

## **Cisco Unified Presence Server Serviceability Administration Guide**

Release 1.0(3)

### **Corporate 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: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

*Cisco Unified Presence Server Serviceability Administration Guide*  
Copyright © 2006 Cisco Systems, Inc. All rights reserved.



## **Preface ix**

Purpose	ix
Audience	x
Organization	x
Related Documentation	xi
Conventions	xi
Obtaining Documentation	xii
Cisco.com	xii
Product Documentation DVD	xiii
Ordering Documentation	xiii
Documentation Feedback	xiii
Cisco Product Security Overview	xiii
Reporting Security Problems in Cisco Products	xiv
Obtaining Technical Assistance	xv
Cisco Technical Support & Documentation Website	xv
Submitting a Service Request	xv
Definitions of Service Request Severity	xvi
Obtaining Additional Publications and Information	xvi

---

## **PART 1**

### **Cisco Unified Presence Server Serviceability**

---

## **CHAPTER 1**

### **Introduction 1-1**

Cisco Unified Presence Server Serviceability Overview	1-1
Accessing Cisco Unified Presence Server Serviceability	1-2
Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	1-3
HTTPS Overview for Internet Explorer	1-3
Saving the Certificate to the Trusted Folder in Internet Explorer	1-3
Using Netscape to Save the Certificate to the Trusted Folder	1-4
Using the Cisco Unified Presence Server Serviceability Interface	1-5
Accessibility Features	1-6
Where to Find More Information	1-7
Related Topics	1-7

**PART 2**

**Service Management**

**CHAPTER 2**

**Managing Services 2-1**

- Activating and Deactivating Feature Services 2-1
- Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center 2-2
- Using a Command Line Interface to Start and Stop Services 2-3
- Related Topics 2-3

**PART 3**

**Alarm Configuration**

**CHAPTER 3**

**Alarm Configuration 3-1**

- Configuring or Updating an Alarm for a Service 3-1
- Alarm Destination Settings 3-2
- Alarm Event Level Settings 3-3
- Related Topics 3-4

**CHAPTER 4**

**Alarm Definitions 4-1**

- Viewing Alarm Definitions and Adding User-Defined Descriptions 4-1
- Alarm Definition Catalog Descriptions 4-2
- Related Topics 4-3

**PART 4**

**Trace Configuration**

**CHAPTER 5**

**Trace Configuration 5-1**

- Configuring Trace Parameters 5-1
- Trace Fields 5-3
- Debug Trace Level Settings 5-4
- Trace Output Settings Descriptions and Defaults 5-5
- Related Topics 5-6

**CHAPTER 6**

**Troubleshooting Trace Setting Configuration 6-1**

- Related Topics 6-2

**PART 5**

**Monitoring Tools Configuration**

**CHAPTER 7****Real-Time Monitoring Configuration 7-1**

- Installing the Real-Time Monitoring Tool (RTMT) 7-1
- Upgrading RTMT 7-2
- Uninstalling RTMT 7-3
- Using RTMT 7-3
- Configuring E-mail Notification 7-5
- Working with Configuration Profiles 7-5
  - Using the Default Configuration Profile 7-5
  - Adding Configuration Profiles 7-6
  - Restoring Profiles 7-6
  - Deleting Configuration Profiles 7-7
- Working with Predefined Objects 7-7
- Viewing/Monitoring a Predefined Object 7-7
- Working with Devices 7-10
  - Finding Specific Devices to Monitor 7-10
  - Viewing Phone Information 7-12
  - Viewing Device Properties 7-13
  - Configuring Polling Rate Performance Monitoring Counters 7-13
- Working with Categories 7-14
  - Adding a Category 7-14
  - Renaming a Category 7-14
  - Deleting a Category 7-15
- Where to Find More Information 7-15
- Related Topics 7-15

**CHAPTER 8****Alert Configuration in RTMT 8-1**

- Working with Alerts 8-1
- Setting Alert Properties 8-3
- Suspending Alerts on Cisco Unified Presence Server Nodes or the Cluster 8-5
- Configuring E-mails for Alert Notification 8-6
- Configuring Alert Actions 8-6
- Related Topics 8-6

**CHAPTER 9****Configuring and Using Performance Monitoring 9-1**

- Displaying Performance Counters 9-1
- Removing a Counter from the RTMT Performance Monitoring Pane 9-3
- Adding a Counter Instance 9-4

- Configuring Alert Notification for a Counter 9-4
- Zooming a Counter 9-7
- Displaying a Counter Description 9-8
- Configuring a Data Sample 9-9
- Viewing Counter Data 9-10
- Local Logging of Data from Perfmon Counters 9-10
  - Starting the Counter Logs 9-10
  - Stopping the Counter Logs 9-11
- Displaying Log Files on the Perfmon Log Viewer 9-11
- Zooming In and Out 9-13
- Related Topics 9-13

**CHAPTER 10**

- Trace Collection and Log Central in RTMT 10-1**
  - Importing Certificates 10-2
  - Displaying Trace & Log Central Options in RTMT 10-2
  - Collecting Traces 10-3
  - Using the Query Wizard 10-5
  - Scheduling Trace Collection 10-9
  - Viewing Trace Collection Status and Deleting Scheduled Collections 10-12
  - Collecting a Crash Dump 10-12
  - Using Local Browse 10-14
  - Using Remote Browse 10-15
  - Using Q931 Translator 10-17
  - Displaying QRT Report Information 10-18
  - Using Real Time Trace 10-19
    - View Real Time Data 10-19
    - Monitor User Event 10-20
  - Updating the Trace Configuration Setting for RTMT 10-22
  - Related Topics 10-22

**CHAPTER 11**

- Using SysLog Viewer in RTMT 11-1**
  - Related Topics 11-2

**CHAPTER 12**

- Using Plug-ins 12-1**
  - Related Topics 12-1

---

<b>CHAPTER 13</b>	<b>Log Partition Monitoring Configuration</b>	<b>13-1</b>
	Enabling Log Partition Monitoring	13-1
	Configuring Log Partition Monitoring	13-1
	Related Topics	13-2
<b>PART 6</b>	<b>Reporting Tools Configuration</b>	
<b>CHAPTER 14</b>	<b>Serviceability Reports Archive Configuration</b>	<b>14-5</b>
	Related Topics	14-6
<b>PART 7</b>	<b>SNMP Configuration</b>	
<b>CHAPTER 15</b>	<b>SNMP V1/V2c Configuration</b>	<b>15-1</b>
	SNMP Community String Configuration	15-1
	SNMP Notification Destination	15-3
	SNMP Notification Destination Configuration for V1/V2c	15-3
	Related Topics	15-4
<b>CHAPTER 16</b>	<b>SNMP V3 Configuration</b>	<b>16-1</b>
	SNMP User Configuration	16-1
	SNMP Notification Destination Configuration for V3	16-3
	Related Topics	16-4
<b>CHAPTER 17</b>	<b>MIB2 System Group Configuration</b>	<b>17-1</b>
	Related Topics	17-2
<b>INDEX</b>		







# Preface

---

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

The preface covers these topics:

- [Purpose, page vii](#)
- [Audience, page vii](#)
- [Organization, page viii](#)
- [Related Documentation, page ix](#)
- [Conventions, page ix](#)
- [Obtaining Documentation, page x](#)
- [Documentation Feedback, page xi](#)
- [Cisco Product Security Overview, page xi](#)
- [Product Alerts and Field Notices, page xii](#)
- [Obtaining Technical Assistance, page xiii](#)
- [Obtaining Additional Publications and Information, page xiv](#)

## Purpose

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

## Audience

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

# Organization

The following table shows how this guide is organized:

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

Chapter	Description
<a href="#">Chapter 16, “SNMP V3 Configuration”</a>	Provides procedures for configuring SNMP version 3.
<a href="#">Chapter 17, “MIB2 System Group Configuration”</a>	Provides procedures for configuring the system contact and system location objects for the MIB-II system group.

## Related Documentation

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

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/<release #>/doc\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm)

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands and keywords are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	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 <code>screen font</code> .
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	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

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

## Cisco Product Security Overview

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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

---

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



### Tip

#### Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411  
Australia: 1 800 805 227  
EMEA: +32 2 704 55 55  
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>



- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>





## **PART 1**

# **Cisco Unified Presence Server Serviceability**







## Introduction

---

This chapter comprises the following topics:

- [Cisco Unified Presence Server Serviceability Overview, page 1-1](#)
- [Accessing Cisco Unified Presence Server Serviceability, page 1-1](#)
- [Using Hypertext Transfer Protocol over Secure Sockets Layer \(HTTPS\), page 1-2](#)
- [Using the Cisco Unified Presence Server Serviceability Interface, page 1-5](#)
- [Accessibility Features, page 1-6](#)
- [Where to Find More Information, page 1-7](#)

## Cisco Unified Presence Server Serviceability Overview

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

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

## Accessing Cisco Unified Presence Server Serviceability

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

## Procedure

- Step 1** By using Netscape 7.1 (or later) or Internet Explorer 6.0 (or later), browse into the Cisco Unified Presence Server 1.0 server where Cisco Unified Presence Server Serviceability service runs.



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

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

- Step 2** Click the **Cisco Unified Presence Server Administration** link.
- Step 3** If the system prompts you about certificates, see the “[Using Hypertext Transfer Protocol over Secure Sockets Layer \(HTTPS\)](#)” section on page 1-2.
- Step 4** The first time that the system prompts you for a user name and password, enter **CCMAadministrator** for the username and the application user password that you specified during installation for the password.



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

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



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

## Additional Information

See the [Related Topics](#), page 1-7.

# Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

This section contains information on the following topics:

- [HTTPS Overview for Internet Explorer](#), page 1-3
- [Saving the Certificate to the Trusted Folder in Internet Explorer](#), page 1-3

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

## HTTPS Overview for Internet Explorer

The first time that you (or a user) accesses Cisco Unified Presence Server Administration or other Cisco Unified Presence Server SSL-enabled virtual directories after the Cisco Unified Presence Server 1.0 installation/upgrade, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must perform one of the following tasks:

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



### Note

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

### Additional Information

See the [Related Topics, page 1-7](#).

## Saving the Certificate to the Trusted Folder in Internet Explorer

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

### Procedure

- Step 1** Browse to the application on the Tomcat web server.
- Step 2** When the Security Alert dialog box displays, click **View Certificate**.
- Step 3** In the Certificate pane, click **Install Certificate**.
- Step 4** Click **Next**.
- Step 5** Click the **Place all certificates in the following store** radio button; click **Browse**.
- Step 6** Browse to **Trusted Root Certification Authorities**.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.

- Step 9** To install the certificate, click **Yes**.  
A message states that the import was successful. Click **OK**.
- Step 10** In the lower, right corner of the dialog box, click **OK**.
- Step 11** To trust the certificate, so you do not receive the dialog box again, click **Yes**.

---

#### Additional Information

See the [Related Topics, page 1-7](#).

## Using Netscape to Save the Certificate to the Trusted Folder

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



#### Tip

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

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

#### Procedure

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

The certificate authority dialog box displays.

- Step 2** Click one of the following radio buttons:
- Accept this certificate for this session
  - Do not accept this certificate and do not connect
  - Accept this certificate forever (until it expires)



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



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

- Step 3** Click **OK**.  
The Security Warning dialog box displays.
- Step 4** Click **OK**.

---

#### Additional Information

See the [Related Topics, page 1-7](#).









# Using the Cisco Unified Presence Server Serviceability Interface







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

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

**Table 1-1** *Icons in Cisco Unified Presence Server Serviceability*

Icon	Purpose
	Adds a new configuration
	
	Cancels the operation
	Clears the configuration that you specify
	Deletes the configuration that you choose
	Shows the online help for the configuration

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

Icon	Purpose
	Refreshes the window to display the latest configuration
	Restarts the service that you choose
	Saves the information that you entered
	Sets the default for the configuration
	Starts the service that you choose
	Stops the service that you choose

## Accessibility Features

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

Use [Table 1-2](#) as a guide for navigating the interface by using keyboard shortcuts.

**Table 1-2** *Navigation Shortcuts for Cisco Unified Presence Server Serviceability*

Keystroke	Action
Alt	Moves focus to the browser menu bar.
Enter	Chooses the item with focus (menu option, button, and so on.)
Alt, arrow keys	Moves between browser menus.
Spacebar	Toggles control; for example, checks and unchecks a check box.

**Table 1-2** *Navigation Shortcuts for Cisco Unified Presence Server Serviceability*

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

## Where to Find More Information

- *Cisco Unified Presence Server Administration Guide*

### Additional Information

See the [Related Topics](#), page 1-7.

## Related Topics

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





## **PART 2**

# **Service Management**







## Managing Services

---

This chapter contains information on the following topics:

- [Activating and Deactivating Feature Services, page 2-1](#)
- [Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center, page 2-2](#)
- [Using a Command Line Interface to Start and Stop Services, page 2-3](#)

### Activating and Deactivating Feature Services

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

Cisco Unified Presence Server allows you to activate and deactivate feature services. You may activate or deactivate as many services as you want at the same time. Some feature services depend on other services, and the dependent services get activated before the feature service activates.

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

#### Procedure

---

- Step 1** Choose **Tools > Service Activation**.
- The Service Activation window displays.
- Step 2** From the Server drop-down list box, choose the server.
- The window displays the service names for the server that you chose and the activation status of the services.
- Step 3** Click the **Set Default** button or activate the services that you want to use by checking the check box next to the service that you want to activate.
- Step 4** After you finish making the appropriate changes, click **Save**.



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

---

**Additional Information**

See the [Related Topics, page 2-3](#).

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

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

**Note**

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

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

**Procedure**

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

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

**Tip**

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

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

**Step 2** From the Server drop-down list box, choose the server.

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

**Step 3** Perform one of the following tasks:

- Click the radio button next to the service that you want to start and click the **Start** button.  
The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to restart and click the **Restart** button.  
A message indicates that restarting may take a while. Click **OK**.
- Click the radio button next to the service that you want to stop and click the **Stop** button.  
The Status changes to reflect the updated status.
- To get the latest status of the services, click the **Refresh** button.



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

**Additional Information**

See the [Related Topics, page 2-3](#).

## Using a Command Line Interface to Start and Stop Services

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

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

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

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

**Tip**

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

---

**Additional Information**

See the [Related Topics, page 2-3](#).

## Related Topics

- [Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center, page 2-2](#)
- [Activating and Deactivating Feature Services, page 2-1](#)





## **PART 3**

# **Alarm Configuration**







## Alarm Configuration

---

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

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

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

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

This chapter contains the following topics:

- [Configuring or Updating an Alarm for a Service, page 3-1](#)
- [Alarm Destination Settings, page 3-2](#)
- [Alarm Event Level Settings, page 3-3](#)

## Configuring or Updating an Alarm for a Service

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



### Note

---

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

---

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

### Procedure

---

**Step 1** Choose **Alarm > Configuration**.

The Alarm Configuration window displays.

- Step 2** From the Server drop-down box, choose the server for which you want to configure the alarm.
- Step 3** From the Service drop-down box, choose the service for which you want to configure the alarm.



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

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

- Step 4** Check the check box or boxes for the desired alarm destination as described in [Table 3-1](#).
- Step 5** In the Alarm Event Level selection box, click the Down arrow.  
A list with event levels displays.
- Step 6** Click the desired alarm event level as described in [Table 3-2](#).
- Step 7** To apply the current settings for selected services to all nodes in a cluster, check the **Apply to all Nodes** check box.
- Step 8** To save your configuration, click the **Save** button.



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

#### Additional Information

See the [Related Topics, page 3-4](#).

## Alarm Destination Settings

[Table 3-1](#) describes the alarm destination settings.

**Table 3-1 Alarm Destinations**

Name	Destination description
Enable Alarm for Local Syslogs	<p>SysLog Viewer. The program logs Cisco Unified Presence Server errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Serviceability Real-Time Monitoring Tool.</p> <p>For information on viewing logs with the SysLog Viewer, see the <a href="#">“Using SysLog Viewer in RTMT”</a> section on page 11-1.</p>

**Table 3-1 Alarm Destinations (continued)**

Name	Destination description
Enable Alarm for Remote Syslogs	<p>Syslog file. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified Presence Server does not send the Syslog messages.</p> <p><b>Note</b> If you want to send the alarms to CiscoWorks 2000, specify the CiscoWorks 2000 server name.</p>
Enable Alarm for SDI Trace	<p>The SDI trace library.</p> <p>To log alarms in the SDI trace log file, check this check box, and check the Trace On check box in Trace Configuration window for the chosen service.</p> <p>For more information on by using the Trace Configuration window, see the <a href="#">“Configuring Trace Parameters”</a> section on page 5-1.</p>

**Additional Information**

See the [Related Topics, page 3-4](#).

## Alarm Event Level Settings

[Table 3-2](#) describes the alarm event level settings.

**Table 3-2 Alarm Event Levels**

Name	Description
Emergency	This level designates system as unusable.
Alert	This level indicates that immediate action is needed.
Critical	Cisco Unified Presence Server detects a critical condition.
Error	This level signifies an error condition exists.
Warning	This level indicates that a warning condition is detected.
Notice	This level designates a normal but significant condition.
Informational	This level designates information messages only.
Debug	This level designates detailed event information that Cisco TAC engineers use for debugging.

**Additional Information**

See the [Related Topics, page 3-4](#).

## Related Topics

- [Configuring or Updating an Alarm for a Service, page 3-1](#)
- [Alarm Destination Settings, page 3-2](#)
- [Alarm Event Level Settings, page 3-3](#)





## Alarm Definitions

---

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

This chapter contains the following topics:

- [Viewing Alarm Definitions and Adding User-Defined Descriptions, page 4-1](#)
- [Alarm Definition Catalog Descriptions, page 4-2](#)

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

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

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

## Viewing Alarm Definitions and Adding User-Defined Descriptions

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

### Procedure

---

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

The Alarm Message Definitions window displays.

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

**Step 3** Click the **Find** button.

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



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

- Step 4** In the list, click the hyperlink alarm definition for which you want alarm details. The Alarm Details window displays.
- Step 5** If you want to add information to the alarm, enter text in the User Defined Text box, and click the **Update** button.
- Step 6** To return to the Alarm Message Definitions window, choose **Back to Find/List Alarms** from the Related Links drop-down list box and click **Go**.

#### Additional Information

See the [Related Topics, page 4-3](#).

## Alarm Definition Catalog Descriptions

Table 4-1 contains the alarm definition catalog descriptions.

**Table 4-1 Alarm Definition Catalogs**

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

## Related Topics

- [Viewing Alarm Definitions and Adding User-Defined Descriptions, page 4-1](#)
- [Alarm Definition Catalog Descriptions, page 4-2](#)





## **PART 4**

### **Trace Configuration**







## Trace Configuration

---

The Trace Configuration window allows you to specify the parameters that you want to trace for troubleshooting Cisco Unified Presence Server problems. You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, and size of file). You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

After you have configured which information you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in the Real-Time Monitoring Tool (RTMT). For more information on collecting traces, see the [“Trace Collection and Log Central in RTMT” section on page 10-1](#).



### Note

---

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

---

This chapter contains the following topics:

- [Configuring Trace Parameters, page 5-1](#)
- [Debug Trace Level Settings, page 5-3](#)
- [Trace Output Settings Descriptions and Defaults, page 5-4](#)

## Configuring Trace Parameters

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

### Procedure

---

**Step 1** Choose **Trace > Configuration**.

The Trace Configuration window displays.

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

**Step 3** From the Service drop-down list box, choose the service for which you want to configure trace.



### Note

---

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

---

The trace parameters display for the service that you chose.



**Note** If you configured Troubleshooting Trace for this service, a message displays at the top of the window that indicates that Troubleshooting Traces have been set. The system disables all fields on the window except the Output Settings. To configure the Output Settings, go to [Step 9](#). To reset Troubleshooting trace, see the [“Troubleshooting Trace Setting Configuration”](#) section on [page 6-1](#).

- Step 4** If you want trace to apply to all Cisco Unified Presence Server servers in the cluster, check the **Apply to All Nodes** check box.
- Step 5** Check the **Trace On** check box.
- Step 6** From the Debug Trace Level drop-down list box, choose the level of information that you want traced as described in [“Debug Trace Level Settings”](#) section on [page 5-3](#).
- Step 7** Check the Trace Fields check box for the service that you chose; for example, Cisco UPS SIP Proxy Trace Fields.
- Step 8** If the service that you chose has multiple trace fields, such as the Cisco UPS SIP Proxy service, check the check boxes next the trace fields that you want to enable. For a description of the Cisco UPS SIP Proxy service trace filter setting, see [Table 5-1](#).
- Step 9** To limit the number and size of the trace files, specify the trace output setting. See [Table 5-3](#) for descriptions and default values.
- Step 10** To save your trace parameters configuration, click the **Save** button.

The changes to trace configuration take effect immediately for all services except Cisco Messaging Interface. The trace configuration changes for Cisco Messaging Interface take effect in 3 to 5 minutes.



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

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

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



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

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

**Additional Information**

See the [Related Topics](#), page 5-5.

## Debug Trace Level Settings

[Table 5-2](#) describes the debug trace level settings for services.

**Table 5-2 Debug Trace Levels for Services**

Level	Description
Arbitrary	Traces all Entry/Exit conditions plus low-level debugging information.  <b>Note</b> Do not use this trace level with the Cisco UPS Presence Engine service or the Cisco IP Voice Media Streaming Application service during normal operation.
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation.  Trace level that turns on all logging
Detailed	Traces all Arbitrary conditions plus detailed debugging information.  <b>Note</b> Do not use this trace level with the Cisco UPS Presence Engine service or the Cisco IP Voice Media Streaming Application service during normal operation.
Entry/Exit	Traces all Significant conditions plus entry and exit points of routines. Not all services use this trace level (for example, Cisco Presence Server does not).
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.

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

Level	Description
Fatal	Traces very severe error events that may cause the application to abort.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation.
Warn	Traces potentially harmful situations.

**Additional Information**

See the [Related Topics, page 5-5](#).

## Trace Output Settings Descriptions and Defaults

[Table 5-3](#) contains the trace log file descriptions and defaults.

**Caution**

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

**Table 5-3** *Trace Output Settings*

Field	Description
Maximum number of files	This field specifies the total number of trace files for a given service. Cisco Unified Presence Server automatically appends a sequence number to the file name to indicate which file it is; for example, esp000005. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum file size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

**Additional Information**

See the [Related Topics, page 5-5](#).

## Related Topics

- [Configuring Trace Parameters, page 5-1](#)
- [Trace Output Settings Descriptions and Defaults, page 5-4](#)
- [Debug Trace Level Settings, page 5-3](#)





## Troubleshooting Trace Setting Configuration

---

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



---

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

---

### Procedure

---

**Step 1** Choose **Trace > Troubleshooting Trace Settings**.

**Step 2** Do one of the following tasks:

- To set troubleshooting trace, check the check box of the service(s) from the list of services for each node. If you want to check all services on a particular node, check the **Check all Services for a Node** check box under that node. If you want to check all services for all nodes, check the **Check all Services for a Node** check box in the services list.

Then, click the **Apply Troubleshooting Traces** button.



---

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

---

- To restore the original trace settings for the services in the cluster, click **Reset Troubleshooting Traces**.



---

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

---

### Additional Information

See the [Related Topics](#), page 6-2.

## Related Topics

- [Trace Configuration, page 5-1](#)



## **PART 5**

# **Monitoring Tools Configuration**









## Real-Time Monitoring Configuration

---

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



### Note

---

Some options that are available in the current version of the Cisco Real-Time Monitoring Tool do not apply to Cisco Unified Presence Server, Release 1.0(3).

---

- [Installing the Real-Time Monitoring Tool \(RTMT\), page 7-1](#)
- [Upgrading RTMT, page 7-2](#)
- [Uninstalling RTMT, page 7-3](#)
- [Using RTMT, page 7-3](#)
- [Configuring E-mail Notification, page 7-5](#)
- [Working with Configuration Profiles, page 7-5](#)
- [Working with Predefined Objects, page 7-7](#)
- [Working with Devices, page 7-9](#)
- [Where to Find More Information, page 7-11](#)



### Tip

---

For information on alert, performance monitoring, trace collection, and syslog viewer configuration, see the “[Where to Find More Information](#)” section on page 7-11.

---

## Installing the Real-Time Monitoring Tool (RTMT)

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



### Note

---

If you have previously installed RTMT for use with a Cisco Unified CallManager server that is running Microsoft Windows, you must install RTMT for Cisco Unified Presence Server 1.0 in a different folder on your local computer.

---

To install the tool, perform the following procedure:

#### Procedure

- 
- Step 1** From Cisco Unified Presence Server Administration, choose **Application > Plugins**.
  - Step 2** Click the **Find** button.
  - Step 3** Click the **Download** link for the Cisco Unified Presence Server Real-Time Monitoring Tool.
  - Step 4** Download the executable to your preferred location.
  - Step 5** Double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file.  
The extraction process begins.
  - Step 6** In the RTMT welcome window, click **Next**.
  - Step 7** To accept the license agreement, click **Yes**.
  - Step 8** Choose the location where you want to install RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.
  - Step 9** To begin the installation, click **Next**.  
The Setup Status window displays. Do not click **Cancel**.
  - Step 10** To complete the installation, click **Finish**.
- 

#### Additional Information

See the [Related Topics, page 7-12](#).

## Upgrading RTMT

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



#### Tip

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

To upgrade RTMT, perform the following procedure:

#### Procedure

- 
- Step 1** From Cisco Unified Presence Server Administration, choose **Application > Plugins**.
  - Step 2** Click the **Find** button.
  - Step 3** If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Windows. If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Linux.

- Step 4** Download the executable to your preferred location.
- Step 5** Double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file.
- The extraction process begins.
- Step 6** In the RTMT welcome window, click **Next**.
- Step 7** Because you cannot change the installation location for upgrades, click **Next**.
- The Setup Status window displays; do not click Cancel.
- Step 8** In the Maintenance Complete window, click **Finish**.
- 

#### Additional Information

See the [Related Topics, page 7-12](#).

## Uninstalling RTMT

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

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

#### Additional Information

See the [Related Topics, page 7-12](#).

## Using RTMT

### Before You Begin

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

### Procedure

---

- Step 1** After you install the plug-in, perform one of the following tasks:
- From your Windows desktop, double-click the **Cisco Unified CallManager Real-Time Monitoring Tool** icon.
  - Choose **Start > Programs > Cisco CallManager Serviceability > Real-Time Monitoring Tool > Real-Time Monitoring Tool**.
- The Real-Time Monitoring Tool Login window displays.
- Step 2** In the Host IP Address field, enter either the IP address or host name of the first node.
- Step 3** In the User Name field, enter the CCMAAdministrator application user username; for example, the default username for this user equals **CCMAAdministrator**.

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



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

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

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

**Step 7** Click **OK**.

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

**Step 9** See the following list for tasks that you can perform in RTMT:

- To configure the mail server for e-mail alerts, see the “[Configuring E-mail Notification](#)” section on [page 7-5](#).
- To create configuration profiles, see the “[Adding Configuration Profiles](#)” section on [page 7-6](#).
- To monitor predefined objects, see the “[Working with Predefined Objects](#)” section on [page 7-7](#).
- To work with devices, see the “[Working with Devices](#)” section on [page 7-9](#).
- To work with Alerts, see the “[Alert Configuration in RTMT](#)” section on [page 8-1](#).
- To work with performance monitoring objects, see the “[Configuring and Using Performance Monitoring](#)” section on [page 9-1](#).
- To collect and view traces, see the “[Trace Collection and Log Central in RTMT](#)” section on [page 10-1](#).
- To use SysLog Viewer, see the “[Using SysLog Viewer in RTMT](#)” section on [page 11-1](#).
- To configure the trace setting for RTMT, choose **Edit > Trace Setting**. Click the radio button that applies.
- To hide the Quick Launch Channel, which is the pane that displays on the left side of the window, choose **Edit > Hide Quick Launch Channel**.  
To display the Quick Launch Channel after it is hidden, choose **Edit > Hide Quick Launch Channel**.
- To close a monitoring window, choose **Window > Close**. To close all monitoring windows that display, choose **Window > Close All Windows**.
- To access Cisco Unified Presence Server Administration or Cisco Unified Presence Server Serviceability from the RTMT window, choose **Application > CCMAAdmin webpage** (or **CCM Serviceability webpage**).
- To access the Serviceability Report Archive option from RTMT, choose **System > Report Archive**. If the Security Alert window displays, click **Yes**. Enter the administrative user name and password for the server; then, click **OK**.
- To determine the RTMT version that is installed, choose **Help > About**. The version information displays in the window. After you view the information, click **OK**.

- To access documentation for RTMT, choose **Help > Help Topics** (or **For this Window**). For additional information on RTMT or Cisco Unified Presence Server Serviceability, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified Presence Server Serviceability Administration Guide*.
- To monitor JVM information, click **System > JVM Information**. The JAVA heap memory usage displays in the window. Click **OK**.
- To log out of RTMT, choose **System > Log Off**. Performing this task logs off the current user, and the Real-Time Monitoring Tool Login window displays.
- To exit the application, choose **System > Exit**. Performing this task closes the application.

---

**Additional Information**

See the [Related Topics, page 7-12](#).

## Configuring E-mail Notification

To configure e-mail notification, perform the following procedure:

**Procedure**

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | In the Mail Server field, enter the e-mail recipient information. |
| <b>Step 2</b> | In the Port field, enter the port number of the mail server.      |
| <b>Step 3</b> | Click <b>OK</b> .   |
- 

**Additional Information**

See the [Related Topics, page 7-12](#).

## Working with Configuration Profiles

This section provides information on the following topics:

- [Using the Default Configuration Profile, page 7-5](#)
- [Adding Configuration Profiles, page 7-6](#)
- [Restoring Profiles, page 7-6](#)
- [Deleting Configuration Profiles, page 7-7](#)

### Using the Default Configuration Profile

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

See the [“Adding Configuration Profiles”](#) section on page 7-6 for information on how to create your own configuration profile.

**Additional Information**

See the [Related Topics](#), page 7-12.

## Adding Configuration Profiles

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

The following procedure describes how to create a profile.

**Procedure**

- 
- Step 1** Choose **System > Profile**.  
The Preferences dialog box displays.
- Step 2** Click **Save**.  
The Save Current Configuration dialog box displays.
- Step 3** In the Configuration name field, enter a name for this particular configuration profile.
- Step 4** In the Configuration description field, enter a description of this particular configuration profile.



---

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

---

The system creates the new configuration profile.

---

**Additional Information**

See the [Related Topics](#), page 7-12.

## Restoring Profiles

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

**Procedure**

- 
- Step 1** Choose **System > Profile**.  
The Preferences dialog box displays.
- Step 2** Click the profile that you want to restore.
- Step 3** Click **Restore**.

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

---

**Additional Information**

See the [Related Topics, page 7-12](#).

## Deleting Configuration Profiles

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

**Procedure**

- 
- Step 1** Choose **System > Profile**.  
The Preferences dialog box displays.
- Step 2** Click the profile that you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **Close**.
- 

**Additional Information**

See the [Related Topics, page 7-12](#).

## Working with Predefined Objects

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

This section provides information on the following topics:

- [Viewing/Monitoring a Predefined Object, page 7-7](#)
- [Working with Devices, page 7-9](#)

## Viewing/Monitoring a Predefined Object

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

**Procedure**

- 
- Step 1** To view or monitor a category, perform one of the following tasks:

- In the Quick Launch Channel, click the **View** tab. Then, click a category; for example, Summary, Server, Call Process, and so on. If an icon displays for the category, click the icon to display the information that you want to monitor.



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

- Depending on which category you want to display, choose one of the following options from [Table 7-1](#):

**Table 7-1** *Menu Path for Categories*

Category	Menu Path	Data that Displays
Summary	Monitor > Summary	<p><b>Note</b> Some options that are in in the current version of RTMT do not apply to Cisco Unified Presence Server.</p> <p>Displays memory usage and CPU usage</p>
Server	Monitor > Server > CPU Usage and Memory (or Process, Disk Usage, or Critical Services)	<ul style="list-style-type: none"> <li>• CPU Usage and Memory—Displays memory and CPU usage</li> <li>• Process—Displays the process name, process ID (PID) and percentage of CPU and memory that is used by the process, the resident and shared memory, and the Nice (level)</li> <li>• Disk Usage—Displays the percentage of disk usage per the largest partition in each host</li> <li>• Critical Services—Displays the services for a specific server</li> </ul>
Service	Monitor > Service > Cisco TFTP (or Heartbeat or Database Summary)	<ul style="list-style-type: none"> <li>• Cisco TFTP—Displays Cisco TFTP status for each Cisco Unified Presence Server in the cluster, including total TFTP requests, total TFTP requests found, and total TFTP requests aborted</li> <li>• Heartbeat—Displays heartbeat information for the Cisco Unified Presence Server, Cisco TFTP, and the Cisco Presence Server Attendant Console service</li> <li>• Database Summary—Displays summary information for the database on the Cisco Unified Presence Server, including connection requests that are queued in the database, connection requests that are queued in memory, total number of clients connected, and the number of device resets that are in the queue.</li> </ul>
Performance	Performance > Open Performance	<p>Displays perfmon counters.</p> <p>For more information on using perfmon counters, see the <a href="#">“Configuring and Using Performance Monitoring”</a> section on <a href="#">page 9-1</a>.</p>

**Step 2** Some categories allow you to choose a specific server or device type to monitor. To choose a specific server or device type to monitor, perform one of the following tasks in the panes that are listed:

- CPU and Memory Usage pane—To monitor CPU and memory usage for specific server, choose the server from the Host drop-down list box.
- Disk Usage pane—To monitor disk usage for a specific server, choose the server from the Disk Usage at Host drop-down list box.



- Critical Services pane—To monitor critical services for a specific server, choose the server from the Critical Services at Host drop-down list box.

**Note**

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

---

**Additional Information**

See the [Related Topics](#), page 7-12.

## Working with Devices

**Note**

The Device options that are in in the current version of RTMT do not apply to Cisco Unified Presence Server.

---

## Viewing Phone Information

**Note**

The Phone Information options that are in in the current version of RTMT do not apply to Cisco Unified Presence Server.

---

## Viewing Device Properties

**Note**

The Device Properties options that are in in the current version of RTMT do not apply to Cisco Unified Presence Server.

---

## Configuring Polling Rate Performance Monitoring Counters

**Note**

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

---

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

**Note**

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

The default value for devices equals 10 minutes.

Perform the following procedure to update the polling rate:

**Procedure**

- Step 1** Display the performance-monitoring counter in the RTMT monitoring pane.
- Step 2** Click the device and choose **Edit > Polling Rate**.
- Step 3** In the Polling Interval pane, specify the time that you want to use.
- Step 4** Click **OK**.

**Additional Information**

See the [Related Topics, page 7-12](#).

## Working with Categories

**Note**

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

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

## Adding a Category

To add a category, perform the following procedure:

**Procedure**

- Step 1** Display the Performance Monitoring or Devices tree hierarchy.
- Step 2** Choose **Edit > Add New Category**.
- Step 3** Enter the name of the category; click **OK**.

The category tab displays at the bottom of the window.

---

**Additional Information**

- See the [Related Topics, page 7-12](#).

## Renaming a Category

To rename a category, perform the following procedure:

**Procedure**

- 
- Step 1** Perform one of the following tasks:
- Right-click the category tab that you want to rename and choose **Rename Category**.
  - Click the category tab that you want to rename and choose **Edit > Rename Category**.
- Step 2** Enter the new name and click **OK**.
- The renamed category displays at the bottom of the window.
- 

**Additional Information**

- See the [Related Topics, page 7-12](#).

## Deleting a Category

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

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

**Additional Information**

See the [Related Topics, page 7-12](#).

## Where to Find More Information

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

**Additional Information**

See the [Related Topics, page 7-12](#).

## Related Topics

- [Adding a Category, page 7-10](#)
- [Renaming a Category, page 7-11](#)
- [Deleting a Category, page 7-11](#)
- [Configuring and Using Performance Monitoring, page 9-1](#)
- [Working with Devices, page 7-9](#)
- [Viewing Device Properties, page 7-9](#)
- [Viewing Phone Information, page 7-9](#)
- [Configuring Polling Rate Performance Monitoring Counters, page 7-9](#)
- [Using the Default Configuration Profile, page 7-5](#)
- [Restoring Profiles, page 7-6](#)
- [Using the Default Configuration Profile, page 7-5](#)
- [Deleting Configuration Profiles, page 7-7](#)
- [Adding Configuration Profiles, page 7-6](#)
- [Working with Configuration Profiles, page 7-5](#)
- [Working with Predefined Objects, page 7-7](#)
- [Alert Configuration in RTMT, page 8-1](#)
- [Configuring and Using Performance Monitoring, page 9-1](#)
- [Using SysLog Viewer in RTMT, page 11-1](#)
- [Installing the Real-Time Monitoring Tool \(RTMT\), page 7-1](#)
- [Uninstalling RTMT, page 7-3](#)
- [Upgrading RTMT, page 7-2](#)
- [Using RTMT, page 7-3](#)



## Alert Configuration in RTMT

---

RTMT comprises two kinds of alerts: preconfigured and user defined. You can configure both kinds of alerts, but you cannot delete preconfigured alerts. You can disable both preconfigured and user-defined alerts in RTMT.

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

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

This chapter provides information on the following topics:

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

## Working with Alerts

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

### Procedure

---

- Step 1** Perform one of the following tasks:
- In the Quick Launch Channel, click the **Tools** tab and then the **Alert** tab; click the **Alert Central** icon.
  - Choose **Tools > Alert > Alert Central**.
- The Alert Central monitoring window displays and shows the alert status and alert history of the alerts that RTMT generated for the Cisco Unified Presence Server cluster.
- Step 2** Perform one of the following tasks:
- To set alert properties, see the “[Setting Alert Properties](#)” section on page 8-2.
  - To suspend alerts on Cisco Unified Presence Server nodes, see the “[Suspending Alerts on Cisco Unified Presence Server Nodes or the Cluster](#)” section on page 8-5.

- To configure e-mails for alert notification, see the “[Configuring E-mails for Alert Notification](#)” section on page 8-5.
- To configure alert actions, see the “[Configuring Alert Actions](#)” section on page 8-6.
- To sort alert information in the Alert Status pane, click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or InSafeRange column.

You can sort alert history information by clicking the up/down arrow in the columns in the Alert History pane. To see alert history that is out of view in the pane, use the scroll bar on the right side of the Alert History pane.

- To enable, disable, or remove an alert, perform one of the following tasks:
  - From the Alert Status window, right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
  - Highlight the alert in the Alert Status window and choose **Tools > Alert > Disable/Enable** (or **Remove**) **Alert**.




---

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

---

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

After you clear an alert, it changes from red to black.

- To view alert details, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Alert Details**.
  - Highlight the alert in the Alert Status window and choose **Tools > Alert > Alert Details**.




---

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

---

#### Additional Information

See the [Related Topics](#), page 8-6.

## Setting Alert Properties

The following procedure describes how to set alert properties.

#### Procedure

- 
- Step 1** Display Alert Central, as described in the “[Working with Alerts](#)” section on page 8-1.

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

**Step 3** Perform one of the following tasks:

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



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

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

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

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

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

**Step 7** Click **Next**.

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

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

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

**Step 10** Click **Next**.

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

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

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

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

**Step 13** Click **Next**.

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

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

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

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

- a. Click **Add**.
- b. In the Name field, enter a name for the alert action.
- c. In the Description field, enter a description of the alert action.

- d. To add an e-mail recipient, click **Add**.
- e. In the Enter email/epage address field, enter an e-mail or e-page address of the recipient that you want to receive the alert action.
- f. Click **OK**.

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




---

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

---

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

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

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

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

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

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

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

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

- a. Click **Next**.
- b. In the Alert Properties: TCT Download window, check the Enable TCT Download check box.
- c. The SFTP Parameters Dialog window displays. Enter the IP address, a user name, password, port and download directory path where the trace will be saved. To ensure that you have connectivity with the SFTP server, click **Test Connection**. **If the connection test fails, your settings will not be saved.**
- d. To save your configuration, click **OK**.
- e. In the TCT Download Parameters window, enter the number and frequency of downloads. Setting the number and frequency of download will help you to limit the number of trace files that will be downloaded. The setting for polling provides the basis for the default setting for the frequency.




---

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

---




---

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

---

#### Additional Information

See the [Related Topics](#), page 8-6.



# Suspending Alerts on Cisco Unified Presence Server Nodes or the Cluster

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

## Procedure

---

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



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

---

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

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

**Step 4** Click **OK**.



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

---

## Additional Information

See the [Related Topics, page 8-6](#).

# Configuring E-mails for Alert Notification

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

## Procedure

---

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

The Mail Server Configuration window displays.

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

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

**Step 4** Click **OK**.

---

**Additional Information**

See the [Related Topics](#), page 8-6.

## Configuring Alert Actions

The following procedure describes how to configure new alert actions.

**Procedure**

- 
- Step 1** Display Alert Central, as described in the “[Working with Alerts](#)” section on page 8-1.
- Step 2** Choose **Alert > Config Alert Action**.
- Step 3** Perform [Step 17](#) through [Step 20](#) in the “[Setting Alert Properties](#)” section on page 8-2 to add, edit, or delete alert actions.
- 

**Additional Information**

See the [Related Topics](#), page 8-6.

## Related Topics

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



# Configuring and Using Performance Monitoring

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

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

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

This chapter contains information on the following topics:

- [Displaying Performance Counters, page 9-1](#)
- [Removing a Counter from the RTMT Performance Monitoring Pane, page 9-3](#)
- [Adding a Counter Instance, page 9-4](#)
- [Configuring Alert Notification for a Counter, page 9-4](#)
- [Zooming a Counter, page 9-7](#)
- [Displaying a Counter Description, page 9-8](#)
- [Configuring a Data Sample, page 9-8](#)
- [Viewing Counter Data, page 9-9](#)
- [Local Logging of Data from Perfmon Counters, page 9-10](#)
- [Displaying Log Files on the Perfmon Log Viewer, page 9-11](#)

## Displaying Performance Counters

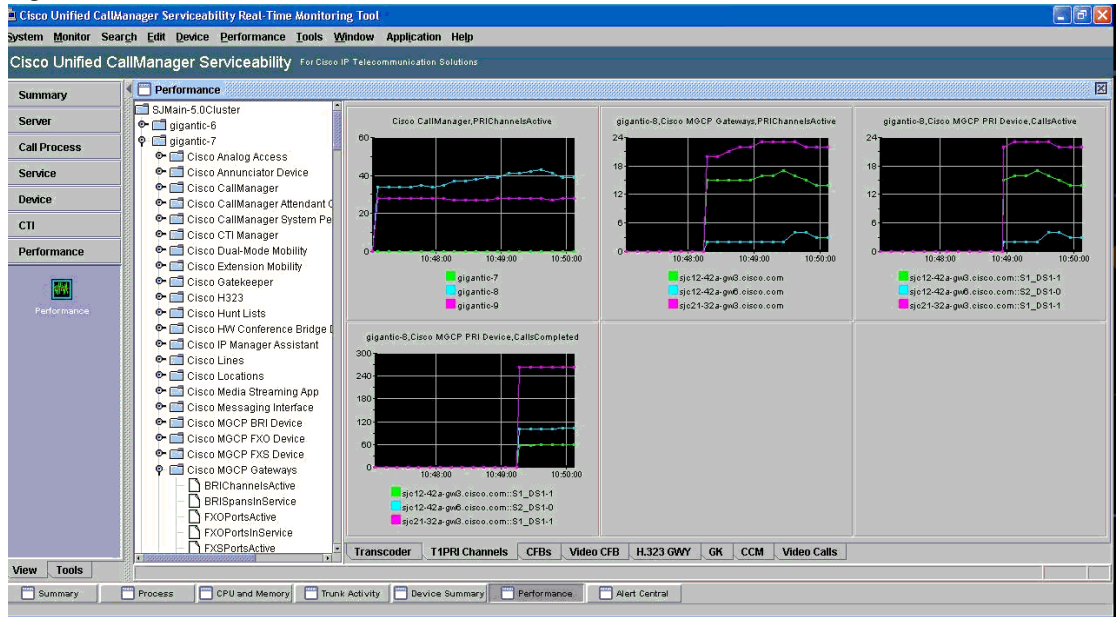
RTMT displays perfmon counters in chart or table format. The chart format, as shown in [Figure 9-1](#), displays the perfmon counter information by using line charts. For each category tab that you create, you can display up to six charts in the RTMT Perfmon Monitoring pane with up to three counters in one chart.



**Tip**

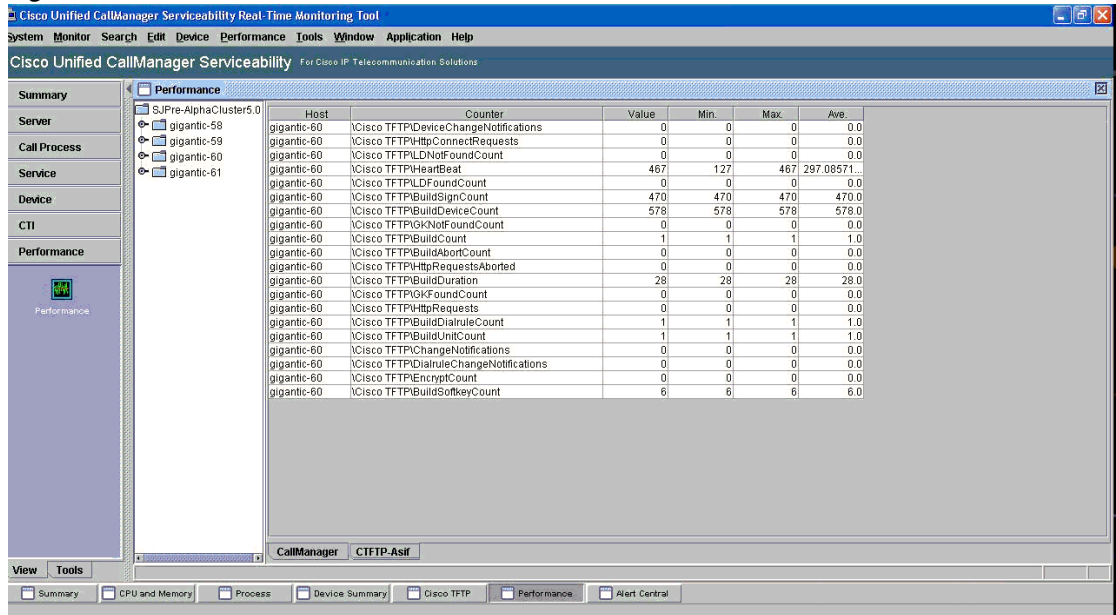
You can display up to three counters in one chart in the RTMT Perfmon Monitoring pane. To add another counter in a chart, click the counter and drag it to the RTMT Perfmon Monitoring pane. Repeat again to add up to three counters.

Figure 9-1 Performance Counters In a Chart Format



By default, RTMT displays perfmon counters in a chart format. You can also choose to display the perfmon counters in a table format, as shown in Figure 9-2. To display the perfmon counters in table format, you need to check the **Present Data in Table View** check box when you create a new category.

Figure 9-2 Performance Counters in a Table Format



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

### Procedure

- 
- Step 1** Perform one of the following tasks:
- In the Quick Launch Channel, click **Performance**; then, click the **Perfmon Monitoring** icon.
  - Choose **Performance > Open Performance Monitoring**.
- Step 2** Click the name of the server where you want to add a counter to monitor.  
The tree hierarchy expands and displays all the perfmon objects for the node.
- Step 3** To monitor a counter in table format, see [Step 4](#). To monitor a counter in chart format, see [Step 5](#).
- Step 4** To monitor a counter in table format, perform the following procedure.
- a. Choose **Edit > New Category**.
  - b. In the Enter Name field, enter a name for the tab.
  - c. To display the perfmon counters in table format, check the **Present Data in Table View** check box.
  - d. Click **OK**.
- A new tab with the name that you entered displays at the bottom of the pane.
- e. Click the file icon next to the object name that lists the counters that you want to monitor.




---

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

---

- Step 5** To monitor a counter in chart format, perform the following tasks:
- Click the file icon next to the object name that lists the counters that you want to monitor.  
A list of counters displays.
  - To display the counter information, either right-click the counter and click **Counter Monitoring**, double-click the counter, or drag and drop the counter into the RTMT Perfmon Monitoring pane.
- The counter chart displays in the RTMT Perfmon Monitoring pane.
- 

### Additional Information

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Removing a Counter from the RTMT Performance Monitoring Pane

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

Perform one of the following tasks:

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

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

**Additional Information**

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Adding a Counter Instance

To add a counter instance, perform the following procedure:

**Procedure**

- 
- Step 1** Display the performance monitoring counter, as described in the [“Displaying Performance Counters” section on page 9-1](#).
- Step 2** Perform one of the following tasks:
- Double-click the performance monitoring counter in the performance monitoring tree hierarchy.
  - Click the performance monitoring counter in the performance monitoring tree hierarchy and choose **Performance > Counter Instances**.
  - Right-click the performance monitoring counter in the performance monitoring tree hierarchy and choose **Counter Instances**.
- Step 3** In the Select Instance window, click the instance; then, click **Add**.
- The counter displays.
- 

**Additional Information**

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Configuring Alert Notification for a Counter

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

**Tip**

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

---

**Procedure**

- 
- Step 1** Display the performance counter, as described in the [“Displaying Performance Counters” section on page 9-1](#).
- Step 2** From the counter chart or table, right-click the counter for which you want to configure the alert notification, and choose **Alert/Threshold**.
- Step 3** Check the **Enable Alert** check box.
- Step 4** In the Severity drop-down list box, choose the severity level at which you want to be notified.
- Step 5** In the Description pane, enter a description of the alert.
- Step 6** Click **Next**.

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

**Table 9-1 Counter Alert Configuration Parameters**

Setting	Description
<b>Threshold Pane</b>	
Trigger alert when following conditions met (Over, Under)	<p>Check the check box and enter the value that applies.</p> <ul style="list-style-type: none"> <li>Over—Check this check box to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress.</li> <li>Under—Check this check box to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress.</li> </ul> <p><b>Tip</b> Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.</p>
<b>Value Calculated As Pane</b>	
Absolute, Delta, % Delta	<p>Click the radio button that applies.</p> <ul style="list-style-type: none"> <li>Absolute—Because some counter values are accumulative (for example, CallsAttempted or CallsCompleted), choose Absolute to display the data at its current status.</li> <li>Delta—Choose Delta to display the difference between the current counter value and the previous counter value.</li> <li>% Delta—Choose % Delta to display the counter performance changes in percentage.</li> </ul>
<b>Duration Pane</b>	
Trigger alert only when value constantly...; Trigger alert immediately	<ul style="list-style-type: none"> <li>Trigger alert only when value constantly...—If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent.</li> <li>Trigger alert immediately—If you want the alert notification to be sent immediately, click this radio button.</li> </ul>

Table 9-1 Counter Alert Configuration Parameters (continued)

Setting	Description
<b>Frequency Pane</b>	
Trigger alert on every poll; trigger up to...	<p>Click the radio button that applies.</p> <ul style="list-style-type: none"> <li>trigger alert on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button.</li> </ul> <p>If the calls in progress continue to go over or under the threshold, the system does not send another alert notification. When the threshold is normal (between 50 and 100 calls in progress), the system deactivates the alert notification; however, if the threshold goes over or under the threshold value again, the system reactivates alert notification.</p> <ul style="list-style-type: none"> <li>trigger up to...—If you want the alert notification to activate at certain intervals, click this radio button and enter the number of alerts that you want sent and the number of minutes within which you want them sent.</li> </ul>
<b>Schedule Pane</b>	
24-hours daily; start/stop	<p>Click the radio button that applies:</p> <ul style="list-style-type: none"> <li>24-hours daily—If you want the alert to be triggered 24 hours a day, click this radio button.</li> <li>start/stop—If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If the check box is checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.</li> </ul>

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

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

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



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

The Alert Action dialog box displays.

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

The Action Configuration dialog box displays.

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

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

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

The Input dialog box displays.



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

**Step 16** Click **OK**.

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



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

**Step 17** Click **OK**.

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



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

**Step 19** Click **Close**.

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

**Step 21** Click **Activate**.

#### Additional Information

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Zooming a Counter

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

#### Procedure

**Step 1** Perform one of the following tasks:

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

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

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

#### Additional Information

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Displaying a Counter Description

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

### Procedure

- 
- Step 1** Perform one of the following tasks:
- In the Perfmon tree hierarchy, right-click the counter for which you want property information and choose **Counter Description**.
  - In the RTMT Performance Monitoring pane, click the counter and choose **Perfmon > Counter Description**.



**Tip** To display the counter description and to configure data-sampling parameters, see the [“Configuring a Data Sample” section on page 9-8](#).

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

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

### Additional Information

See the [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Configuring a Data Sample

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

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

### Procedure

- 
- Step 1** Display the counter, as described in the [“Displaying Performance Counters” section on page 9-1](#).
- Step 2** Perform one of the following tasks:
- Right-click the counter for which you want data sample information and choose **Monitoring Properties** if you are using chart format and **Properties** if you are using table format.
  - Click the counter for which you want data sample information and choose **Perfmon > Monitoring Properties**.

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

- Step 3** To configure the number of data samples for the counter, click the **Data Sample** tab.
- Step 4** From the No. of data samples drop-down list box, choose the number of samples (between 100 and 1000). The default specifies 100.
- Step 5** From the No. of data points shown on chart drop-down list box, choose the number of data points to display on the chart (between 10 and 50). The default specifies 20.
- Step 6** Click one parameter, as described in [Table 9-2](#).

**Table 9-2 Data Sample Parameters**

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

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

#### Additional Information

See [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

## Viewing Counter Data

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

#### Procedure

- Step 1** In the RTMT Perfmon Monitoring pane, right-click the counter chart for the counter for which you want to view data samples and choose **View All Data**.
- The counter chart displays all data that has been sampled. The green dots display close together, almost forming a solid line.
- Step 2** Right-click the counter that currently displays and choose **View Current**.
- The counter chart displays the last configured data samples that were collected. See the [“Configuring a Data Sample” section on page 9-8](#) procedure for configuring data samples.

#### Additional Information

See [•Choose Performance > Open Performance Log Viewer, page 9-11](#).

# Local Logging of Data from Perfmon Counters

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer. See [“Displaying Log Files on the Perfmon Log Viewer”](#) section on page 9-11.

## Starting the Counter Logs

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

### Procedure

- 
- Step 1** Display the performance monitoring counters, as described in the [“Displaying Performance Counters”](#) section on page 9-1.
  - Step 2** If you are displaying perfmon counters in the chart format, right-click the graph for which you want data sample information and choose **Start Counter(s) Logging**. If you want to log all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Start Counter(s) Logging**.

The Counter Logging Configuration dialog box displays.

- Step 3** In the Logger File Name field, enter a file name and choose OK.  
RTMT saves the CSV log files in the log folder in the .jrtmt directory under the user home directory. For example, in Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.

To limit the number and size of the files, specify the maximum file size and maximum number of files parameter in the trace output settings. See [“Configuring Trace Parameters”](#) section on page 5-1.

---

## Stopping the Counter Logs

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

### Procedure

- 
- Step 1** Display the performance monitoring counters, as described in the [“Displaying Performance Counters”](#) section on page 9-1.
  - Step 2** If you are displaying perfmon counters in the chart format, right-click the graph for which counter logging is started and choose **Stop Counter(s) Logging**. If you want to stop logging of all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Stop Counter(s) Logging**.
-

# Displaying Log Files on the Perfmon Log Viewer

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

The local perfmon logs consist of data from counters that you choose and store locally on your computer. For more information on how to choose the counters and how to start and stop local logging, see “[Local Logging of Data from Perfmon Counters](#)” section on page 9-10.

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

## Procedure

- 
- Step 1** Perform one of the following tasks:
- In the Quick Launch Channel, click **Performance**; then, click the **Performance Log Viewer**.
  - Choose **Performance > Open Performance Log Viewer**
- Step 2** Choose the type of perfmon logs that you want to view:
- For AMC or RisDC Perfmon Logs, perform the following steps:
    - a. Click on either AMC Perfmon Logs or Perfmon Logs and choose a node from the Select a node drop-down box.
    - b. Click **Open**.  
The File Selection Dialog Box displays.
    - c. Choose the file and Click **Open File**.  
The Select Counters Dialog Box displays.
    - d. Choose the counters that you want to display by checking the check box next to the counter.
    - e. Click **OK**.
  - For locally stored data, perform the following steps:
    - a. Click Local Perfmon Logs.
    - b. Click **Open**.  
The File Selection Dialog Box displays. RTMT saves the perfmon CSV log files in the log folder in the .jrtmt directory under the user home directory. In Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.
    - c. Browse to the file directory.
    - d. Choose the file that you are interested in viewing or enter the file name in the filename field.

e. Click **Open**.

The Select Counters Dialog Box displays.

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

g. Click **OK**.

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

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

**Tip**

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

**Table 9-3** Performance Log Viewer

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

## Zooming In and Out

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

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

## Related Topics

- [Displaying Performance Counters, page 9-1](#)
- [Removing a Counter from the RTMT Performance Monitoring Pane, page 9-3](#)
- [Configuring Alert Notification for a Counter, page 9-4](#)
- [Zooming a Counter, page 9-7](#)
- [Displaying a Counter Description, page 9-8](#)
- [Configuring a Data Sample, page 9-8](#)
- [Viewing Counter Data, page 9-9](#)

- [Local Logging of Data from Perfmon Counters, page 9-10](#)
- [Displaying Log Files on the Perfmon Log Viewer, page 9-11](#)







## Trace Collection and Log Central in RTMT

---

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



**Note**

---

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

---



**Note**

---

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

---



**Note**

---

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

---

This chapter contains information on the following topics:

- [Importing Certificates, page 10-2](#)
- [Displaying Trace & Log Central Options in RTMT, page 10-2](#)
- [Collecting Traces, page 10-3](#)
- [Using the Query Wizard, page 10-5](#)
- [Scheduling Trace Collection, page 10-9](#)
- [Viewing Trace Collection Status and Deleting Scheduled Collections, page 10-11](#)
- [Collecting a Crash Dump, page 10-12](#)
- [Using Local Browse, page 10-14](#)
- [Using Remote Browse, page 10-14](#)
- [Using Q931 Translator, page 10-16](#)
- [Displaying QRT Report Information, page 10-17](#)

- [Using Real Time Trace, page 10-17](#)
- [Updating the Trace Configuration Setting for RTMT, page 10-20](#)

## Importing Certificates

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

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

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

## Displaying Trace & Log Central Options in RTMT

Before you begin, make sure that you have imported the security certificates as described in the [“Importing Certificates” section on page 10-2](#).

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

- In the Quick Launch Channel, click the **Tools** tab; then, click **Trace** and the **Trace & Log Central** icon.
- Choose **Tools > Trace > Open Trace & Log Central**.



### Tip

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

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

- Collect traces for services, applications, and system logs on one or more servers in the cluster. See [“Collecting Traces” section on page 10-3](#)
- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use. See [“Using the Query Wizard” section on page 10-5](#)
- Schedule a recurring trace collection and download the trace files to an SFTP server on your network. See [“Scheduling Trace Collection” section on page 10-9](#)
- Collect a crash dump file for one or more servers on your network. See [“Collecting a Crash Dump” section on page 10-12](#).
- View the trace files that you have collected. See the [“Using Local Browse” section on page 10-14](#).
- View all of the trace files on the server. See the [“Using Remote Browse” section on page 10-14](#).
- View the current trace file that is being written on the server for each application. You can perform a specified action when a search string appears in the trace file. See [“Using Real Time Trace” section on page 10-17](#).

# Collecting Traces

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



---

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

---

If you want to collect trace files that contain search criteria that you specify or you want to use trace collection criteria that you saved for later use, see the [“Using the Query Wizard” section on page 10-5](#).

## Before You Begin

Perform one or more of the following tasks:

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

## Procedure

---

**Step 1** Display the Trace & Log Central options, as described in the [“Displaying Trace & Log Central Options in RTMT” section on page 10-2](#).

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

The Select Presence Server Services/Applications tab displays.



---

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

---

**Step 3** Perform one of the following tasks:

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



---

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

---



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

**Step 4** Click **Next**.

The Select System Logs tab displays.

**Step 5** Perform one of the following tasks:

- To collect all system logs for all servers in the cluster, check the **Select All Logs on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the IP address of the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply. For example, to collect CSA logs, check the Cisco Security Agent check box in the Select System Logs tab. To access user logs that provide information about users that are logging in and out, check the Security Logs check box in the Select System Logs tab.
- To continue the trace collection wizard without collecting traces for system logs, go to [Step 6](#).

**Step 6** Click **Next**.

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

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

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

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

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

- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

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

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

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

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



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

- Step 9** To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Server Serviceability\jrtmt\<server IP address>\<download time>.
- Step 10** To create a zip file of the trace files that you collect, choose the **Zip File** radio button. To download the trace files without zipping the files, choose the **Do Not Zip Files** radio button.
- Step 11** To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.
- Step 12** Click **Finish**.
- The window shows the progress of the trace collection. If you want to stop the trace collection, click **Cancel**.
- When the trace collection process is complete, the message “Completed downloading for node <IP address>” displays at the bottom of the window.
- Step 13** To view the trace files that you collected, you can use the Local Browse option of the trace collection feature. For more information, see the [“Using Local Browse” section on page 10-14](#).

#### Additional Information

See the [Related Topics, page 10-20](#).

## Using the Query Wizard

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

#### Before You Begin

Perform one or more of the following tasks:

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

#### Procedure

- Step 1** Display the Trace & Log Central options, as described in the [“Displaying Trace & Log Central Options in RTMT” section on page 10-2](#).

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



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

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

- Saved Query

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

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

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

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

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

- Create Query

**Step 4** Click **Next**.

The Select Cisco Presence Server Services/Applications tab displays.

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



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



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



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

**Step 6** Click **Next**.

**Step 7** In the Select System Logs tab, check all check boxes that apply.

**Tip**

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

**Step 8** Click **Next**.

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

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

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

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

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

- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

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

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

**Step 12** Choose one of the following options:

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

The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **OK** and continue with [Step 17](#).

- To save the query, click the **Save Query** button and continue with [Step 13](#).

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

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

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



---

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

---

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

**Step 14** Click **Finish**.

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

**Step 16** Do one of the following tasks:

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

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

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



---

**Tip** After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the [“Using Local Browse” section on page 10-14](#).

---

- To save the query, click **Save Query** and complete [Step 13](#) through [Step 15](#).
- 

#### Additional Information

See the [Related Topics, page 10-20](#).



# Scheduling Trace Collection

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

**Note**

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

**Before You Begin**

Perform one or more of the following tasks:

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

**Procedure**

**Step 1** Display the Trace & Log Central options, as described in the [“Displaying Trace & Log Central Options in RTMT” section on page 10-2](#).

**Step 2** In the tree hierarchy, double-click **Schedule Collection**.  
The Select Presence Server Services/Applications tab displays.

**Note**

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

**Step 3** Perform one of the following tasks:

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

**Note**

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




---

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

---

**Step 4** Click **Next**.

The System Logs tab displays.

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

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

**Step 6** Click **Next**.

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

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

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

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




---

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

---

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

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

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

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

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

**Step 15** Choose one or more of the following actions:

- Download Files
- Run Another Query
- Generate Syslog

**Step 16** Do one of the following:

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

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



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

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



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

**Step 19** Click **Finish**.

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



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

**Step 20** Click **OK**.

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



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

#### Additional Information

See the [Related Topics](#), page 10-20.

## Viewing Trace Collection Status and Deleting Scheduled Collections

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

**Procedure**

- 
- Step 1** Display the Trace & Log Central options, as described in the “[Displaying Trace & Log Central Options in RTMT](#)” section on page 10-2.
- Step 2** In the Quick Launch Channel, click the **Job Status** icon.
- Step 3** From the Select a Node drop-down list box, choose the server for which you want to view or delete trace collection events.
- This list of scheduled trace collections displays.
- Possible job types include Scheduled Job, OnDemand, RealTimeFileMon, and RealTimeFileSearch.
- Possible statuses include Pending, Terminated, Running, Cancel, and Terminated.
- Step 4** To delete a scheduled collection, choose the event that you want to delete and click **Delete**.




---

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

---

**Additional Information**

See the [Related Topics, page 10-20](#).

## Collecting a Crash Dump

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

**Procedure**

- 
- Step 1** Display the Trace & Log Central tree hierarchy, as described in “[Displaying Trace & Log Central Options in RTMT](#)” section on page 10-2.
- Step 2** Double-click **Collect Crash Dump**.




---

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

---

- Step 3** In the Select Core Files tab, check the Core Files check box for servers that apply.
- Step 4** Click **Next**.
- Step 5** In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:
- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

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

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

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

- **Relative Range**—Specify the amount of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

**Step 6** From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

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

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



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

**Step 7** To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies C:\Program Files\Cisco\Presence Server Serviceability\jrtmt\<server IP address>\<download time>.

**Step 8** To create a zip file of the crash dump files that you collect, choose the **Zip File** radio button. To download the crash dump files without zipping the files, choose the **Do Not Zip Files** radio button.



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

**Step 9** To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

**Step 10** Click **Finish**.

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



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

**Additional Information**

See the [Related Topics](#), page 10-20.

## Using Local Browse

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

**Note**

---

Do not use NotePad to view collected trace files.

---

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

**Before You Begin**

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

- “[Collecting Traces](#)” section on page 10-3
- “[Using the Query Wizard](#)” section on page 10-5
- “[Scheduling Trace Collection](#)” section on page 10-9

**Procedure**

- 
- Step 1** Display the Trace & Log Central options, as described in the “[Displaying Trace & Log Central Options in RTMT](#)” section on page 10-2.
- Step 2** Double-click **Local Browse**.
- Step 3** Browse to the directory where you stored the log file and choose the file that you want to view.
- Step 4** To display the results, double-click the file or click **Finish**.

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

---

**Additional Information**

See the [Related Topics](#), page 10-20.

## Using Remote Browse

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



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

**Before You Begin**

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

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

**Procedure**

- 
- Step 1** Display the Trace & Log Central options, as described in the “[Displaying Trace & Log Central Options in RTMT](#)” section on page 10-2.
- Step 2** Double-click **Remote Browse**.
- Step 3** Choose the appropriate radio button, and click **Next**. If you choose Trace Files, go to [Step 4](#). If you choose Crash Dump, go to [Step 8](#).
- Step 4** Perform one of the following tasks:
- To choose traces for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.
  - To choose traces for all services and applications on a particular server, check the check box next to the IP address of the server.
  - To choose traces for particular services or applications on particular servers, check the check boxes that apply.
  - To continue the remote browse wizard without choosing traces for services or applications, go to [Step 5](#).
-  **Note** The services that you have not activated also display, so you can choose traces for those services.
-  **Note** You can install some listed services/applications only on a particular node in the cluster. To choose traces for those services/applications, make sure that you choose traces from the server on which you have activated the service/application.
- 
- Step 5** Click **Next**.  
The System Logs tab displays.
- Step 6** Perform one of the following tasks:
- To choose all system logs for all servers in the cluster, check the **Select All Logs on all Servers** check box.
  - To choose traces for all system logs on a particular server, check the check box next to the IP address of the server.
  - To choose traces for particular system logs on particular servers, check the check boxes that apply.
  - To continue the remote browse wizard without collecting traces for system logs, go to [Step 9](#).
- Step 7** Go to [Step 9](#).
- Step 8** Perform one of the following tasks:
- To choose crash dump files for all services and applications for all servers in the cluster, check the **Select All Services on All Servers** check box.

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

**Step 9** Click **Finish**.

**Step 10** After the traces become available, a message displays. Click **Close**.

**Step 11** Perform one of the following tasks:

- To display the results, navigate to the file through the tree hierarchy. After the log file name displays in the pane on the right side of the window, double-click the file.



**Tip**

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

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

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



**Tip**

After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the [“Using Local Browse” section on page 10-14](#).

#### Additional Information

See the [Related Topics, page 10-20](#).

## Using Q931 Translator



**Note**

Cisco Unified Presence Server does not support the Q931 Translator.



# Displaying QRT Report Information

**Note**

Cisco Unified Presence Server does not support QRT report information.

## Using Real Time Trace

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

The real-time trace provides the following options:

- [View Real Time Data, page 10-17](#)
- [Monitor User Event, page 10-18](#)

## View Real Time Data

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

**Note**

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

### Procedure

**Step 1** Display the Trace & Log Central tree hierarchy, as described in “[Displaying Trace & Log Central Options in RTMT](#)” section on page 10-2.

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

**Note**

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

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

The Real Time Data wizard displays.

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

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

**Note**

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

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

- Step 6** Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear. Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.
- Step 7** Repeat this procedure to view data for additional services. You can view data for up to 10 services, 5 of which can exist on a single node. A message displays if you attempt to view data for too many services or too many services on a single node.
- Step 8** When you are done viewing the real time data, click **Close** on the generic log viewer.

---

#### Additional Information

See the [Related Topics, page 10-20](#).

## Monitor User Event

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

#### Before you Begin

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

#### Procedure

---

- Step 1** Display the Trace & Log Central tree hierarchy, as described in [“Displaying Trace & Log Central Options in RTMT” section on page 10-2](#).
- Step 2** Double-click **Real Time Trace**.



---

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

---

- Step 3** Double-click **Monitor User Event**.  
The Monitor User Event wizard displays.

- Step 4** Perform one of the following tasks:
- To view the monitoring events that you have already set up, choose the **View Configured Events** radio button, choose a server from the drop-down list box, and click **Finish**.  
The events configured for the server that you choose display.



---

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

---

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

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

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




---

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

---

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

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

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

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

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

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

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




---

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

---




---

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

---

**Step 10** Click **Finish**.

---

**Additional Information**

See the [Related Topics](#), page 10-20.

## Updating the Trace Configuration Setting for RTMT

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



**Tip**

---

The Error radio button equals the default setting.

---

**Additional Information**

See the [Related Topics](#), page 10-20.

## Related Topics

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



## Using SysLog Viewer in RTMT

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

### Procedure

- Step 1** Perform one of the following tasks:
- In the Quick Launch Channel, click the **Tools** tab; then, click **SysLog Viewer** and the **SysLog Viewer** icon.
  - Choose **Tools > SysLog Viewer > Open SysLog Viewer**.
- Step 2** From the Select a Node drop-down list box, choose the server where the logs that you want to view are stored.
- Step 3** Click the tab for the logs that you want to view.
- Step 4** After the log displays, double-click the log icon to list the file names in the same window.
- Step 5** To view the contents of the file at the bottom of the window, click the file name.
- Step 6** Click the entry that you want to view.
- Step 7** To view the complete syslog message, double-click the syslog message. You can also use the following buttons that are described in [Table 11-1](#) to view the syslog messages:



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



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



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

**Table 11-1 Syslog Viewer Buttons**

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

**Additional Information**

See the [Related Topics, page 11-2](#).

## Related Topics

- [Real-Time Monitoring Configuration, page 7-1](#)



## Using Plug-ins

---

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

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

### Procedure

---

- Step 1** Choose **Application > CCO Webpage**.
  - Step 2** The Login Prompt displays. Enter your Cisco.com user name and password and click OK.
  - Step 3** Download the file to your PC.
  - Step 4** To begin the installation, double-click the download file.
  - Step 5** Follow the installation instruction.
- 

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

### Procedure

---

- Step 1** Perform one of the following tasks:
  - In the Quick Launch Channel, click the **Tools** tab and then the **Plugins** tab; click the icon of the application in which you are interested.
  - Choose the plug-in that you want to launch under **Tools > Plugin**.

The application displays in the plugin window.

Refer to the application document for usage information.

---

## Related Topics

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







## Log Partition Monitoring Configuration

---

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

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

## Enabling Log Partition Monitoring

To enable Log Partition Monitoring, perform the following procedure:

### Procedure

- 
- Step 1** In Cisco Unified Presence Server Serviceability, choose **Tools > Control Center > Network Services**.
  - Step 2** From the Servers drop-down list box, choose the server where you want to monitor the disk usage.
  - Step 3** Under CCM Services, verify the status of the Cisco Log Partition Monitoring Tool (LPM).
  - Step 4** If the LPM is not running, click the radio button next to Cisco LPM and click the Start button
- 

## Configuring Log Partition Monitoring

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

### Additional Information

See the [Related Topics, page 13-2](#).

## Related Topics

- [Log Partition Monitoring](#), *Cisco Unified CallManager Serviceability System Guide*
- [Alert Configuration in RTMT](#), *Cisco Unified CallManager Serviceability System Guide*
- [Trace Collection and Log Central in RTMT](#), *Cisco Unified Presence Server Serviceability Administration Guide*



## **PART 6**

# **Reporting Tools Configuration**







## Serviceability Reports Archive Configuration

---

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

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

### Before you Begin

Activate the Cisco Serviceability Report service. Because the Serviceability Reporter service is CPU intensive, Cisco recommends that you activate the service on a non-callprocessing server.

### Procedure

---

- Step 1** Choose **Tools > Serviceability Reports Archive**.
- The Serviceability Reports Archive window displays the month and year for which the reports are available.
- Step 2** From the Month-Year group box, choose the month for which you want to display reports. The month and year that you chose displays.
- Step 3** To view reports, click the link that corresponds to the day for which RTMT generated reports. The report files for the day that you chose display.
- Step 4** To view a particular PDF report, click the link of the report that you want to view. A window opens and displays the PDF file of the report that you chose.



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

---

### Additional Information

See the [Related Topics, page 14-5](#).

## Related Topics

- [Real-Time Monitoring Configuration, page 7-1](#)

## ■ Related Topics

- [Real-Time Monitoring Tool](#), *Cisco Unified CallManager Serviceability System Guide*
- [Serviceability Reports Archive](#), *Cisco Unified CallManager Serviceability System Guide*



## **PART 7**

# **SNMP Configuration**









## SNMP V1/V2c Configuration

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

- [SNMP Community String Configuration, page 15-1](#)
- [SNMP Notification Destination Configuration for V1/V2c, page 15-3](#)



Tip

If you use SNMP version 3, see the “[SNMP V3 Configuration](#)” section on page 16-1.

## SNMP Community String Configuration

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 Presence Server system. Change the community string to limit access to the Cisco Unified Presence Server system. To add, modify, and delete community strings, access the SNMP Community String configuration window.

### Procedure

- Step 1** Choose **Snmip > V1/V2c Configuration > Community String**.
- Step 2** From the Server drop-down list box, choose the server for which you want to configure a community string.
- Step 3** Perform one of the following tasks:
  - To add a new community string, click the **Add New** button and go to [Step 4](#).
  - To modify an existing community string, click the name of the community string that you want to edit and go to [Step 5](#).
  - To delete a community string, check the check box next to the community string(s) that you want to delete and click **Delete Selected**. A message indicates that the system will delete notification entries that relate to this community string. To continue the deletion, click **OK** and then go to [Step 9](#).
- Step 4** In the Community String Name field, 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.

- Step 5** From the Host IP Addresses Information group box, indicate from which host you want to receive SNMP packets. Click one of the following options:
- To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.
  - To accept SNMP only from specified hosts, click the **Accept SNMP Packets only from these hosts** radio button. 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**.
- Step 6** From the Access Privileges 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.




---

**Note** To change the Cisco Unified Presence Server trap configuration parameters, you need to use a community with NotifyOnly or ReadWriteNotify privileges.

---

- Step 7** To apply the community string to all nodes in the cluster, check the **Apply To All Nodes** check box.
- Step 8** Click **Insert** to save a new community string or click **Save** to save changes to an existing community string.
- Step 9** 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 “[Managing Services](#)” section on page 2-1.

---

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, page 15-4](#).

## SNMP Notification Destination

Choose the appropriate topic:


- [SNMP Notification Destination Configuration for V1/V2c, page 15-3](#)

- [SNMP Notification Destination Configuration for V3, page 16-2](#)

## SNMP Notification Destination Configuration for V1/V2c

Perform the following procedure to configure the notification destination (trap/inform receiver) for V1/V2c.

### Procedure

- 
- Step 1** Choose **Snmp > V1/V2c Configuration > Notification Destination**.
- Step 2** From the Server drop-down list box, choose the server for which you want to configure notification destination.
- Step 3** Perform one of the following tasks:
- To add a new SNMP notification destination, click the **Add New** button and go to [Step 4](#).
  - To modify an existing SNMP notification destination, click the name of the SNMP notification destination that you want to edit and go to [Step 5](#).
  - To delete an SNMP notification destination, check the check box next to the SNMP notification destination(s) that you want to delete and click **Delete Selected**. Go to [Step 11](#).
- Step 4** From the Host IP Addresses 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.
- Step 5** In the Port Number field, enter the notification receiving port number on the destination server that receives SNMP packets.
- Step 6** From the SNMP Version Information Group 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, continue with [Step 8](#). If you choose V2C, continue with [Step 7](#).
- Step 7** From the Notification Type drop-down list box, choose the appropriate notification type.
- Step 8** From the Community String drop-down list box, choose the community name to be used in the notification messages that this host generates.
-  **Tip** 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** button to create a community string. For information on how to create a community string, see the [“SNMP Community String Configuration”](#) section on page 15-1.
- 
- Step 9** To apply the notification destination to all nodes in the cluster, check the **Apply To All Nodes** check box.
- Step 10** Click **Insert** to save a notification destination or click **Save** to save changes to an existing notification destination.
- Step 11** 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 [“Managing Services” section on page 2-1](#).

**Additional Information**

See the [Related Topics, page 15-4](#).

## Related Topics

- [SNMP Community String Configuration, page 15-1](#)
- [SNMP V3 Configuration, page 16-1](#)
- [MIB2 System Group Configuration, page 17-1](#)
- Simple Network Management Protocol, *Cisco Unified CallManager Serviceability System Guide*
- [SNMP Notification Destination Configuration for V1/V2c, page 15-3](#)



## SNMP V3 Configuration

---

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

- [SNMP User Configuration, page 16-1](#)
- [SNMP Notification Destination Configuration for V3, page 16-2](#)



**Tip**

---

If you use SNMP v1 or v2c, see the [“SNMP V1/V2c Configuration” section on page 15-1](#).

---

## SNMP User Configuration

Perform the following procedure to configure user(s) for SNMP.

### Procedure

---

- Step 1** Choose **Snmip > V3 Configuration > User**.
- Step 2** From the Server drop-down list box, choose the server where you want to provide access.
- Step 3** Perform one of the following tasks:
- To add a new SNMP user, click the **Add New** button and go to [Step 4](#).
  - To modify an existing SNMP user, click the name of the SNMP user that you want to edit and go to [Step 5](#).
  - To delete an SNMP user, check the check box next to the SNMP user(s) that you want to delete and click **Delete Selected**. Go to [Step 11](#).
- Step 4** In the User Name 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).

---

- Step 5** To require authentication, check the Authentication Required 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.

**Step 6** If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the Privacy Required 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.

**Step 7** From the Host IP Addresses Information group box, indicate the host from which you want to receive SNMP packets. Choose one of the following options:

- To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.
- To accept SNMP packets from specific hosts, click the **Accept SNMP Packets only from these hosts** 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 list box and click **Remove**.

**Step 8** From the Access Privileges drop-down list box, choose the appropriate access level.

**Step 9** To apply the user configuration to all of the nodes in the cluster, check the **Apply To All Nodes** check box.

**Step 10** Click **Insert** to save a new user, or click **Save** to save changes to an existing user.

**Step 11** A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.



**Tip** Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the “[Managing Services](#)” section on page 2-1.



**Note** To access this Cisco Unified Presence Server server with the user that you configure, make sure that you configure this user on the NMS with the appropriate authentication and privacy settings.

#### Additional Information

See the [Related Topics](#), page 16-4.

## SNMP Notification Destination Configuration for V3

Perform the following procedure to configure the trap/Inform receiver.

#### Procedure

**Step 1** Choose **Snmip > V3 Configuration > Notification Destination**.

- Step 2** From the Server drop-down list box, choose the server for which you want to configure notification destination.
- Step 3** Perform one of the following tasks:
- To add a new SNMP notification destination, click the **Add New** button and go to [Step 4](#).
  - To modify an existing SNMP notification destination, click the name of the SNMP notification destination that you want to edit and go to [Step 5](#).
  - To delete an SNMP notification destination, check the check box next to the SNMP notification destination(s) that you want to delete and click **Delete Selected**. Go to [Step 12](#).
- Step 4** From the Host IP Addresses drop-down list box, choose the Host IP address or choose Add New. If you chose Add New, enter the IP address.
- Step 5** In the Port Number field, enter the notification receiving port number on the destination server.
- Step 6** From the Notification Type drop-down list box, choose the appropriate notification type. If you choose Inform, go to [Step 7](#). If you choose Trap, go to [Step 8](#).



---

**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.

---

- Step 7** From the Remote SNMP Engine Id 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.
- Step 8** From the Security Level 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.
- Step 9** From the User Information group box, 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 “[SNMP User Configuration](#)” section on page 16-1.
  - To modify an existing user, check the user check box and click **Updated Select User**; then, see the “[SNMP User Configuration](#)” section on page 16-1.
  - To delete a user, check the check box of the user and click **Delete Selected User**.



---

**Note** The users that display vary depending on the security level that you chose from the previous step.

---

- Step 10** To apply the notification destination to all nodes in the cluster, check the **Apply To All Nodes** check box.
- Step 11** To save a notification destination, click **Insert**, or click **Save** to save changes to an existing notification destination.
- Step 12** A message indicates that changes will not take effect until you restart the SNMP master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.

**Tip**

---

Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service. For information on how to restart the service, see the [“Managing Services” section on page 2-1](#).

---

The SNMP v.3 Notification Destination window displays the destination IP address, port number, security model version, security name, level, and notification type.

---

**Additional Information**

See the [Related Topics, page 16-4](#).

## Related Topics

- [SNMP V1/V2c Configuration, page 15-1](#)
- [MIB2 System Group Configuration, page 17-1](#)
- [SNMP User Configuration, page 16-1](#)
- [SNMP Notification Destination Configuration for V3, page 16-2](#)
- Simple Network Management Protocol, *Cisco CallManager Serviceability System Guide*





## MIB2 System Group Configuration

Cisco Unified Presence Server 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.

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 Configuration > MIB2 System Group Configuration**.
- Step 2** From the Server drop-down list box, choose the server for which you want to configure contacts.
- Step 3** In the Contact field, enter a person to notify when problems occur.
- Step 4** In the System Location field, enter the location of the person that is identified as the system contact.
- Step 5** To apply the system configuration to all of the nodes in the cluster, check the **Apply To All Nodes** check box.
- Step 6** Click **Save**.  
A message indicates that changes will not take effect until you restart the SNMP master agent.
- Step 7** 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 Contact and System Location fields, click the **Clear** button. To delete the system configuration, click the **Clear** button and the **Save** button.

### Additional Information

See the [Related Topics, page 17-2](#).

## Related Topics

- Simple Network Management Protocol, *Cisco CallManager Serviceability System Guide*
- [SNMP V1/V2c Configuration, page 15-1](#)
- [SNMP V3 Configuration, page 16-1](#)



---

## A

accessibility features [1-6](#)

Alarm configuration, described [3-1](#)

Alarm definitions

catalog descriptions [4-2](#)

creating user-defined [4-1](#)

described [4-1](#)

searching and viewing

procedure [4-1](#)

searching for [4-1](#)

viewing [4-1](#)

Alarms

configuring, procedure [3-1](#)

destinations [3-2](#)

destination settings [3-2](#)

event levels [3-3](#)

event level settings [3-3](#)

Event Viewer [3-2](#)

SDI trace library [3-2](#)

SDL trace library [3-2](#)

Syslog [3-2](#)

updating, procedure [3-1](#)

alert central, accessing [8-1](#)

alert notification

configuring parameters for counter (table) [9-5](#)

e-mail for counter [9-4](#)

message [9-4](#)

schedule [9-4](#)

thresholds [9-4](#)

alert notification, configuring [8-6](#)

alerts

accessing alert central [8-1](#)

configuring actions [8-6](#)

configuring e-mail for [8-6](#)

setting properties [8-3](#)

suspending [8-5](#)

---

## C

category

adding [7-14](#)

deleting [7-15](#)

renaming [7-14](#)

Cisco Unified CallManager, service [5-1](#)

CLI

starting services [2-3](#)

stopping services [2-3](#)

community string [15-1](#)

configuration profile

adding [7-6](#)

deleting [7-7](#)

restoring [7-6](#)

using default [7-5](#)

Control Center

starting services [2-2](#)

stopping services [2-2](#)

viewing status [2-2](#)

conventions [xi](#)

counters

alert notification parameters (table) [9-5](#)

configuring alert notification for [9-4](#)

data sample, configuring [9-9](#)

data sample parameters (table) [9-9](#)

viewing data [9-10](#)

zooming [9-7](#)

CTI  
 finding CTI devices [7-10](#)

---

## D

data sample  
 configuring parameters (table) [9-9](#)

debug trace levels  
 defined [5-4](#)

document  
 audience [x](#)  
 conventions [xi](#)  
 organization [x](#)  
 purpose [ix](#)

documentation  
 related [xi](#)

---

## E

e-mail configuration  
 alerts [8-6](#)

error codes [1-5](#)

event levels for alarms [3-3](#)

---

## F

feature services  
 activating [2-1](#)  
 deactivating [2-1](#)  
 starting [2-2](#)  
 stopping [2-2](#)  
 viewing status [2-2](#)

---

## H

HTTPS  
 overview (IE) [1-3](#)  
 saving certificate to trusted folder (IE) [1-3](#)

saving certificate to trusted folder (Netscape) [1-4](#)

---

## I

informs  
 V1/V2 [15-3](#)  
 V3 [16-3](#)

---

## L

Log Partition Monitoring  
 configuring [12-1, 13-1](#)

---

## M

MIB2  
 configuring system group [17-1](#)

monitoring  
 CTI devices [7-10](#)  
 gateways [7-10](#)  
 H.323 devices [7-10](#)  
 hunt list [7-10](#)  
 media resources [7-10](#)  
 phones [7-10](#)  
 predefined objects [7-7](#)  
 services [7-7](#)  
 SIP trunk [7-10](#)  
 voice-mail devices [7-10](#)

---

## N

network services  
 starting [2-2](#)  
 stopping [2-2](#)  
 viewing status [2-2](#)

notification destination  
 V1/V2 [15-3](#)  
 V3 [16-3](#)

NT Event Viewer [3-2](#)

---

## O

organization [x](#)

overview

- accessing error codes [1-5](#)
- accessing interface [1-2](#)
- accessing online help [1-5](#)
- icons in interface (table) [1-5](#)
- serviceability [1-1](#)
- verifying version [1-5](#)

---

## P

performance counter

- adding a counter instance [9-4](#)
- removing [9-3](#)

performance counters

- displaying in chart format [9-1](#)
- displaying in table format [9-1](#)

performance monitoring

- configuring alert notification for counters [9-4](#)
- viewing counter data [9-10](#)

plugins

- accessing [12-1](#)
- downloading [12-1](#)

polling rate [7-13](#)

predefined objects

- monitoring [7-7](#)

---

## Q

Q931 Translator, using [10-17](#)

---

## R

Real-Time Monitoring Tool

alert notification

- configuring for a counter [9-4](#)

alerts

- accessing alert central [8-1](#)
- configuring alert actions [8-6](#)
- configuring e-mail for [8-6](#)
- setting properties [8-3](#)
- suspending [8-5](#)

category

- adding [7-14](#)
- deleting [7-15](#)
- renaming [7-14](#)

collecting a crash dump [10-12](#)

collecting traces [10-3](#)

collecting traces using the query wizard [10-5](#)

collecting traces using the schedule collection option [10-9](#)

configuration profile

- adding [7-6](#)
- deleting [7-7](#)
- restoring [7-6](#)
- using default [7-5](#)

counters

- data sample [9-9](#)
- displaying property description [9-8](#)
- viewing data [9-10](#)
- zooming [9-7](#)

data samples [9-9](#)

deleting scheduled collections [10-12](#)

displaying trace and log central options [10-2](#)

e-mail notification, configuring [7-5](#)

finding

- devices [7-10](#)

installing [7-1](#)

loading [7-3](#)

monitoring

- call processing [7-7](#)
- CTIManager [7-7](#)
- devices [7-7](#)

- predefined objects [7-7](#)
- server [7-7](#)
- services [7-7](#)
- summary [7-7](#)
- monitoring predefined objects [7-7](#)
- monitoring summary [7-7](#)
- polling rate, configuring [7-13](#)
- related topics for trace collection [10-22](#)
- SysLog Viewer [11-1](#)
- uninstalling [7-3](#)
- updating trace configuration settings [10-22](#)
- upgrading [7-2](#)
- using [7-3](#)
- using the real time trace option [10-19](#)
- using the real time trace option, monitor user event [10-20](#)
- using the real time trace option, view real time data [10-19](#)
- viewing
  - device properties [7-13](#)
  - phone information [7-12](#)
- viewing trace collection status [10-12](#)
- viewing trace files using the local browse option [10-14](#)
- viewing trace files using the remote browse option [10-15](#)
- zooming a counter [9-7](#)
- related documentation [xi](#)

---

## S

- security
  - HTTPS for IE [1-3](#)
  - HTTPS for Netscape [1-4](#)
- server authentication certificates
  - importing using the trace collection option [10-2](#)
- serviceability
  - accessing [1-2](#)
  - accessing error codes [1-5](#)
  - icons (table) [1-5](#)

- introduction [1-1](#)
- overview [1-1](#)
- verifying version [1-5](#)

### Serviceability Reports Archive

- configuration [14-5](#)

### service activation

- activating [2-1](#)
- deactivating [2-1](#)

### services

- activating [2-1](#)
- deactivating [2-1](#)
- monitoring [7-7](#)
- starting [2-2](#)
- stopping [2-2](#)
- viewing status [2-2](#)

### Simple Network Management Protocol

- configuring community string [15-1](#)
- configuring MIB2 system group [17-1](#)
- configuring user (V3) [16-1](#)
- informs (V1/V2) [15-3](#)
- notification destination (V1/V2) [15-3](#)
- notification destination (V3) [16-3](#)
- traps (V1/2) [15-3](#)

### SNMP

- configuring community string [15-1](#)
- configuring MIB2 system group [17-1](#)
- configuring user (V3) [16-1](#)
- informs (V1/V2) [15-3](#)
- notification destination (V1/V2) [15-3](#)
- notification destination (V3) [16-3](#)
- traps (V1/V2) [15-3](#)

### SysLog Viewer [11-1](#)

---

## T

### Trace

- collection
  - collecting crash dump option [10-12](#)
  - collecting files option [10-3](#)

- configuration, described [10-1](#)
- deleting scheduled collections [10-12](#)
- displaying options [10-2](#)
- list of topics [10-1](#)
- related topics [10-22](#)
- schedule collection option [10-9](#)
- using the local browse option [10-14](#)
- using the query wizard option [10-5](#)
- using the real time trace option [10-19](#)
- using the real time trace option, monitor user event [10-20](#)
- using the real time trace option, view real time data [10-19](#)
- using the remote browse option [10-15](#)
- viewing status [10-12](#)
- configuration
  - described [5-1](#)
  - list of topics [5-1](#)
- configuring [5-1](#)
- debug trace levels for services [5-4](#)
- debug trace levels for servlets [5-4](#)
- device name based trace monitoring [5-1](#)
- log files
  - output settings [5-5](#)
- traps
  - V1/V2 [15-3](#)
  - V3 [16-3](#)
- Troubleshooting Trace Setting
  - configuration [6-1](#)

---

## U

- user-defined alarm descriptions [4-1](#)

---

## Z

- zooming a counter [9-7](#)

