer that asks the operator to do something, such as enter a command, enter a password, or enter data, or that indicates that the computer is ready to accept input.

publisher

The primary runtime server is also referred to as a publisher as it *publishes* (replicates) the OAMP configuration data in the Cisco Unified Expert Advisor cluster.

In Cisco Unified Expert Advisor, the terms publisher and subscriber are used in the context of database replication. The Cisco Unified Expert Advisor publisher (primary runtime server) publishes OAMP configuration data. The Cisco Unified Expert Advisor subscribers (high availability and reporting servers) subscribe to the data.

purge

To delete both a set of data and all references to the data.

R

Real-Time Monitoring Tool

See RTMT.

record

In a database, a group of fields that make up one complete entry is called a record (or database record). For example, a record about a customer might contain fields for name, address, and telephone number.

reporting adapter

The reporting adapter is the software subsystem in each runtime server which forwards reporting events to the reporting server.

reporting server

The reporting server is added as a subsequent server in a Cisco Unified Expert Advisor cluster (also referred to as subscribers). The reporting server, also referred to as the historical reporting server, is an optional server.

reporting user

Cisco Unified Expert Advisor reporting users are created in the Cisco Unified Expert Advisor operations console after the installation. They have read-only access to the Reporting database and can generate reports using the Cisco predefined templates.

See also super user and administrator.

resource

A person or automaton (for example, a self-service prompt/response) that can provide help to a Contact.

RISDC

Real-time Information Server Data Collection (RISDC). Cisco Unified Expert Advisor collects system performance information that is written on the Cisco Unified Expert Advisor server. You can use this performance data to troubleshoot problems. By default, RISDC perfmon logging gets enabled. Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging.

RTMT

The Real-Time Monitoring Tool (RTMT) for Cisco Unified Expert Advisor, which runs as a client-side application, uses HTTPS and TCP to monitor system performance and device status for Cisco Unified Expert Advisor. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

runtime server

The primary runtime server is also referred to as a runtime server or a publisher or active server. This is the first runtime server installed in a cluster. If the primary runtime server fails, you cannot configure the system.

S

scheduler

A program that resides on a Cisco Unified Expert Advisor reporting server. The Scheduler maintains information about each scheduled report, including when the report should execute and what information the report should contain. The scheduler also executes scheduled reports at their scheduled times, based on the time and date of the reporting server.

schedule backups

A Cisco Unified Expert Advisor administrator can schedule backups at predesignated times. DRS includes a comprehensive scheduling system which provides the ability to backup one time, daily, weekly, or monthly.

script

A sequence of steps constructed to control the flow of a call. Scripts are sometimes also called *flows*, *call flows*, or *work flows*.

server

See node.

A computer that belongs to a cluster. A server is also referred to as a node. The term node and server are used interchangeably in the Cisco Unified Expert Advisor documentation set.

service

A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

serviceability

Generally, *serviceability* refers to the collection tools and mechanisms by which a customer, partner, or technical assistance engineer can service the product. In a Cisco Unified Expert Advisor system, some of those tools are contained in the Serviceability drawer in the Cisco Unified Expert Advisor system's operations console, and some are in the Cisco Unified Serviceabilty for Cisco Unified Expert Advisor application. This application is available from the Navigation dropdown list in the upper right corner of the operations console.

session (historical reporting)

Historical reporting seats are also called historical reporting sessions. Historical reporting sessions (seats) refer to the number of historical reporting clients that can be started at the same time on different client machines.

SFTP server

Secure File Transfer Protocol (SFTP) server. You must have an SFTP server configured in order to back up data to a remote network device. You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

You may use any SFTP server:

- Open SSH (for Unix systems)
- Cygwin (refer to http://sshwindows.sourceforge.net/)
- freeFTPD (refer to http://www.freeftpd.com/?ctt=download)

SFTP network location

A SFTP network location to store backup is specified as a remote server. This server is not one of node in a Cisco Unified Expert Advisor cluster. The server must have sufficient disk space to hold one or more backups. This network storage server can be Windows or Linux based.

SIP

Session Initiation Protocol. A peer-to-peer, multimedia signaling protocol developed in the IETF. SIP is ASCII-based, resembling HTTP, and reuses existing IP protocols (DNS, SDP, etc.) to provide media setup and tear down.

You may need to create a SIP Trunk on Cisco Unified Communications Manager so that the Unified Presence server can communicate with Cisco Unified Communications Manager. Optionally, you may need to configure Unified CVP to use an outbound SIP proxy to send all SIP-based calls to the Cisco Unified Presence Server to take advantage of static routes.

skill group

When you create an assignment queue in the Cisco Unified Expert Advisor system, the system automatically creates a corresponding skill group in Unified ICM. A skill group automatically configured in Unified ICM is marked in Unified ICM as “used by peripheral”. Such items cannot be edited using the Unified ICM configuration tools. If you later delete that assignment queue, once the auto-configuration operation completes, Unified ICM removes the “used by peripheral” flag, but it does not delete the skill group. The skill group, along with any subordinate objects and references from other objects, remains intact and can only be deleted manually.

A skill group is the Unified ICM concept (and object) that corresponds to an assignment queue in Cisco Unified Expert Advisor.

SMTP

SimpleMail Transfer Protocol (SMTP). When you install Cisco Unified Expert Advisor, you can choose to configure an optional SMTP host for outbound e-mail. If you want the system to send you e-mail, you must configure an SMTP host. The SMTP Settings window in the Cisco Unified Operating System administration console allows you to view or set the SMTP host name and indicates whether the SMTP host is active.

SNMP

Simple Network Management Protocol (SNMP). The standard protocol for network management software. Using SNMP, programs called SNMP agents monitor devices on the network. The database created by the monitoring operations is called a MIB.

SNMP agent

Hardware or software that monitors devices on a network. Data from an SNMP agent, which is contained in a MIB, helps in network management and troubleshooting.

SNMP service

An operating system service that provides a framework for SNMP and provides the SNMP agent that interfaces with SNMP subagents.

SNMP subagent

Cisco provides SNMP subagents to support each MIB. The SNMP service loads the SSNMP subagent and it exchanges SNMP messages with the SNMP subagent. The SNMP service formats information as MIBs and sends this information to a Network Management System (NMS). It also sends traps from the SNMP subagent to the appropriate SNMP trap receivers.

standby server

You must deploy at least two servers in each Cisco Unified Expert Advisor cluster for high availability: one active server (master) and one standby (not active) server. The non-active server will be in PARTIAL-SERVICE.

subscriber

Subsequent servers in the Cisco Unified Expert Advisor cluster are referred to as subscribers. These servers include the secondary runtime server and the reporting server.

In Cisco Unified Expert Advisor, the terms publisher and subscriber are used in the context of database replication. The Cisco Unified Expert Advisor publisher (primary server) publishes OAMP configuration data. The Cisco Unified Expert Advisor subscribers (high availability and reporting servers) subscribe to the data.

subsystem

A subsystem is an extensible modular development environment that performs a particular function. In the context of Cisco Unified Expert Advisor, each subsystem has a specific set of responsibilities which when joined together create Cisco Unified Expert Advisor functionalities such as Resource Manager, Contact Manager and Work Assigner.

super user

The application user defined in the installation wizard becomes the default Cisco Unified Expert Advisor super user. The super user has access to all Daily Management and system level features, such as installing upgrades. The default super user can create additional users from the Cisco Unified Expert Advisor operations console. These additional users include additional super users, other administrators (who have no access to system-level functions), and reporting users.

See the *Installation Guide for Cisco Unified Expert Advisor* for more information.

See also administrator.

syslog

A Cisco standard that allows for logging of errors across an enterprise. Provides local logging of network events to files. Also provides remote logging to various systems via standard protocols.

system

The Cisco Unified Expert Advisor system is referred to as *system*.

T

table (also database table)

A presentation of information organized in rows and columns.

tape device

A tape device is a USB-based external device such as a Digital Linear Tape (DLT) backup solution.

TFTP

Trivial File Transfer Protocol. A simple file transfer protocol used to transfer small files between hosts on a network.

trace route

A TCP/IP utility that allows you to determine the route packets are taking to a particular host. Trace route works by increasing the “time to live” value of packets and seeing how far they get, until they reach the given destination.

Trace & Log Central

Trace and Log Central is part of the RTMT for the Cisco Unified Expert Advisor. It is used to manage and collect trace and log files from the Cisco Unified Expert Advisor servers.

translation routing

Translation routing is a process that ensures that the association between a call and its related data is maintained throughout the life of the call.

trap (also SNMP trap)

A program interrupt, usually caused by some exceptional situation in an application. In most cases, after such an interrupt, the operating system performs some action, then returns control to the application.

U

Unified Gateway

The Unified Gateway is a PG which you configure on the Unified ICM software. The Unified Gateway provides for the integration of the Unified ICM system with Cisco Unified Expert Advisor.

Unified ICM

Cisco Unified Intelligent Contact Management. The Unified Contact Center component that is responsible for making routing decisions and performing ACD functions.

USB drive

Universal Serial Bus (USB) drive is a data storage device integrated with a USB connector. Cisco Unified Expert Advisor supports the use of a USB drive for downloading and storing configuration data.

V

variable

A placeholder for data.

W

wizard

A wizard is a computer utility designed to lead you through the execution of tasks. Cisco Unified Expert Advisor uses wizards for installation and for initial configuration.

X

XML

Extensible Markup Language. A programming language developed by the World Wide Web Consortium (W3C) that allows Web developers to create customized tags that will organize and deliver efficiently. XML is a metalanguage, containing a set of rules for constructing other markup languages.