Cisco Unified Serviceability 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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor
Copyright © 2009 Cisco Systems, Inc. All rights reserved.

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 *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor* provides descriptions and procedures for configuring alarms, traces, SNMP, and so on, through Cisco Unified Serveciability. Use this guide in conjunction with the following documents:

- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*—This document describes how to use RTMT, a tool that allows you to monitor many aspects of the system (critical services, alerts, performance counters, and so on).
- *Administration and Configuration Guide for Cisco Unified Expert Advisor*—This document describes how to use the Cisco Unified Expert Advisor Option to configure serviceability features specific to expert advisors.

Audience

The *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor* assists administrators that configure, troubleshoot, and support Cisco Unified Expert Advisor. 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 Serviceability"	Provides an overview of Cisco Unified Serveciability including browser support and information on how to access and use the GUI.
Chapter 2, "Using Cisco Unified Serviceability"	Provides procedures to access Cisco Unified Serveciability and elaborates on the features and benefits of using this program.
Chapter 3, "Understanding Alarms"	Provides an overview of Cisco Unified Serveciability alarms and alarm definitions.
Chapter 4, "Configuring Alarms"	Provides procedures for configuring alarms in Cisco Unified Serveciability.
Chapter 5, "Viewing and Updating Alarm Definitions"	Provides procedural information for searching and editing Cisco Unified Serveciability alarm definitions.
Chapter 6, "Understanding Trace"	Provides an overview of trace collection in Cisco Unified Expert Advisor RTMT.
Chapter 7, "Configuring Trace"	Provides procedures for configuring trace parameters for Cisco Unified Expert Advisor services.
Chapter 8, "Configuring Troubleshooting Trace Settings"	Provides procedures for configuring the troubleshooting trace settings for services in Cisco Unified Serveciability.
Chapter 9, "Understanding Services"	Provides a description of each network and feature service that displays in Cisco Unified Serveciability.
Chapter 10, "Understanding Serviceability Reports Archive"	Provides procedures and recommendations for activating, deactivating, starting, and stopping Cisco Unified Serveciability services.
Chapter 11, "Configuring Services"	Provides an overview of reports that are generated by the Cisco Serviceability Reporter service
Chapter 12, "Configuring Serviceability Reports Archive"	Provides procedures for viewing reports generated by the Serviceability Reporter service.
Chapter 13, "Understanding Simple Network Management Protocol"	Provides an overview of Cisco Unified Expert Advisor support of SNMP versions. Administrators use SNMP to troubleshoot and to perform diagnostics and network management tasks.
Chapter 14, "Configuring SNMP V1/V2c"	Provides procedures for configuring SNMP versions 1 and 2c.
Chapter 15, "Configuring SNMP V3"	Provides procedures for configuring SNMP version 3.
Chapter 16, "Configuring the MIB2 System Group"	Provides procedures for configuring the system contact and system location objects for the MIB-II system group.

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 Serviceability

This chapter contains information on the following topics:

Cisco Unified Serviceability Overview

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

- Saves alarms and events for troubleshooting and provides alarm message definitions.
- Saves trace information to various log files for troubleshooting.
- Monitors real-time behavior of components through the Cisco Unified Expert Advisor Real-Time Monitoring Tool (RTMT).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Cisco Unified Expert Advisor to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a node (or all nodes in the cluster).

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.

- Monitors the disk usage of the log partition on a server.
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.

Tip Cisco Unified Communications Manager Administration defaults are used in the Cisco RIS Data Collector (RISDC) for the Cisco Unified Expert Advisor. These values cannot be changed.

Reporting and Monitoring Tools

Cisco Unified Serviceability provides the following reporting tools:

- Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT)—Monitors real-time behavior of components through RTMT; creates daily reports that you can access through the Serviceability Reports Archive. For more information, refer to the *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*.
- Serviceability Reports Archive—Archives reports that the Cisco Unified Serveciability Reporter service generates.

Remote Serviceability Tools

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

Cisco Unified Expert Advisor supports the following capabilities for remote serviceability:

- Simple Network Management Protocol (SNMP)—Provides remote management for managed devices such as Cisco Unified Expert Advisor
- Show Command Line Interface—Displays Cisco Unified Expert Advisor system data.
- Cisco Unified Operations Manager supports the maintenance of Cisco networks and devices.

Browser Support

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

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

Cisco Unified Serviceability uses HTTPS to establish secure connections.

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

Where to Find More Information

For additional documentation, refer to the following URLs:

- Cisco Unified Expert Advisor:
  http://www.cisco.com/go/cc
- Cisco Unified Operations Manager:
  http://www.cisco.com/en/US/products/ps6535/tsd_products_support_general_information.html

CHAPTER 2

Using Cisco Unified Serviceability

This chapter comprises the following topics:

Accessing Cisco Unified Serviceability

Tip After you log in to Cisco Unified Serviceability, you can access all applications that display in the Navigation drop-down list box, except for the Cisco Unified Operating System or Disaster Recovery System (DRS), without having to log in to each application. You cannot access the Cisco Unified Operating System or DRS GUIs with the same username and password that you use to access Cisco Unified Serviceability. To access these applications from Cisco Unified Serviceability, you must click the **Logout** link in the upper, right corner of the Cisco Unified Serviceability window; then, choose the application from the Navigation drop-down list box, and click **Go**.

If you have already logged in to one of the applications that display in the Navigation drop-down list box (not Cisco Unified Operating System or DRS), you can access Cisco Unified Serviceability without logging in; from the Navigation drop-down list box, choose Cisco Unified Serviceability; then, click **Go**.

To access Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 By using a compatible browser, browse into the server where the Cisco Unified Serviceabilty for Cisco Unified Expert Advisor service runs.

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

Step 2 By using a compatible browser, browse into the node where the Cisco Unified Serviceability operations console runs.

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

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

Step 3 If the system prompts you about certificates, see the "Using HTTPS" section on page 2-2.

Step 4 Enter the username and the application user password that you specified during installation; click **Login**.

To clear the username and password before you log in, click **Reset**.

Tip Only super users can access Cisco Unified Serviceabilty for Cisco Unified Expert Advisor. For more information on user management, refer to the *Administration and Configuration Guide for Cisco Unified Expert Advisor*.

Additional Information

See the "Related Topics" section on page 2-6.

Using HTTPS

This section contains information on the following topics:

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

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

HTTPS Overview for Internet Explorer

The first time that you (or a user) access Cisco Unified Serviceability, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must perform one of the following tasks:

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

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

Additional Information

See the "Related Topics" section on page 2-6.

Using Internet Explorer to Save the Certificate to the Trusted Folder

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

Procedure

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

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

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

Step 4 Click **Next**.

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

Step 6 Browse to **Trusted Root Certification Authorities**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

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

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

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

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

Additional Information

See the "Related Topics" section on page 2-6.

Using Netscape to Save the Certificate to the Trusted Folder

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

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

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

Procedure

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

The certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

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

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

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

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Additional Information

See the "Related Topics" section on page 2-6.

Using the Cisco Unified Serviceability Interface

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

- To display documentation for a single window, choose **Help > This Page** in Cisco Unified Serviceability.
- To display a list of documents that are available with this release (or to access the online help index), choose **Help > Contents** in Cisco Unified Serviceability.
- To verify the version of Cisco Unified Serviceability that runs on the server, choose **Help > About** or click the **About** link in the upper, right corner of the window.
- To go directly to the home page in Cisco Unified Serviceability from a configuration window, choose **Cisco Unified Serviceability** from the Navigation drop-down list box in the upper, right corner of the window.
- To access other application GUIs, choose the appropriate application from the Navigation drop-down list box in the upper, right corner of the window; then, click **Go**.
- To log out of Cisco Unified Serviceability, click the **Logout** link in the upper, right corner of the Cisco Unified Serviceability window.
- In each Cisco Unified Serviceability configuration window, configuration icons display that correspond to the configuration buttons at the bottom of the window; for example, you can either click the Save icon or the Save button to complete the task.

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

Using Accessibility Features

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

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

Table 2-1 Navigation Shortcuts for Cisco Unified Serviceability

Keystroke	Action
Alt	Moves focus to the browser menu bar.
Enter	Chooses the item with focus (menu option, button, and so on.)
Alt, arrow keys	Moves between browser menus.
Alt+underlined letter	Takes you to the menu; for example, Alt+A moves you to the Alarms menu.
Spacebar	Toggles control; for example, checks and unchecks a check box.
Tab	Moves focus to the next item in the tab order or to next control group.

Table 2-1 Navigation Shortcuts for Cisco Unified Serviceability

Keystroke	Action
Shift+Tab	Moves focus to the previous item or group in the tab order.
Arrow keys	Moves among controls within a group.
Home	Moves to the top of the window if more than one screenful of information exists. Also, moves to the beginning of a line of user-entered text.
End	Moves to the end of a line of user-entered text. Moves to the bottom of the window if more than one screenful of information exists.
Page Up	Scrolls up one screen.
Page Down	Scrolls down one screen.

Where to Find More Information

For additional documentation, refer to the following URLs:

- Cisco Unified Expert Advisor:
  http://www.cisco.com/go/cc
- Cisco Unified Operations Manager:
  http://www.cisco.com/en/US/products/ps6535/tsd_products_support_general_information.html

Related Topics

- Accessing Cisco Unified Serviceability, page 2-1
- Using HTTPS, page 2-2
- Using the Cisco Unified Serviceability Interface, page 2-5
- Using Accessibility Features, page 2-5

CHAPTER 3

Understanding Alarms

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

Understanding Alarms

Cisco Unified Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting, even for problems that are not on your local Cisco Unified Expert Advisor. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog) or Syslog file (remote syslog). When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure. The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

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

You use the Trace & Log Central option in the Cisco Unified Expert Advisor RTMT to collect alarms. You use the SysLog Viewer in RTMT to view alarm information that gets sent to the local syslog.

Alarm Configuration

You can configure alarms for services, such as Cisco Database Layer Monitor, on a particular node, or you configure alarms for a particular service on all nodes in the cluster.

To configure an alarm for a service, you choose an alarm event level, such as Error, and the location(s), such as Syslog Viewer (local syslog), where you want the system to send the alarm information. Choosing an event level accomplishes the following tasks: helps you narrow the types of alarms that get collected and prevents the Syslog and trace files from becoming overloaded. For more information on how alarm configuration relates to the alarm definitions, see the "Alarm Definitions" section on page 3-2.

Alarm Definitions

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

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

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

- Sys Log—The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an appropriate event level in the Alarm Configuration window, and enter a server name or IP address for the remote syslog server.
- Event Log—The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Cisco Unified Expert Advisor RTMT, if you enable the alarm for this option and specify an appropriate event level in the Alarm Configuration window.
- Data Collector—System sends the alarm information to the real-time information system (RISDC) (for alert purposes only). You cannot configure this option in the Alarm Configuration window.
- SNMP Traps—System generates an SNMP trap. You cannot configure this option in the Alarm Configuration window.

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

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

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

Viewing Alarm Information

You view alarm information to determine whether problems exist. The method that you use to view the alarm information depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the trace log file by using the Trace & Log Central option in RTMT or by using a text editor. You can view alarm information that gets sent to local syslog by using the SysLog Viewer in RTMT.

Alarm Configuration Checklist

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

Table 3-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Choose the server and service for which you want the alarm information.	• Understanding Alarms, page 3-1 • Configuring an Alarm for a Service, page 4-1
Step 2	Choose the destination of the alarm. • All services can go to the SysLog Viewer. • To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name.	• Configuring an Alarm for a Service, page 4-1 • Alarm Configuration Settings, page 4-3
Step 3	Choose the alarm event level.	• Configuring an Alarm for a Service, page 4-1 • Alarm Configuration Settings, page 4-3
Step 4	If desired, add a definition to an alarm.	• Alarm Definitions, page 3-2 • Viewing and Updating Alarm Definitions, page 5-1
Step 5	If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in RTMT.	*Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*
Step 6	See the corresponding alarm definition for the description and recommended action.	Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1

Where to Find More Information

Related Topics

- Configuring an Alarm for a Service, page 4-1
- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1

- System Alarm Catalog Descriptions, page 5-2
- Related Topics, page 5-2
- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*

CHAPTER 4

Configuring Alarms

This chapter contains the following topics:

Configuring an Alarm for a Service

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

Procedure

Step 1 Choose **Alarm > Configuration**.

The Alarm Configuration window displays.

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

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

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

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

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

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

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

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

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

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

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

Additional Information

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

Service Groups in Alarm Configuration

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

Caution CTI and CDR Services are not supported in Cisco Unified Serviceabilty for Cisco Unified Expert Advisor.

Table 4-1 Service Groups in Alarm Configuration

Service Group	Services	Notes
CM Services	Cisco TFTP. **Caution** This service is not supported in Cisco Unified Serviceabilty for Cisco Unified Expert Advisor.	For a description of these services, see the "Understanding Services" section on page 9-1.
Database and Admin Services	Cisco Database Layer Monitor	For a description of these services, see the "Understanding Services" section on page 9-1.
Performance and Monitoring Services	Cisco AMC Service and Cisco RISDC	For a description of these services, see the "Understanding Services" section on page 9-1.
Directory Services	Cisco DirSync **Caution** Cisco DirSync service does not apply to Cisco Unified Expert Advisor.	For a description of this service, see the "Understanding Services" section on page 9-1.
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master	For a description of these services, see the "Understanding Services" section on page 9-1.

Table 4-1 Service Groups in Alarm Configuration (continued)

Service Group	Services	Notes
System Services	Cisco Trace Collection Service	For a description of these services, see the "Understanding Services" section on page 9-1.
Platform Services	Cisco Tomcat	For a description of this service, see the "Understanding Services" section on page 9-1.

Alarm Configuration Settings

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

Table 4-2 Alarm Configuration Settings

Name	Description
Server	From the drop-down box, choose the server for which you want to configure the alarm; then, click **Go**.
Service Group	From the drop-down box, choose the category of services, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.
Service	From the Service drop-down box, choose the service for which you want to configure the alarm; then, click **Go**. Only services that support the service group and your configuration display. **Tip** The drop-down list box displays active and inactive services.
Apply to All Nodes	To apply the alarm settings for the service to all nodes in a cluster, check the check box.

Table 4-2 Alarm Configuration Settings (continued)

Name	Description
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Expert Advisor RTMT. For information on viewing logs with the SysLog Viewer, refer to the *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*.
Alarm Event Level	From the drop-down list box, choose one of the following options: • **Emergency**—This level designates system as unusable. • **Alert**—This level indicates that immediate action is needed. • **Critical**—The system detects a critical condition. • **Error**—This level signifies an error condition exists. • **Warning**—This level indicates that a warning condition is detected. • **Notice**—This level designates a normal but significant condition. • **Informational**—This level designates information messages only. • **Debug**—This level designates detailed event information that Cisco TAC engineers use for debugging.

Related Topics

- Configuring an Alarm for a Service, page 4-1
- Service Groups in Alarm Configuration, page 4-2
- Alarm Configuration Settings, page 4-3
- Understanding Alarms, page 3-1
- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*

CHAPTER 5

Viewing and Updating Alarm Definitions

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

Viewing Alarm Definitions and Adding User-Defined Descriptions

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

Procedure

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

The Alarm Message Definitions window displays.

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

Step 3 From the Equals drop-down list box, choose a catalog of alarm definitions or enter the alarm name in the Enter Alarm Name field. For a list of System Alarm Catalog options, see Table 5-1.

Step 4 Click the **Find** button.

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

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

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

The Alarm Information window displays.

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

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

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

Additional Information

See the "Related Topics" section on page 5-2.

System Alarm Catalog Descriptions

Table 5-1 contains the System Alarm Catalog alarm descriptions.

Table 5-1 System Catalogs

Name	Description
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Expert Advisor RTMT alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters.
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services.
TFTPAlarmCatalog	All Cisco TFTP alarm definitions. **Note** The TFTPAlarmCatalog is part of the underlying Cisco Unified Communications Manager legacy platform and does not apply to Cisco Unified Expert Advisor.
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP traps from the Command Line Interface (CLI). For information on the CLI, refer to the *Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor*.

Additional Information

See the "Related Topics" section on page 5-2.

Related Topics

- Understanding Alarms, page 3-1
- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1
- System Alarm Catalog Descriptions, page 5-2

CHAPTER 6

Understanding Trace

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

Understanding Trace

Cisco Unified Serviceability provides trace tools to assist you in troubleshooting issues with serviceability applications within Cisco Unified Expert Advisor. Cisco Unified Serviceability supports SDI (System Diagnostic Interface) trace and Log4J trace (for Java applications).

Tip See the *Administration and Configuration Guide for Cisco Unified Expert Advisor* for more information on application tracing.

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

In the Alarm Configuration window, you can direct alarms to various locations, including SDI trace log files. If you want to do so, you can configure trace for alerts in the Cisco Unified Expert Advisor RTMT.

After you have configured information that you want to include in the trace files for the various services, you can collect and view all trace files (including application files) by using the Trace & Log Central option in the Cisco Unified Expert Advisor RTMT.

Trace Configuration

You can configure trace parameters for any feature or network service that is available on any Cisco Unified Expert Advisor node in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting problems.

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

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

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the Trace & Log Central option in RTMT. For more information regarding trace collection, see the "Trace Collection" section on page 6-2.

Troubleshooting Trace Setting

The Troubleshooting Trace Settings window allows you to choose the services in Cisco Unified Serviceability for which you want to set predetermined troubleshooting trace settings. In this window, you can choose the services on different Cisco Unified Expert Advisor nodes in the cluster, so the trace settings of the chosen services get changed to the predetermined trace settings. You can choose specific activated services for a single node, all activated services for the node, specific activated services for all nodes in the cluster, or all activated services for all nodes in the cluster. In the window, N/A displays next to inactive services.

Note The predetermined troubleshooting trace settings for a Cisco Unified Expert Advisor feature or network service include SDI, and Log4j trace settings. Before the troubleshooting trace settings get applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings get restored.

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

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for the given service(s). From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings; for example, maximum number of files. You can modify these parameters even after you apply troubleshooting trace settings

Trace Collection

Caution This feature is addressed by the application serviceability feature in the Cisco Unified Expert Advisor operations console. See the *Administration and Configuration Guide for Cisco Unified Expert Advisor* for more information.

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

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

Tip Do not use NotePad to view collected trace files.

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

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

Trace Configuration and Collection Checklist

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

Table 6-1 Trace Configuration and Collection Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Configure application-level tracing as applicable to your network.	*Administration and Configuration Guide for Cisco Unified Expert Advisor*
Step 2	Configure the trace setting for the service for which you want to collect traces. You can configure trace for the service on one server or on all servers in the cluster. To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields. You can also configure trace for specific devices if you are configuring trace for the Cisco Unified Expert Advisor service. If you want to run predetermined traces on services, set troubleshooting trace for those services.	• Understanding Trace, page 6-1 • Configuring Trace, page 7-1 • Configuring Troubleshooting Trace Settings, page 8-1
Step 3	Install the Cisco Unified Expert Advisor RTMT on a local PC.	*Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*
Step 4	If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in RTMT. You can find the LogFileSearchStringFound alarm in the LpmTctCatalog. (In Cisco Unified Serviceability, choose **Alarms > Definitions**. In the Find alarms where drop-down list box, choose the **System Alarm Catalog**; in the Equals drop-down list box, choose **LpmTctCatalog**).	• *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor* • Viewing Alarm Definitions and Adding User-Defined Descriptions, page 5-1

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

Configuration Steps		Related Procedures and Topics
Step 5	If you want to automatically capture traces for alerts such as CriticalServiceDown, check the **Enable Trace Download** check box in the Set Alert/Properties dialog box for the specific alert in RTMT; configure how often that you want the download to occur.	*Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*
Step 6	Collect the traces.	
Step 7	View the log file in the appropriate viewer.	
Step 8	If you enabled troubleshooting trace, reset the trace settings services, so the original settings get restored. **Note** Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.	Configuring Troubleshooting Trace Settings, page 8-1

Where to Find More Information

- Alarm Configuration Checklist, page 3-3
- Understanding Trace, page 6-1
- Configuring Troubleshooting Trace Settings, page 8-1
- *Administration and Configuration Guide for Cisco Unified Expert Advisor*
- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*

CHAPTER 7

Configuring Trace

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

This chapter contains the following topics:

Configuring Trace Parameters

Tip Cisco Unified Expert Advisor operations console defaults are used in the Cisco RISDC for Cisco Unified Expert Advisor. These values cannot be changed.

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

Procedure

Step 1 Choose **Trace > Configuration**.

The Trace Configuration window displays.

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

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

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

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

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

If you configured Troubleshooting Trace for the service, a message displays at the top of the window that indicates that the Troubleshooting Traces feature is set, which means that the system disables all fields in the Trace Configuration window except for Trace Output Settings. To configure the Trace Output Settings, go to Step 10. To reset Troubleshooting Trace, see the "Configuring Troubleshooting Trace Settings" section on page 8-1.

The trace parameters display for the service that you chose. In addition, the Apply to All Nodes check box displays.

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

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

Step 7 From the Debug Trace Level drop-down list box, choose the level of information that you want traced, as described in "Debug Trace Level Settings" section on page 7-5.

Step 8 Check the Trace Fields check box for the service that you chose; for example, Cisco Log Partition Monitoring Tool Trace Fields.

Step 9 If the service does not have multiple trace settings where you can specify the traces that you want to activate, check the **Enable All Trace** check box. If the service that you chose has multiple trace settings, check the check boxes next the trace check boxes that you want to enable, as described in the following sections:

- Cisco RIS Data Collector Trace Fields, page 7-7
- Trace Output Settings Descriptions and Defaults, page 7-7

Caution Device Name Based Trace monitoring does not apply to Cisco Unified Expert Advisor.

Step 10 To limit the number and size of the trace files, specify the trace output setting. See Table 7-6 for descriptions and default values.

Step 11 To save your trace parameters configuration, click the **Save** button.

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

Additional Information

See the "Related Topics" section on page 7-8.

Service Groups in Trace Configuration

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

Table 7-1 Service Groups in Trace Configuration

Service Group	Services and Trace Libraries	Notes
CM Services	Cisco CTIManager, Cisco Unified Expert Advisor, Cisco IP Phone Service, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Extended Functions, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, Cisco TFTP, and Cisco Unified Mobile Voice Access Service. **Caution** This service does not apply to Cisco Unified Expert Advisor. **Tip** In Cisco Unified Expert Advisor, runtime service and reporting service is supported. See the *Administration and Configuration Guide for Cisco Unified Expert Advisor* for more information.	For a description of these services, see the "Understanding Services" section on page 9-1. For most services in the CM Services group, you run trace for specific components, instead of enabling all trace for the service. The "Trace Field Descriptions" section on page 7-6 lists the services for which you can run trace for specific components.
Database and Admin Services	Cisco CCM DBL Web Library, Cisco CCMAdmin Web Service, Cisco Database Layer Monitor, Cisco License Manager, and Cisco Role-based Security **Caution** Cisco AXL Web Service and Cisco Bulk Provisioning does not apply to Cisco Unified Expert Advisor.	For a description of these services (not the Cisco CCM DBL Web Library or Cisco Role-based Security options), see the "Understanding Services" section on page 9-1. Choosing the Cisco CCM DBL Web Library option activates the trace for database access for Java applications. For database access for C++ applications, activate trace for Cisco Database Layer Monitor, as described in the "Cisco Database Layer Monitor Trace Fields" section on page 7-6. Choosing the Cisco Role-based Security option, which supports Cisco Unified Expert Advisor, activates trace for user-role authorization. For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components.

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

Service Group	Services and Trace Libraries	Notes
Performance and Monitoring Services	Cisco AMC Service, Cisco CCM NCS Web Library, Cisco Log Partition Monitoring Tool, Cisco RISDC, and Cisco RTMT Web Service **Caution** Cisco CCM PD Web Service and Cisco CallManager SNMP Service are not applicable to the Cisco Unified Expert Advisor.	For a description of these services (not the Cisco CCM NCS Web Library or the Cisco RTMT Web Service), see the "Understanding Services" section on page 9-1. Choosing the Cisco CCM NCS Web Library option activates trace for database change notification for the Java client. Choosing the Cisco RTMT Web Service option activates trace for the RTMT servlets; running this trace creates the server-side log for RTMT client queries.
Security Services	Cisco CTL Provider **Caution** Cisco Certificate Authority Proxy Function is not applicable to the Cisco Unified Expert Advisor.	For a description of these services, see the "Understanding Services" section on page 9-1. You enable all trace for each service, instead of running trace for specific components.
Directory Service	Cisco DirSync **Caution** Cisco DirSync service does not apply to Cisco Unified Expert Advisor.	For a description of this service, see the "Understanding Services" section on page 9-1. You enable all trace for this service, instead of running trace for specific components.
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master	For a description of these services, see the "Understanding Services" section on page 9-1. You enable all trace for each service, instead of running trace for specific components.
System Services	Cisco CCMRealm Web Service, Cisco CCMService Web Service, Cisco Common User Interface, and Cisco Trace Collection Service	For a description of the Cisco Trace Collection service, see the "Understanding Services" section on page 9-1. Choosing the Cisco CCMRealm Web Service option activates trace for login authentication. Choosing the Cisco Common User Interface option activates trace for the common code that multiple applications use; for example, Cisco Unified Operating System and Cisco Unified Serviceability. Choosing the Cisco CCMService Web Service option activates trace for the Cisco Unified Serviceability operations console. You enable all trace for each option/service, instead of running trace for specific components.

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

Service Group	Services and Trace Libraries	Notes
SOAP Services	Cisco SOAP Web Service	Choosing the Cisco SOAP Web Service option activates the trace for the AXL Serviceability API. **Caution** The Cisco AXL Web Service does not apply to Cisco Unified Expert Advisor You enable all trace for this service, instead of running trace for specific components.
Platform Services	Cisco Unified OS Admin Web Service	The Cisco Unified OS Admin Web Service supports Cisco Unified Operating System Administration, which is the web application that provides management of platform-related functionality such as certificate management, version settings, and installations and upgrades. You enable all trace for this service, instead of running trace for specific components.

Debug Trace Level Settings

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

Table 7-2 Debug Trace Levels for Services

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

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

Table 7-3 Debug Trace Levels for Servlets

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

Additional Information

See the "Related Topics" section on page 7-8.

Trace Field Descriptions

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

- For application tracing, see the *Administration and Configuration Guide for Cisco Unified Expert Advisor*
- Cisco RIS Data Collector Trace Fields, page 7-7

Cisco Database Layer Monitor Trace Fields

Table 7-4 describes the Cisco Database Layer Monitor trace fields.

Table 7-4 Cisco Database Layer Monitor Trace Fields

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

Additional Information

See the "Related Topics" section on page 7-8.

Cisco RIS Data Collector Trace Fields

Table 7-5 describes the Cisco RIS Data Collector (RISDC) trace fields.

Table 7-5 Cisco RIS Data Collector Trace Fields

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

Additional Information

See the "Related Topics" section on page 7-8.

Trace Output Settings Descriptions and Defaults

Table 7-6 contains the serviceability trace log file descriptions and defaults.

Tip See the *Administration and Configuration Guide for Cisco Unified Expert Advisor* for more information on application tracing.

Caution When you change either the maximum number of files or the maximum file size settings in the Trace Configuration window, the system deletes all service log files except for the current file, that is, if the service is running; if the service has not been activated, the system deletes the files immediately after

you activate the service. Before you change the maximum number of files setting or the maximum file Size setting, download and save the service log files to another server if you want to keep a record of the log files; to perform this task, use Trace & Log Central in RTMT.

Table 7-6 Trace Output Settings

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

Additional Information

See the "Related Topics" section on page 7-8.

Related Topics

- Configuring Trace Parameters, page 7-1
- Service Groups in Trace Configuration, page 7-3
- Debug Trace Level Settings, page 7-5
- Trace Field Descriptions, page 7-6
- Trace Output Settings Descriptions and Defaults, page 7-7

CHAPTER 8

Configuring Troubleshooting Trace Settings

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

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

Procedure

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

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

Note A list of services display. The services that are not activated on the node display as N/A.

Step 3 Perform one of the following tasks:

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

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

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

Step 4 Click the **Save** button.

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

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

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

Additional Information

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

Related Topics

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

CHAPTER 9

Understanding Services

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

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

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

Feature Services

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

After the Cisco Unified Expert Advisor installation, the system does not automatically activate feature services, which are related services that are required if you want to use Cisco Unified Expert Advisor features. After you activate feature services, you can modify associated service parameters in Cisco Unified Expert Advisor operations console.

If you are upgrading Cisco Unified Expert Advisor, those services that you activated on the system prior to the upgrade automatically activate and start after the upgrade.

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

- Network Services, page 9-2

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

Tip For service activation recommendations, see the "Service Activation" section on page 9-7 and the "Configuring Services" section on page 11-1.

Database and Admin Services

This section describes the Database and Admin Services:

Cisco AXL Web Service,

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

Caution The Cisco AXL Web Service does not apply to Cisco Unified Expert Advisor

Performance and Monitoring Services

This section describes the Performance Monitoring Services.

Cisco Serviceability Reporter

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

This service gets installed on all the Cisco Unified Expert Advisor nodes in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco Unified Serviceability from the Tools menu. Each summary report comprises different charts that display the statistics for that particular report. After you activate the service, report generation may take up to 24 hours.

Caution Cisco DirSync service does not apply to Cisco Unified Expert Advisor.

Network Services

Installed automatically, network services include services that the Cisco Unified Expert Advisor system requires to function; for example, database and platform services. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Call Control—Network Services window.

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

- Performance and Monitoring Services, page 9-3

Performance and Monitoring Services

This section describes the Performance and Monitoring Services.

Cisco CallManager Serviceability RTMT

Caution While the legacy software calls it "CallManager", this service also applies to Cisco Unified Serviceabilty for Cisco Unified Expert Advisor.

The Cisco Unified Serveciability RTMT servlet supports Cisco Unified Expert Advisor RTMT, which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor devices, system performance.

Note Even if the product name has changed to the Cisco Unified Communications Manager, Cisco CallManager Serviceability RTMT servlet continues to remain as Cisco CallManager as it is part of the underlying legacy platform.

Cisco RTMT Reporter Servlet

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

Cisco Log Partition Monitoring Tool

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

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

Cisco Tomcat Stats Servlet

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

Cisco RIS Data Collector

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

The Cisco RISDC service provides an interface for applications, such as the Cisco Unified Expert Advisor RTMT, SOAP applications, and so on, to retrieve the information that is stored in on the RIS server.

Cisco AMC Service

Used for the Cisco Unified Expert Advisor RTMT, this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on nodes in the cluster. Used for the Cisco Unified Expert Advisor RTMT, this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server.

Backup and Restore Services

This section describes the Backup and Restore Services.

Cisco DRF Master

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

Cisco DRF Local

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

System Services

This section describes the System Services.

Cisco CallManager Serviceability

Caution While the legacy software calls it “CallManager”, this service applies to Cisco Unified Serviceabilty for Cisco Unified Expert Advisor.

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

Cisco CDP

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

Cisco Trace Collection Servlet

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

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

Cisco Trace Collection Service

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

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

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

Platform Services

This section describes the Platform Services.

A Cisco DB

A Cisco DB service supports the Informix database engine.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

SNMP Master Agent

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

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

MIB2 Agent

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

Host Resources Agent

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

Native Agent Adaptor

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

System Application Agent

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

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified Expert Advisor server. This service implements the CISCO-CDP-MIB.

Cisco Syslog Agent

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

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

Cisco Electronic Notification

This service works with Cisco Unified Operating System operations console, so you can send e-mails about software updates.

Cisco Certificate Expiry Monitor

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

Note The Cisco License Manager service is part of the underlying Cisco Unified Communications Manager legacy platform. This service do not apply to Cisco Unified Expert Advisor.

Cisco DB Replicator

The Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent nodes in the cluster. This service is used to monitor the OAMP data replication for the Cisco Unified Communications Manager.

DB Services

This section describes the DB Services.

Cisco Database Layer Monitor

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

SOAP Services

This section describes the SOAP Services.

Cisco SOAP-Real-Time Service APIs

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

Cisco SOAP-Performance Monitoring APIs

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

Cisco SOAP-Log Collection APIs

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

Service Activation

You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in Cisco Unified Serviceability. Cisco Unified Serviceability activates feature services in automatic mode and checks for service dependencies. When you choose to activate a feature service, Cisco Unified Serviceability prompts you to select all the other services, if any, that depend on that service to run. When you click the **Set Default** button, Cisco Unified Serviceability chooses those services that are required to run on the server. Cisco Unified Serviceability activates feature services in automatic mode and checks for service dependencies based on a single-node configuration. When you choose to activate a feature service, Cisco Unified Serviceability prompts you to select all the other services, if any, that depend on that service to run based on a single-node configuration. When you click the **Set Default** button, Cisco Unified Serviceability chooses those services that are required to run Cisco Unified Expert Advisor based on a single-node configuration. Activating a service automatically starts the service. You start/stop services from Control Center.

Control Center

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

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

Services Configuration Checklist

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

Table 9-1 Services Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate the feature services that you want to run.	• Feature Services, page 9-1 • Activating and Deactivating Feature Services, page 11-1
Step 2	If necessary, troubleshoot problems by using the Cisco Unified Serviceability trace tools.	• Configuring Trace, page 7-1 • *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*

Where to Find More Information

Related Topics

- Control Center, page 9-7
- Feature Services, page 9-1
- Network Services, page 9-2

CHAPTER 10

Understanding Serviceability Reports Archive

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

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

Note Because the Cisco Serviceability Reporter is only active on the first node, at any time, Reporter generates reports only on the first node, not the other nodes.

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

The reports contain 24-hour data for the previous day. A suffix that is added to the report names shows the date for which Reporter generated them; for example, AlertRep_mm_dd_yyyy.pdf. The Serviceability Reports Archive window uses this date to display the reports for the relevant date only. The reports generate from the data that is present in the log files, with the timestamp for the previous day. The system considers log files for the current date and the previous two days for collecting data to take into account the time zone differences between the server locations. The time that is shown in the report reflects the first node "System Time." If the first node and subsequent node(s) are in different time zones, the first node "System Time" shows in the report.

Note You can continue to download log files from all nodes in the cluster while you are generating reports. See the *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor* for more information on downloading log files, The Cisco Unified Expert Advisor Option provides reporting options for agent and assignment activity and metrics such as the number of offered calls an expert handled, rejected, and so forth. See the *Reporting Guide for Cisco Unified Expert Advisor* for more information on generating reports.

Serviceability Reporter Service Parameters

Caution The values for these parameters are obtained from the Cisco Unified Communications Manager defaults.

Cisco Serviceability Reporter uses the following service parameters:

- RTMT Reporter Designated Node—Specifies the designated node on which RTMT Reporter runs. This default equals the IP address of the server on which the Cisco Serviceability Reporter service is first activated.
- Report Generation Time—Specifies the number of minutes after midnight. Reports generate at this time for the most recent day. The minimum value equals 0 and the maximum value equals 1439.
- Report Deletion Age—Specifies the number of days that the report must be kept on the disk. The system deletes reports that are older than the specified age. The minimum value equals 0, and the maximum value equals 30.

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

Note If a node gets removed completely from the network (the node should be removed from the network and also from the list of servers in Cisco Unified Expert Advisor operations console, Reporter does not consider this node while it is generating reports, even if the log file contains the data for that node.

Server Statistics Report

The Server Statistics Report provides the following line charts:

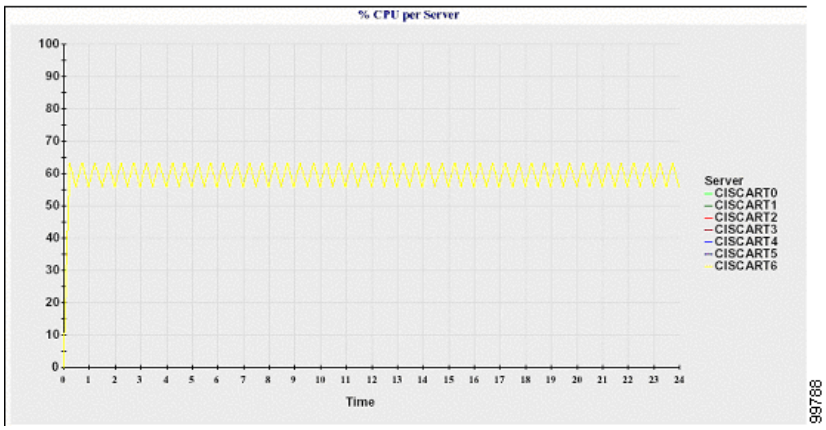
- Percentage of CPU per Server, page 10-2
- Percentage of Memory Usage per Server, page 10-3
- Percentage of Hard Disk Usage of the Largest Partition per Server, page 10-3

Percentage of CPU per Server

A line chart displays the percentage of CPU usage per Cisco Unified Expert Advisor node. A line chart displays the percentage of CPU usage for the server. Each line in the chart represents the data for each node in the Cisco Unified Expert Advisor cluster (for which data is available). Each data value in the chart represents the average CPU usage for a 15-minute duration. If no data exists for any one node, Reporter does not generate the line that represents that node. If no data exists for all nodes, Reporter does not generate the chart. If no data exists, Reporter does not generate the chart. The message “No data for Server Statistics report available” displays.

Figure 10-1 shows a line chart example that represents the percentage of CPU usage per Cisco Unified Expert Advisor node.

Figure 10-1 Line Chart That Depicts the Percentage of CPU Per Node

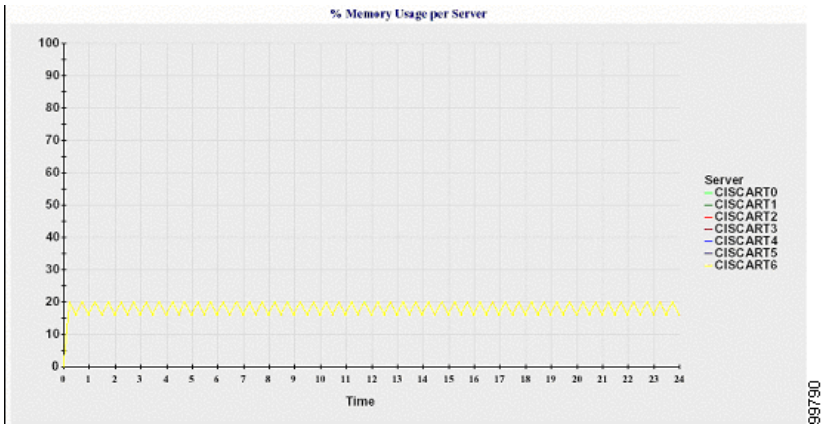


Percentage of Memory Usage per Server

A line chart displays the percentage of Memory Usage per Cisco Unified Expert Advisor node (%MemoryInUse). A line chart displays the percentage of Memory Usage for the server (%MemoryInUse). Each line in the chart represents the data for each node in the Cisco Unified Expert Advisor cluster (for which data is available). Each data value in the chart represents the average memory usage for a 15-minute duration. If no data exists for any node, Reporter does not generate the line that represents that node. If no data exists for all nodes, Reporter does not generate the chart. If no data exists, Reporter does not generate the chart.

Figure 10-2 shows a line chart example that represents the percentage of memory usage per Cisco Unified Expert Advisor node.

Figure 10-2 Line Chart That Depicts Percentage of Memory Usage Per Node



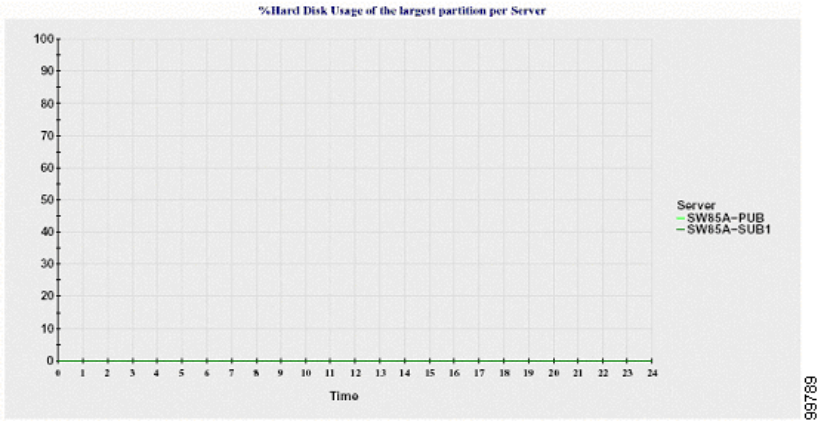
Percentage of Hard Disk Usage of the Largest Partition per Server

A line chart displays the percentage of disk space usage for the largest partition per Cisco Unified Expert Advisor node (%DiskSpaceInUse). A line chart displays the percentage of disk space usage for the largest partition on the server (%DiskSpaceInUse). Each line in the chart represents the data for each node in the Cisco Unified Expert Advisor cluster (for which data is available). Each data value in the

chart represents the average disk usage for a 15-minute duration. If no data exists for any one node, Reporter does not generate the line that represents that node. If no data exists for all nodes, Reporter does not generate the chart. If no data exists, Reporter does not generate the chart.

Figure 10-3 shows a line chart example that represents the percentage of hard disk usage for the largest partition per Cisco Unified Expert Advisor node.

Figure 10-3 Line Chart That Depicts Percentage of Hard Disk Usage of the Largest Partition Per Node



Each server in the cluster contains log files that match the file name pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The server contains log files that match the file name pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- % CPU usage on each node
- % CPU usage on the server
- % Memory usage (%MemoryInUse) on each node
- % Memory usage (%MemoryInUse) on the server
- % Hard disk usage of the largest partition (%DiskSpaceInUse) on each node
- % Hard disk usage of the largest partition (%DiskSpaceInUse) on the server

Alert Summary Report

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

- Number of Alerts per Server, page 10-4
- Number of Alerts per Severity for the Cluster, page 10-5
- Top 10 Alerts in the Cluster, page 10-6

Number of Alerts per Server

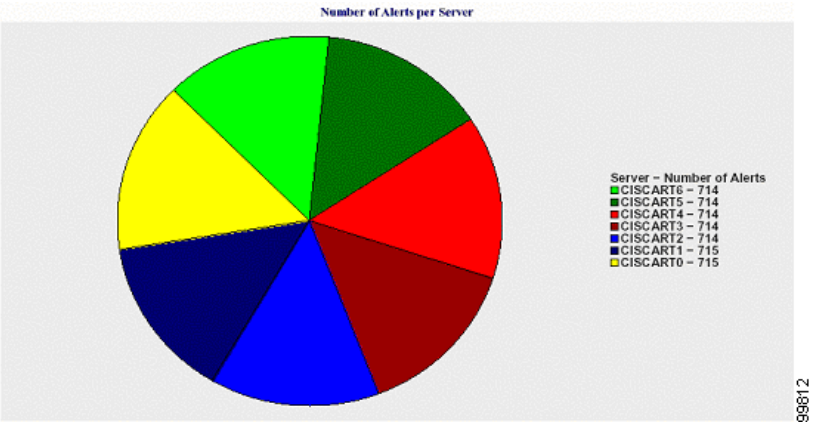
A pie chart provides the number of alerts per Cisco Unified Expert Advisor node. The chart displays the serverwide details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated for a particular server in the Cisco Unified Expert Advisor cluster. The chart includes as many number of sectors as there are servers (for which Reporter generates alerts in the day) in the

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

A pie chart provides the number of alerts for the server. The chart displays the serverwide details of the alerts that are generated. If no data exists for the server, Reporter does not generate the chart. The message “No alerts were generated for the day” displays.

Figure 10-4 shows a pie chart example that represents the number of alerts per server.

Figure 10-4 Pie Chart That Depicts Number of Alerts Per Server

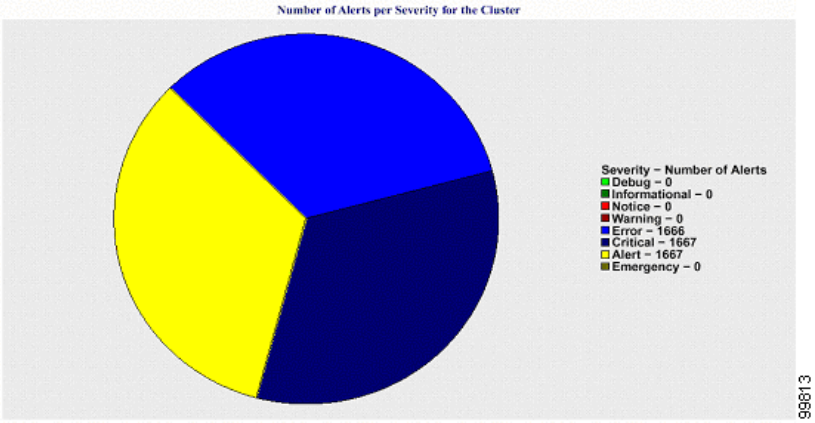


Number of Alerts per Severity for the Cluster

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

Figure 10-5 shows a pie chart example that represents the number of alerts per severity for the cluster.

Figure 10-5 Pie Chart That Depicts Number of Alerts Per Severity for the Cluster

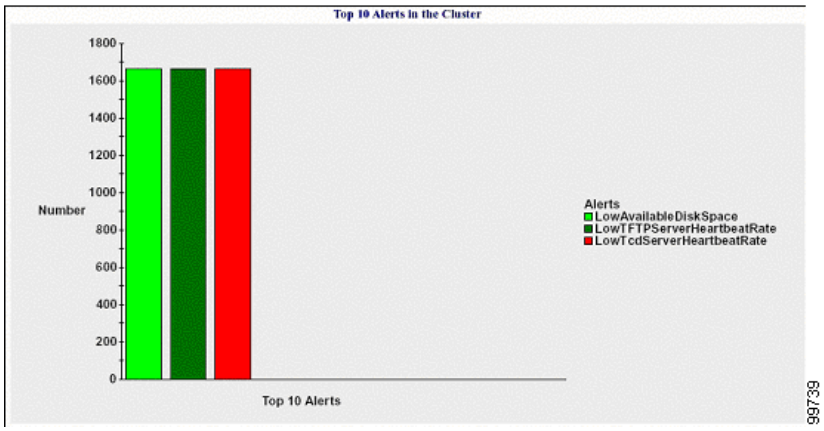


Top 10 Alerts in the Cluster

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

Figure 10-6 shows a bar chart example that represents the top 10 alerts in the cluster.

Figure 10-6 Bar Chart That Depicts Top 10 Alerts in the Cluster



Each server in the cluster contains log files that match the file name pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The server contains log files that match the file name pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

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

Serviceability Reports Archive Configuration Checklist

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

Table 10-1 Serviceability Reports Archive Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Activate the Cisco Serviceability Reporter service.	Activating and Deactivating Feature Services, page 11-1
Step 2	View the reports that the Cisco Serviceability Reporter service generates.	Configuring Serviceability Reports Archive, page 12-1

Where to Find More Information

Related Topics

- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*
- Configuring Serviceability Reports Archive, page 12-1
- *Reporting Guide for Cisco Unified Expert Advisor*

CHAPTER 11

Configuring Services

This chapter contains information on the following topics:

Activating and Deactivating Feature Services

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

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

Tip Before you activate services in the Service Activation window, review Table 11-1.

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

Procedure

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

The Service Activation window displays.

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

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

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

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

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

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

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

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

Additional Information

See the "Related Topics" section on page 11-4.

Cluster Service Activation Recommendations

Caution The Cisco Unified Communications Manager service types continue to be displayed in the Cisco Unified Operating System operations console, but are not populated by Cisco Unified Expert Advisor.

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

Table 11-1 Service Activation Recommendations

Service/Servlet	Activation Recommendations
Database and Admin Services	
Cisco AXL Web Service	Activate on only the first node. Failing to activate the service causes the inability to update the Cisco Unified Expert Advisor from client-based applications that use AXL. **Note** The service only generates reports on the first node even if you activate the service on other nodes. **Caution** The Cisco AXL Web Service does not apply to Cisco Unified Expert Advisor.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Activate on only the first node. **Note** The service only generates reports on the first node even if you activate the service on other nodes.

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

Control Center in Cisco Unified Serviceability allows you to view status, refresh the status, and to start, stop, and restart feature and network services for a node.

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

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

Procedure

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

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

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

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

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

The window displays the following items:

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

Step 3 Perform one of the following tasks:

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

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

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

  A message indicates that restarting may take a while. Click **OK**.
- To get the latest status of the services, click the **Refresh** button.
- To go to the Service Activation window or to the other Control Center window, choose an option from the Related Links drop-down list box and click **Go**.

Additional Information

See the "Related Topics" section on page 11-4.

Using a Command Line Interface to Start and Stop Services

You can start and stop some services through the CLI. Refer to the *Cisco Unified Communications Operating System Administration Guide* for more information.

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

Additional Information

See the "Related Topics" section on page 11-4.

Related Topics

CHAPTER 12

Configuring Serviceability Reports Archive

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

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

Before you Begin

Activate the Cisco Serviceability Reporter service, which is CPU intensive. Cisco recommends that you activate the service on a non-callprocessing server. After you activate the service, report generation may take up to 24 hours.

Procedure

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

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

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

A list of days that correspond to the month displays.

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

The report files for the day that you chose display.

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

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

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

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

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

Additional Information

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

Related Topics

- *Real-Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*
- Understanding Serviceability Reports Archive, page 10-1

CHAPTER 13

Understanding Simple Network Management Protocol

This chapter provides information on the following topics:

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

You use Cisco Unified Serviceability to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. Likewise, in the SNMP configuration windows, you can apply the settings to all nodes in the cluster.

This section contains information on the following topics:

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- Agent—A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  Cisco Unified Expert Advisor uses a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few MIB variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Cisco Unified Expert Advisor subagent interacts with the local Cisco Unified Expert Advisor only. The Cisco Unified Expert Advisor subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).
- Network Management System (NMS)—A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Cisco Unified Expert Advisor works with the following NMS:
  - Cisco Unified Operating Manager
  - HP OpenView
  - Third-party applications that support SNMP and Cisco Unified Expert Advisor SNMP interfaces

SNMP version 1 Support

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In Cisco Unified Serviceability, you configure SNMP v1 support in the V1/V2c Configuration window.

SNMP version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In Cisco Unified Serviceability, you configure SNMP v2c support in the V1/V2c Configuration window.

SNMP version 3 Support

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the "SNMP Community Strings and Users" section on page 13-4.

In Cisco Unified Serviceability, you configure SNMP v3 support in the V3 Configuration window.

SNMP Services

To support SNMP, you must use the following services, which display in the Service Activation and/or Control Center windows in Cisco Unified Serviceability. For a description of each service, see the "Understanding Services" section on page 9-1.

- Cisco Unified Expert Advisor SNMP service
- SNMP Master Agent
- MIB2 Agent
- Host Resources Agent
- System Application Agent
- Native Agent Adaptor
- Cisco CDP Agent
- Cisco Syslog Agent

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

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMP v1 and v2c only.

SNMP v3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In Cisco Unified Serviceability, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments. You configure the notification destinations by using the SNMP Notification Destination Configuration windows in Cisco Unified Serviceability.

Tip Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string/user correctly.

You configure the SNMP trap destination by choosing **SNMP > V1/V2 > Notification Destination** or **SNMP > V3> Notification Destination** in Cisco Unified Serviceability.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The Simple Network Management Protocol (SNMP) extension agent resides in each Cisco Unified Expert Advisor node and exposes the ciscoMmodalContactAppsMIB that provides detailed information about devices that are known to the node.

Cisco Unified Expert Advisor supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco Unified Expert Advisor CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco Unified Expert Advisor to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- CdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- CdpGlobalRun

- CdpGlobalMessageInterval
- CdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstalled
- sysApplRun
- sysApplMap

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

The system supports trap functionality only. The Cisco Syslog Agent supports only the following objects of CISCO-SYSLOG-MIB:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

ciscoMmodalContactAppsMIB

The CISCO-MMODAL-CONTACT-APPS-MIB contains both dynamic (real-time) and configured (static) information about the local Cisco Unified Expert Advisor.

To view the support lists for the CISCO-MMODAL-CONTACT-APPS-MIB, go to the following link: ftp://ftpeng.cisco.com/pub/mibs/v2

The following list of tables exists in the ciscoMmodalContactAppsMIB:

- General Information:
  - Table 13-1 lists the Cisco Unified Expert Advisor cluster information.

Table 13-1 Cisco Unified Expert Advisor Cluster Description

Name	Type	Description
Index	Integer	An arbitrary integer, selected by the local Cisco Unified Expert Advisor node, which uniquely identifies a device within the cluster.
ClusterName	SAS[1]	The host name of the Cisco Unified Expert Advisor device.
ClusterDescription	SAS	The description for the Cisco Unified Expert Advisor device.
ClusterType	Integer	The Cisco Unified Expert Advisor node type. Runtime(1): The node is a runtime node. reporting(2): The node is a reporting server node. Unknown(3) The type of the remote node is not known.
ClusterStatus	Integer	The current status of the Cisco Unified Expert Advisor node as viewed by this node. A remote Cisco Unified Expert Advisor node is up if the local Cisco Unified Expert Advisor node can communicate with it. Unknown(1): Current status of the remote node is Unknown, local (2): this is the local node in the table, remote-up(3):The local node is running and is able to communicate with the remote node. remote-down(4):The local node is running but it is unable to communicate with the remote node.
ClusterInetAddress Type	IAD[2]	This object identifies the IP address type of the remote Cisco Unified Expert Advisor.
ClusterInetAddress	IA[3]	This object identifies ip address of the Cisco Unified Expert Advisor. The type of address for this is identified by InetAddressType.
ClusterId	SAS	The unique ID of the Cluster to which this Cisco Unified Expert Advisor server belongs. At any point in time, the Cluster Id helps in associating a Cisco Unified Expert Advisor server to any given Cluster.

1. SNMP Administration String (SAS)
2. Internet Address
3. Internet Address Type

  - Table 13-2 lists the Cisco Unified Expert Advisor next node information.

Table 13-2 Cisco Unified Expert Advisor Next Node Description

Name	Type	Description
NxtNodeIndex	Integer	An arbitrary integer, selected by the local Cisco Unified Expert Advisor node.
NxtNodeName	SAS	The name of the node that is connected to the Cisco Unified Expert Advisor device.
NxtNodeType	SAS	A string describing the type of node that is connected to the device. This can be Unknown, ICM(PG), or CUPS.
NxtNodeIpAddr	IA	The IP address of the next node.
NxtNodeIpAddrType	IAD	The address type of the next node.
NxtNodeStatus	SAS	The status (if known) of the next node. This status indicates whether or not the next node is reachable. The values are: Unknown, Available, Unavailable, or Depreciated.

- License Information: Licensing is based on the fixed number of configured experts and not the dynamic number of in-use experts. The number of configured agents are available through the MIB. Table 13-3 lists the Cisco Unified Expert Advisor license information.

Table 13-3 Cisco Unified Expert Advisor License Information

Name	Type	Description
cmmcaLicRtExAdvConfig	G32[1]	The real-time number of expert licenses available on this node.
cmmcaLicTotalExAdvConfig	G32	The total number of expert licenses configured on this device.

1. Gauge 32

- System Conditions: A subsystem can raise or lower a system condition. Generally, these actions result in a SNMP trap. Table 13-4 lists the Cisco Unified Expert Advisor license information.

Table 13-4 Cisco Unified Expert Advisor System Conditions

Name	Type	Description
SystemConditionIndex	I32[1]	An arbitrary index for this table.
SystemConditionId	I32	An unique Id of the system condition, assigned by Cisco Unified Expert Advisor, used to identify a specific system condition.
SystemConditionSeverity	I32	This object specifies the severity level of the raised condition. The values are 1=warn or 2=critical.
SystemConditionDescription	SAS	This object provides a brief description of the raised system condition.
SystemConditionTimeStamp	DT	Timestamp of when the condition was raised in Cisco Unified Expert Advisor.
SystemConditionMessage	SAS	This object provides a message about the event which resulted in the system condition being raised.

1. Integer 32

- Thread Pool: Table 13-5 lists the Cisco Unified Expert Advisor thread pool information.

Table 13-5 Cisco Unified Expert Advisor Thread Pool Information

Name	Type	Description
TPoolRtIdleThreads	G32	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 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	G32	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 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	G32	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 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	G32	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 components 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.
TPoolRtMaxThreadsUsed	G32	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 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.

- Runtime Information: Table 13-6 lists the Cisco Unified Expert Advisor runtime information.

Table 13-6 Cisco Unified Expert Advisor Runtime Information

Name	Type	Description
EnvRtMaxMemUsed	G32	The real-time maximum memory used object is a real-time snapshot metric indicating the peak memory usage by the application within the runtime environment since startup. The object value is expressed as a count of bytes and indicates the high water mark of memory used simultaneously within the environment.
EnvRtCurrMemUsed	G32	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 as a count of bytes and indicates the current amount of memory used by this runtime environment.
EnvRtMaxMemAvail	G32	The real-time maximum memory available object is a real-time snapshot metric indicating the amount of memory available to the runtime environment. The object value is expresses as a count of bytes and indicates the amount of system memory available for use by the runtime environment.
EnvRtCurrMemAvail	G32	The real-time current memory available object is a real-time snapshot metric indicating the amount of available memory in the runtime environment. The object value is expressed as a count of bytes and indicates the amount of current system memory claimed by the runtime environment that is not currently being used.
EnvRtCurrThreadsIn Use	G32	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.
EnvRtMaxThreadsU sed	G32	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	C64	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.
RtMsgQMemPercent Usage	G32	The percentage of available message bus memory in use.
MaxMsgQMemAvail	G32	The actual amount of available message bus memory for use.
RtCongested	Truth Value	whether or not the subsystem is congested as determined by some heuristic

- Services: Not all services are found on all Cisco Unified Expert Advisor servers. Each component has its own service entry thus allowing maximum flexibility.
  - Table 13-7 lists the service information specific to Cisco Unified Expert Advisor.

Table 13-7 Cisco Unified Expert Advisor Services Information

Name	Type	Description
ServiceIndex	U32	The service index is a value that uniquely identifies an entry in the service table. The value is arbitrarily assigned by the SNMP agent.
ServiceType	Integer 32	The service type object identifies the type of Cisco Unified Expert Advisor functional service (see Table 13-8).
ServiceName	SAS	The service name object is a user-intuitive textual name for the Cisco Unified Expert Advisor application service (see Table 13-8).
ServiceStatus	I32	The service status object is the last known status of the Cisco Unified Expert Advisor application service" (see Table 13-9).
ServiceIntLastUpdate	Date and Time	The service interval last update object holds the date and time of the last refresh of interval and aggregate statistic object values for this Cisco Unified Expert Advisor service. Interval and aggregate statistics are reported at a regular interval (the interval held by ServiceIntPeriod).
ServiceIntPeriod	G32	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.
RtRoutingDomain	SAS	The routing domain that contains the subsystem.
RtLogLevel	SAS	The current log level of the subsystem.
RtTraceMask	SAS	The current trace mask for debugging for the subsystem.
RtMessageThroughput	Counter 64	The average message throughput in messages/sec per subsystem.
RtUptime	Counter 64	The number of seconds the subsystem has been up.
RtMsgReceived	Counter 64	The number of messages received by the subsystem.
MaxThreadsAvailable	Counter 64	The maximum number of threads available for this service.
RtThreadsInUse	Counter 64	The number of currently running threads for this service.

  - Table 13-8 lists the each service type and name of the Cisco Unified Expert Advisor.

Table 13-8 Cisco Unified Expert Advisor Service Type and Name Information

Service Type (Integer 32)	Service Name (SAS)
CM(1)	Contact Manager
RM(2)	Resource Manager
WA(3)	Work Assigner
MPA(4)	Media Platform Adapter

Table 13-8 Cisco Unified Expert Advisor Service Type and Name Information

Service Type (Integer 32)	Service Name (SAS)
BRE(5)	Business Rule Engine
ICMGW(6)	ICM GW
RDA(7)	Resource Desktop Adapter
RA(8)	Reporting Adapter
RS(9)	Reporting Subsystem

– Table 13-9 lists the Cisco Unified Expert Advisor service status values.

Table 13-9 Cisco Unified Expert Advisor Service Status Values

Service Status	Definition
disabled(1)	The service has not yet begun to start up.
starting(2)	The service is in initialization procedure, configuring and licensing, not accepting connections yet.
inService(3)	The service is up and running optimally, accepting connections at full QoS (if applicable).
inServiceWarning(4)	The service is running sub-optimally, possibly due to poor QoS or a threshold reached; see transition reason for explanation.
inServiceCritical(5)	The service is running but very near to failure, similar to 'inServiceWarning' but much more dire.
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).
OutOfService(7)	The service is no longer accepting new calls and is down for some reason. It can still be brought in service.
stopping(8)	The service no longer accepts new connections, lets current connections terminate gracefully.
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, and other tasks).
unknown(10)	The status of the Cisco Unified Expert Advisor service is unknown to the SNMP agent either because the link between the agent and the application has been broken or the agent is in the midst of refreshing service status. A refresh typically occurs after an agent restart due to configuration changes.

Vendor-Specific MIBs

The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that are developed by the hardware vendors; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 13-10—Describes supported IBM MIBs

- Table 13-11—Describes supported HP MIBs

Table 13-10 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 13-11 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information

Table 13-11 HP MIBs (continued)

MIB	OID	Description
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

SNMP Trace Configuration

A default setting exists for all agents. For Cisco CDP Agent and Cisco Syslog Agent, use the CLI to change trace settings, as described in the *Administration and Configuration Guide for Cisco Unified Expert Advisor*.

SNMP Configuration Checklist

Table 13-12 provides an overview of the steps for configuring SNMP.

Table 13-12 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the Control Center—Network Services window, verify that the system started the SNMP services.	• SNMP Services, page 13-3 • Understanding Services, page 9-1 • Configuring Services, page 11-1
Step 3	If you are using SNMP v1/v2c, configure the community string.	Configuring a Community String, page 14-2
Step 4	If you are using SNMP v3, configure the SNMP user.	Configuring the SNMP User, page 15-2
Step 5	Configure the notification destination for traps or informs.	• For SNMP v1/v2c—Configuring a Notification Destination for SNMP V1/V2c, page 14-6 • For SNMP v3—Configuring a Notification Destination for SNMP V3, page 15-6 • SNMP Traps and Informs, page 13-4
Step 6	Configure the system contact and location for the MIB2 system group.	Configuring the MIB2 System Group, page 16-1
Step 7	Restart the Master Agent service.	• SNMP Services, page 13-3 • Understanding Services, page 9-1

Troubleshooting

Review this section for troubleshooting tips.

Make sure that all of the feature and network services listed in "SNMP Services" section on page 13-3 are running.

Cannot poll any MIBs from the system

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system.

Note By default, no community string or user is configured on the system.

Check whether the community string or snmp user is properly configured on the system by using the SNMP configuration windows.

Cannot receive any notifications from the system

This condition means that the notification destination is not configured correctly on the system.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Configuring Services, page 11-1
- Configuring SNMP V1/V2c, page 14-1
- Configuring SNMP V3, page 15-1
- Configuring the MIB2 System Group, page 16-1

CHAPTER 14

Configuring SNMP V1/V2c

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

Tip If you use SNMP version 3, see the "Configuring SNMP V3" section on page 15-1.

Finding a Community String

Tip Configure the community string for Cisco Unified Expert Advisor only. The Add New button does not display in the SNMP Community String Configuration window until you click the **Find** button. If no community strings exist and you want to add want a community string, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a community string, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V1/V2c > Community String**.

The Find/List window displays.

Step 2 From the Find Community Strings where Name drop-down list box, choose the specific search criteria that you want to use for the community string.

Step 3 Enter the community string for which you want to search.

Step 4 In the Server field, enter the hostname or IP address of the server where the community string exists.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the community string that you want to view.

Step 8 To add or update a community string, see the "Configuring a Community String" section on page 14-2.

Additional Information

See the "Related Topics" section on page 14-8.

Configuring a Community String

Because the SNMP agent provides security by using community strings, you must configure the community string to access any management information base (MIB) in a Cisco Unified Expert Advisor server. Change the community string to limit access to the Cisco Unified Expert Advisor server. To add, modify, and delete community strings, access the SNMP Community String configuration window.

Procedure

Step 1 Perform the procedure in the "Finding a Community String" section on page 14-1.

Step 2 Perform one of the following tasks:

- To add a new community string, click the **Add New** button and go to Step 3.
- To modify an existing community string, locate the community string, as described in the "Finding a Community String" section on page 14-1; click the name of the community string that you want to edit and go to Step 3.

  You cannot change the name of the community string or the server.
- To delete a community string, see the "Deleting a Community String" section on page 14-4.

Step 3 Enter the configuration settings, as described in Table 14-1.

Tip Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 4 After you complete the configuration, click **Add New** to save a new community string or click **Save** to save changes to an existing community string.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Note Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

The system refreshes and displays the SNMP Community String Configuration window. The community string that you created displays in the window.

Additional Information

See the "Related Topics" section on page 14-8.

Community String Configuration Settings

Table 14-1 describes the community string configuration settings. For related procedures, see the "Related Topics" section on page 14-8.

Table 14-1 Community String Configuration Settings

Field	Description
Server	This setting in the Community String configuration window displays as read only because you specified the server choice when you performed the procedure in the "Finding a Community String" section on page 14-1. To change the server for the community string, perform the procedure in the "Finding a Community String" section on page 14-1.
Community String	Enter a name for the community string. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Choose community string names that will be hard for outsiders to figure out. When you edit a community string, you cannot change the name of the community string.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click this radio button.
Accept SNMP Packets only from these hosts	To accept SNMP only from specified hosts, click this radio button. **Tip** In the Host IP Address field, enter a host from which you want to accept packets and click **Insert**. Repeat this process for each host from which you want to accept packets. To delete a host, choose that host from the Host IP Addresses list box and click **Remove**.

Table 14-1 Community String Configuration Settings (continued)

Field	Description
Access Privileges	From the drop-down list box, choose the appropriate access level from the following list: • **ReadOnly**—The community string can only read the values of MIB objects. • **ReadWrite**—The community string can read and write the values of MIB objects. • **ReadWriteNotify**—The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The community string can only send MIB object values for a trap and inform messages. • **None**—The community string cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a community string with NotifyOnly or ReadWriteNotify privileges.
Apply To All Nodes	To apply the community string to all nodes in the cluster, check this check box.

Deleting a Community String

To delete a community string, perform the following procedure:

Procedure

Step 1 Locate the community string, as described in the "Finding a Community String" section on page 14-1.

Step 2 From the list of matching records, check the check box next to the community string that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message indicates that the system will delete notification entries that relate to this community string. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" section on page 11-3.

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

Additional Information

See the "Related Topics" section on page 14-8.

SNMP Notification Destination

The following sections apply to SNMP notification destination configuration, depending on the SNMP version that you support:

SNMP V1/V2c

SNMP V3

Finding a Notification Destination for SNMP V1/V2c

Tip The Add New button does not display in the SNMP Notification Destination Configuration window until you click the Find button. If no notification destinations exist and you want to add a notification destination, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a notification destination for V1/V2c, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V1/V2c > Notification Destination**.

The Find/List window displays.

Step 2 From the Find Notification where Destination IP drop-down list box, choose the specific search criteria that you want to use to find the notification destination.

Step 3 Enter the notification destination for which you want to search.

Step 4 In the Server field, enter the hostname or IP address of the server that supports the notification destination.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 To view the configuration for one of the items in the search results, click the item.

Step 8 To add or update a notification string, see the "Configuring a Notification Destination for SNMP V1/V2c" section on page 14-6.

Additional Information

See the "Related Topics" section on page 14-8.

Configuring a Notification Destination for SNMP V1/V2c

To configure the notification destination (trap/inform receiver) for V1/V2c, perform the following procedure.

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V1/V2c" section on page 14-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP notification destination, click the **Add New** button and go to Step 3.

  You configure the notification destination for the server that you choose in the Server drop-down list box in the Find/List window.
- To modify an existing SNMP notification destination, locate the notification destination, as described in the "Finding a Notification Destination for SNMP V1/V2c" section on page 14-5; click the name of the SNMP notification destination that you want to edit and go to Step 3.
- To delete an SNMP notification destination, see the "Deleting a Notification Destination for SNMP V1/V2c" section on page 14-8.

Step 3 Enter the configuration settings, as described in Table 14-2.

Tip Before you save the configuration, you can click the **Clear** button at any time to delete all information that you entered for all settings in the window.

Step 4 To save a notification destination, click **Insert**, or click **Save** to save changes to an existing notification destination.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent, click **OK**.

Note Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Additional Information

See the "Related Topics" section on page 14-8.

Notification Destination Configuration Settings for SNMP V1/V2c

Table 14-2 describes the notification destination configuration settings for V1/V2c. For related procedures, see the "Related Topics" section on page 14-8.

Table 14-2 Notification Destination Configuration Settings for V1/V2

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V1/V2c" section on page 14-5. To change the server for the notification destination, perform the procedure in the "Finding a Community String" section on page 14-1.
Host IP Addresses	From the drop-down list box, choose the Host IP address of the trap destination or choose **Add New**. If you choose Add New, enter the IP address of the trap destination. For existing notification destinations, you cannot modify the host IP address configuration.
Port Number	In the field, enter the notification-receiving port number on the destination server that receives SNMP packets.
V1 or V2C	From the SNMP Version Information pane, click the appropriate SNMP version radio button, either V1 or V2C, which depends on the version of SNMP that you are using. • If you choose V1, configure the community string setting. • If you choose V2C, configure the notification type setting and then configure the community string.
Community String	From the drop-down list box, choose the community string name to be used in the notification messages that this host generates. Only community strings with minimum notify privileges (ReadWriteNotify or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click the **Create New Community String** button to create a community string, as described in the "Configuring a Community String" section on page 14-2.

Table 14-2 Notification Destination Configuration Settings for V1/V2 (continued)

Field	Description
Notification Type	From the drop-down list box, choose the appropriate notification type.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box.

Deleting a Notification Destination for SNMP V1/V2c

To delete a notification destination, perform the following procedure:

Procedure

Step 1 Locate the notification destination, as described in the "Finding a Notification Destination for SNMP V1/V2c" section on page 14-5.

Step 2 From the list of matching records, check the check box next to the notification destination that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message asks whether you want to delete the notification entries. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

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

Additional Information

See the "Related Topics" section on page 14-8.

Related Topics

- Understanding Simple Network Management Protocol, page 13-1
- Finding a Community String, page 14-1
- Configuring a Community String, page 14-2
- Community String Configuration Settings, page 14-3
- Deleting a Community String, page 14-4
- SNMP Notification Destination, page 14-5
- Finding a Notification Destination for SNMP V1/V2c, page 14-5

- Configuring a Notification Destination for SNMP V1/V2c, page 14-6
- Notification Destination Configuration Settings for SNMP V1/V2c, page 14-7
- Deleting a Notification Destination for SNMP V1/V2c, page 14-8
- Configuring SNMP V3, page 15-1
- Configuring the MIB2 System Group, page 16-1

CHAPTER 15

Configuring SNMP V3

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

Tip If you use SNMP v1 or v2c, see the "Configuring SNMP V1/V2c" section on page 14-1.

Finding the SNMP User

Tip The Add New button does not display in the SNMP User Configuration window until you click the Find button. If no users exist and you want to add want a user, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a SNMP user, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V3 > User**.

The SNMP User Configuration window displays.

Step 2 From the Find User where Name list box, choose the specific search criteria that you want to use to find the user; for example, begins with.

Step 3 Enter the user name for which you want to search.

Step 4 From the Server drop-down list box, choose the hostname or IP address of the server where you access the user.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the user that you want to view.

Step 8 To add or update a user, see the "Configuring the SNMP User" section on page 15-2.

Additional Information

See the "Related Topics" section on page 15-9.

Configuring the SNMP User

To configure user(s) for SNMP, perform the following procedure:

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 15-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP user, click the **Add New** button in the SNMP User Configuration Find/List window and go to Step 3.
- To modify an existing SNMP user, locate the user, as described in the "Finding a Notification Destination for SNMP V3" section on page 15-5; click the name of the SNMP user that you want to edit and go to Step 3.
- To delete an SNMP user, see the "Deleting the SNMP User" section on page 15-4.

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

Tip Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 4 To add a new user, click **Insert**, or click **Save** to save changes to an existing user.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Note Make sure you configure this user on the NMS with the appropriate authentication and privacy settings.

Additional Information

See the "Related Topics" section on page 15-9.

SNMP User Configuration Settings

Table 15-1 describes the SNMP user configuration settings for V3. For related procedures, see the "Related Topics" section on page 15-9.

Table 15-1 SNMP User Configuration Settings for V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V3" section on page 15-5. To change the server where you want to provide access, perform the procedure in the "Finding the SNMP User" section on page 15-1.
User Name	In the field, enter the name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS). For existing SNMP users, this setting displays as read only.
Authentication Required	To require authentication, check the check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol. The password must contain at least 8 characters.
Privacy Required	If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the check box, enter the password in the Password and Reenter Password fields, and check the protocol check box. The password must contain at least 8 characters. **Tip** After you check the Privacy Required check box, the DES (Data Encryption Standard) check box automatically appears checked. The DES protocol prevents packets from being disclosed.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.

Table 15-1 SNMP User Configuration Settings for V3 (continued)

Field	Description
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Host IP Address field, enter a host from which you want to accept SNMP packets and click **Insert**. Repeat this process for each host from which you want to accept SNMP packets. To delete a host, choose that host from the Host IP Addresses pane and click **Remove**.
Access Privileges	From the drop-down list box, choose one of the following options for the access level: • **ReadOnly**—The user can only read the values of MIB objects. • **ReadWrite**—The user can read and write the values of MIB objects. • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **None**—The user cannot read, write, or send trap information. To change the trap configuration parameters, you need to configure a user with NotifyOnly or ReadWriteNotify privileges.
Apply To All Nodes	To apply the user configuration to all nodes in the cluster, check this check box.

Deleting the SNMP User

To delete a user for SNMP, perform the following procedure:

Procedure

Step 1 Locate the SNMP user, as described in the "Finding the SNMP User" section on page 15-1.

Step 2 From the list of matching records, check the check box next to the user that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message indicates that the system will delete notification entries that relate to this user. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

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

Additional Information

See the "Related Topics" section on page 15-9.

Finding a Notification Destination for SNMP V3

Tip The Add New button does not display in the SNMP Notification Destination Configuration window until you click the Find button. If no users exist and you want to add want a user, click the **Find** button and wait for the window to refresh. The Add New button displays.

To find a notification destination for V3, perform the following procedure:

Procedure

Step 1 Choose **Snmp > V3 > Notification Destination**.

Step 2 From the Find Notification where Destination IP drop-down list box, choose the specific search criteria that you want to use to find the notification destination; for example, begins with.

Step 3 Enter the IP address/hostname of notification destination for which you want to search.

Step 4 In the Server field, choose the hostname or IP address of the server that supports the notification destination.

Step 5 Click **Find**.

After you click the Find button, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 6 If you want to apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.

Step 7 From the list of results, click the notification destination that you want to view.

Step 8 To add or update a notification destination, see the "Configuring a Notification Destination for SNMP V3" section on page 15-6.

Additional Information

See the "Related Topics" section on page 15-9.

Configuring a Notification Destination for SNMP V3

To configure the trap/Inform receiver, perform the following procedure:

Procedure

Step 1 Perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 15-5.

Step 2 Perform one of the following tasks:

- To add a new SNMP notification destination, click the **Add New** button in the search results window and go to Step 3.
- To modify an existing SNMP notification destination, locate the notification destination in the search results window; click the name of the SNMP notification destination that you want to edit and go to Step 3.
- To delete an SNMP notification destination, see the "Deleting a Notification Destination for SNMP V3" section on page 15-8.

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

Tip Before you save the configuration, you can click the **Clear** button at any time to delete all information that you entered for all settings in the window.

Step 4 To save a notification destination, click **Insert**, or click **Save** to save changes to an existing notification destination.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

Additional Information

See the "Related Topics" section on page 15-9.

Notification Destination Configuration Settings for SNMP V3

Table 15-2 describes the notification destination configuration settings for V3. For related procedures, see the "Related Topics" section on page 15-9.

Table 15-2 Notification Destination Configuration Settings for V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure in the "Finding a Notification Destination for SNMP V3" section on page 15-5. To change the server for the notification destination, perform the procedure in the "Finding a Notification Destination for SNMP V3" section on page 15-5.
Host IP Addresses	From the drop-down list box, choose the Host IP address or choose **Add New**. If you chose Add New, enter the IP address for the host.
Port Number	In the field, enter the notification-receiving port number on the destination server.
Notification Type	From the drop-down list box, choose **Inform** or **Trap**. **Tip** Cisco recommends that you choose the Inform option. The Inform function retransmits the message until it is acknowledged, thus, making it more reliable than traps.
Remote SNMP Engine Id	This setting displays if you chose Inform from the Notification Type drop-down list box. From the drop-down list box, choose the engine ID or choose **Add New**. If you chose Add New, enter the ID in the Remote SNMP Engine Id field, which requires a hexidecimal value.
Security Level	From the drop-down list box, choose the appropriate security level for the user. • **noAuthNoPriv**—No authentication or privacy configured. • **authNoPriv**—Authentication configured, but no privacy configured. • **authPriv**—Authentication and privacy configured.

Table 15-2 Notification Destination Configuration Settings for V3 (continued)

Field	Description
User Information pane	From the pane, perform one of the following tasks to associate or disassociate the notification destination with the user. • To create a new user, click the **Create New User** button and see the "Configuring the SNMP User" section on page 15-2. • To modify an existing user, click the radio button for the user and click **Update Select ed User**; then, see the "Configuring the SNMP User" section on page 15-2. • To delete a user, click the radio button for the user and click **Delete Selected User**. The users that display vary depending on the security level that you configured for the notification destination.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box.

Deleting a Notification Destination for SNMP V3

To delete a notification destination, perform the following procedure:

Procedure

Step 1 Locate the SNMP notification destination, as described in the "Finding a Notification Destination for SNMP V3" section on page 15-5.

Step 2 From the list of matching records, check the check box next to the notification destination that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 A message asks you if you want to delete the notification destination. To continue the deletion, click **OK**.

Step 5 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the "Configuring Services" section on page 11-1.

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

Additional Information

See the "Related Topics" section on page 15-9.

Related Topics

- Understanding Simple Network Management Protocol, page 13-1
- Finding the SNMP User, page 15-1
- Configuring the SNMP User, page 15-2
- SNMP User Configuration Settings, page 15-3
- Deleting the SNMP User, page 15-4
- Finding a Notification Destination for SNMP V3, page 15-5
- Configuring a Notification Destination for SNMP V3, page 15-6
- Notification Destination Configuration Settings for SNMP V3, page 15-7
- Deleting a Notification Destination for SNMP V3, page 15-8
- Configuring SNMP V1/V2c, page 14-1
- Configuring the MIB2 System Group, page 16-1

CHAPTER 16

Configuring the MIB2 System Group

Cisco Unified Serviceability provides the MIB2 System Group Configuration window where you can configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location. This chapter contains information on the following topics:

Configuring the MIB2 System Group

Perform the following procedure to configure a system contact and system location for the MIB-II system group.

Tip This procedure supports SNMP v1, v2c, and v3 configuration.

Procedure

Step 1 Choose **Snmp > SystemGroup > MIB2 System Group**.

Step 2 Configure the settings, as described in Table 16-1.

Step 3 Click **Save**.

Step 4 A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent service, click **Cancel**. To restart the SNMP master agent service, click **OK**.

Note To clear the System Contact and System Location fields, click the **Clear All** button. To delete the system configuration, click the **Clear All** button and the **Save** button.

Additional Information

See the "Related Topics" section on page 16-2.

MIB2 System Group Configuration Settings

Table 16-1 describes the MIB2 System Group configuration settings. For related procedures, see the "Related Topics" section on page 16-2.

Table 16-1 MIB2 System Group Configuration Settings

Field	Description
Server	From the drop-down list box, choose the server for which you want to configure contacts; then, click **Go**.
System Contact	In the field, enter a person to notify when problems occur.
System Location	In the field, enter the location of the person that is identified as the system contact.
Apply To All Nodes	To apply the system configuration to all of the nodes in the cluster, check the check box.

Related Topics

- Understanding Simple Network Management Protocol, page 13-1
- Configuring SNMP V1/V2c, page 14-1
- Configuring SNMP V3, page 15-1

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.

INDEX

A

B

C

D

E

F

H

I

L

M

N

O

R

S

T

U

V