Cisco Unified Real-Time Monitoring Tool Administration Guide

Release 8.5(1)

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

Customer Order Number: OL-22519-01

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Unified Real-Time Monitoring Tool Administration Guide
Copyright © 2010 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xv

Purpose xv

Audience xvi

Organization xvi

Related Documentation xviii

Conventions xix

Obtaining Documentation, Obtaining Support, and Security Guidelines xx

Cisco Product Security Overview xx

Related Documentation xxi

PART 1 **Cisco Unified Real-Time Monitoring Tool Basics**

CHAPTER 1 **Understanding Cisco Unified Real-Time Monitoring Tool** 1-1

Services, Servlets, and Service Parameters on the Server 1-2

Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter) 1-3

Where to Find More Information 1-5

CHAPTER 2 **Installing and Configuring Cisco Unified Real-Time Monitoring Tool** 2-1

Installing RTMT 2-1

Uninstalling RTMT 2-3

Launching RTMT 2-3

Navigating RTMT 2-5

Working with Configuration Profiles 2-6

Using the Default Configuration Profile 2-7

Adding Configuration Profiles 2-7

Restoring Profiles 2-7

Deleting Configuration Profiles 2-8

Where to Find More Information 2-8

PART 2 **Performance Monitoring**

CHAPTER 3 **Understanding Performance Monitoring** 3-1

Using RTMT for Performance Monitoring 3-1

Understanding the Performance Counter Interface 3-2

Category Tabs 3-3

Sample Rate 3-3

Zoom Feature 3-3

Highlight Feature 3-4

Counter Properties 3-4

Alert Notification for Counters 3-5

Understanding Perfmon Logs 3-5

Understanding Troubleshooting Perfmon Data Logging 3-5

Where to Find More Information 3-12

CHAPTER 4 **Monitoring Predefined System Objects** 4-1

Predefined System Objects Overview 4-1

Viewing the System Summary 4-3

Monitoring Server Status 4-3

Understanding Server Logs 4-4

Where to Find More Information 4-5

CHAPTER 5 **Monitoring Predefined Cisco Unified Communications Manager Objects** 5-1

Predefined Cisco Unified Communications Manager Objects Overview 5-2

Viewing the Cisco Unified Communications Manager Summary 5-5

Monitoring Call-Processing Activity 5-6

Understanding Call-Processing Logs 5-7

Understanding Session Trace 5-8

Monitoring Services 5-13

Understanding Service Logs 5-13

Monitoring Devices 5-14

Understanding Device Logs 5-16

Working with Devices 5-17

Finding Specific Devices to Monitor 5-17

Viewing Phone Information 5-19

Viewing Device Properties 5-19

Configuring Polling Rate for Devices and Performance Monitoring Counters 5-20

Monitoring CTI Applications, Devices, and Lines 5-20

Working with CTI Applications, Devices, and Lines 5-21

Viewing CTI Manager Information 5-21
Finding CTI Applications to Monitor 5-21
Finding CTI Devices to Monitor 5-22
Finding CTI Lines to Monitor 5-23
Viewing Application Information 5-24
Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature 5-25
Monitoring Intercompany Media Services 5-27
Where to Find More Information 5-28

CHAPTER 6 **Working with Performance Queries** 6-1
Working with Categories 6-1
Adding a Category 6-2
Renaming a Category 6-2
Deleting a Category 6-3
Using Performance Queries to Add a Counter 6-3
Removing a Counter from the Performance Monitoring Pane 6-4
Adding a Counter Instance 6-5
Configuring Alert Notification for a Counter 6-5
Displaying a Counter Description 6-8
Configuring a Data Sample 6-9
Viewing Counter Data 6-10
Local Logging of Perfmon Counters Data 6-10
Starting the Counter Logs 6-10
Stopping the Counter Logs 6-11
Where to Find More Information 6-11

CHAPTER 7 **Viewing and Troubleshooting Perfmon Logs** 7-1
Viewing Perfmon Log Files 7-1
Viewing Log Files on the Performance Log Viewer 7-1
Zooming In and Out 7-3
Viewing the Perfmon Log Files with the Microsoft Performance Tool 7-3
Working with Troubleshooting Perfmon Data Logging 7-4
Configuring Troubleshooting Perfmon Data Logging 7-4
Troubleshooting Perfmon Data-Logging Configuration Settings 7-5
Where to Find More Information 7-6

CHAPTER 8 **Using Cisco Unity Connection Port Monitor** 8-1

Port Monitor Overview 8-1

Using Cisco Unity Connection Port Monitor 8-2

Where to Find More Information 8-2

PART 3 **Alerts**

CHAPTER 9 **Understanding Alerts** 9-1

Using RTMT for Alerts 9-1

Viewing Alerts 9-2

System Alerts 9-2

CallManager Alerts 9-3

Cisco Unity Connection Alerts 9-5

Alert Fields 9-5

Alert Action Configuration 9-7

Enabling Trace Download 9-8

Understanding Alert Logs 9-9

Log Partition Monitoring 9-9

Where to Find More Information 9-10

CHAPTER 10 **Working with Alerts** 10-1

Working with Alerts 10-1

Setting Alert Properties 10-3

Suspending Alerts 10-5

Configuring E-mails for Alert Notification 10-6

Configuring Alert Actions 10-6

Configuring a Global E-Mail List for Alert Notifications 10-7

Where to Find More Information 10-8

PART 4 **Tools for Traces, Logs, and Plug-Ins**

CHAPTER 11 **Working with Trace and Log Central** 11-1

Importing Certificates 11-2

Displaying Trace and Log Central Options in RTMT 11-2

Collecting Trace Files 11-3

Collecting Installation Logs 11-7

Using the Query Wizard 11-8
Scheduling Trace Collection 11-12
Viewing Trace Collection Status and Deleting Scheduled Collections 11-15
Collecting a Crash Dump 11-16
Collecting Audit Logs 11-19
Using Local Browse 11-22
Using Remote Browse 11-23
Displaying QRT Report Information 11-27
Using Real-Time Trace 11-28
View Real-Time Data 11-28
Monitor User Event 11-29
Updating the Trace Configuration Setting for RTMT 11-32
Log Compression 11-32
Where to Find More Information 11-33

CHAPTER 12 **Using SysLog Viewer** 12-1
Where to Find More Information 12-2

CHAPTER 13 **Using Plug-ins** 13-1
Where to Find More Information 13-2

PART 5 **Analysis Manager**

CHAPTER 14 **Understanding Cisco Unified Analysis Manager** 14-1
How the Unified Analysis Manager Works 14-1
Where to Find More Information 14-2

CHAPTER 15 **Installing and Configuring Cisco Unified Analysis Manager** 15-1
Installing Cisco Unified Real-Time Monitoring Tool 15-1
Uninstalling Cisco Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager 15-2
Launching Cisco Unified Analysis Manager 15-3
Configuring Cisco Unified Analysis Manager 15-4
Importing Configurations 15-4
Displaying Job Status 15-4
Uploading Configuration Files 15-5
Cisco Unified Analysis Manager Preferences 15-5
Configuring an FTP Server 15-6

Accessing FTP Server Options 15-6
Adding or Editing an FTP Server 15-6
Configuring a Mail Server 15-7
Adding or Editing a Mail Server and Recipients 15-7
Trace Collection Directory 15-8

CHAPTER 16 **Identifying and Adding Nodes to Cisco Unified Analysis Manager 16-1**
Managing Nodes 16-1
Node Summary 16-2
Adding or Editing a Node 16-2
Managing Groups 16-3
Adding or Editing a Group 16-3
Managing the Trace File Repositories 16-4
Adding or Editing a Trace File Repository 16-4
Managing the Call Record Repositories 16-5
Adding or Editing a Call Record Repository 16-5
Defining Trace Templates 16-6
Adding or Editing a Template 16-6

CHAPTER 17 **Using the Cisco Unified Analysis Manager Tools 17-1**
Analyze Call Path 17-1
Configuration Considerations for Analyze Call Path 17-2
Cisco Unified Communications Manager/Cisco Unified Communications Manager Business Edition 5000 17-2
Cisco Unified Contact Center Express 17-4
Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise 17-4
Cisco Unified Customer Voice Portal 17-5
Cisco Access Control Server and Cisco IOS Gateway 17-6
Call Definitions 17-7
Collecting Traces 17-7
Collect Traces Now 17-8
Schedule Trace Collection 17-8
Schedule Trace Settings and Collection 17-9
Setting Trace Levels 17-9
Viewing a Configuration 17-10

CHAPTER 18 **Cisco Unified Analysis Manager Troubleshooting and Limitations** 18-1

Cisco Unified Analysis Manager Limitations 18-1

Cisco Unified Analysis Manager Troubleshooting 18-2

PART 6 **Cisco Intercompany Media Engine**

CHAPTER 19 **Cisco Intercompany Media Engine** 19-1

Monitoring IME Service 19-1

Monitoring IME System Performance 19-2

PART 7 **Performance Counters and Alerts**

APPENDIX A **System Performance Objects and Counters** A-1

Cisco Tomcat Connector A-2

Cisco Tomcat JVM A-3

Cisco Tomcat Web Application A-4

Database Change Notification Client A-5

Database Change Notification Server A-6

Database Change Notification Subscription A-7

Database Local DSN A-7

DB User Host Information Counters A-7

Enterprise Replication DBSpace Monitors A-7

Enterprise Replication Perfmon Counters A-8

IP A-8

IP6 A-9

Memory A-10

Network Interface A-12

Number of Replicates Created and State of Replication A-13

Partition A-13

Process A-14

Processor A-16

System A-16

TCP A-17

Thread A-18

Where to Find More Information A-18

APPENDIX B **Performance Objects and Counters for Cisco Unified Communications Manager** B-1

Cisco Analog Access B-2
Cisco Annunciator Device B-3
Cisco Call Restriction B-3
Cisco CallManager B-4
Cisco CallManager System Performance B-12
Cisco CTIManager B-14
Cisco Dual-Mode Mobility B-15
Cisco Extension Mobility B-16
Cisco Gatekeeper B-17
Cisco H.323 B-17
Cisco Hunt Lists B-18
Cisco HW Conference Bridge Device B-19
Cisco IP Manager Assistant B-20
Cisco Lines B-20
Cisco Locations B-21
Cisco Media Streaming Application B-22
Cisco Messaging Interface B-25
Cisco MGCP BRI Device B-25
Cisco MGCP FXO Device B-26
Cisco MGCP FXS Device B-26
Cisco MGCP Gateways B-27
Cisco MGCP PRI Device B-28
Cisco MGCP T1 CAS Device B-28
Cisco Mobility Manager B-29
Cisco Music On Hold (MOH) Device B-30
Cisco MTP Device B-31
Cisco Phones B-31
Cisco Presence Feature B-32
Cisco QSIG Feature B-32
Cisco Signaling Performance B-33
Cisco SIP B-33
Cisco SIP Normalization B-34
Cisco SIP Stack B-41
Cisco SIP Station B-49

Cisco SW Conf Bridge Device B-51
Cisco TFTP Server B-51
Cisco Transcode Device B-55
Cisco Video Conference Bridge B-55
Cisco Web Dialer B-56
Cisco WSM Connector B-57
IME Client B-57
IME Client Instance B-59
Where to Find More Information B-59

APPENDIX C **Cisco Unity Connection Performance Objects and Counters** C-1
CUC Data Store C-2
CUC Data Store: Databases C-2
CUC Digital Notifications C-3
CUC Directory Services C-3
CUC Message Store C-3
CUC Message Store: Databases C-5
CUC Personal Call Transfer Rules C-5
CUC Phone System C-5
CUC Phone System: Ports C-8
CUC Replication C-8
CUC Replicator: Remote Connection Locations C-8
CUC Sessions: Calendar Access C-9
CUC Sessions: E-mail Access C-9
CUC Sessions: IMAP Server C-10
CUC Sessions: RSS C-11
CUC Sessions: SMTP Server C-11
CUC Sessions: SpeechView Processor C-12
CUC Sessions: TRaP C-12
CUC Sessions: TTS C-13
CUC Sessions: Unified Client C-13
CUC Sessions: Voice C-13
CUC Sessions: VUI C-15
CUC Sessions: Web C-15
CUC Sessions: Web E-mail Access C-16
Where to Find More Information C-16

APPENDIX D **Performance Objects and Counters for Cisco Intercompany Media Engine** D-1

IME Configuration Manager D-1

IME Server D-2

IME Server System Performance D-3

Where to Find More Information D-5

APPENDIX E **System Alert Descriptions and Default Configurations** E-1

AuthenticationFailed E-2

CiscoDRFFailure E-2

CoreDumpFileFound E-3

CpuPegging E-3

CriticalServiceDown E-4

HardwareFailure E-5

LogFileSearchStringFound E-5

LogPartitionHighWaterMarkExceeded E-6

LogPartitionLowWaterMarkExceeded E-6

LowActivePartitionAvailableDiskSpace E-7

LowAvailableVirtualMemory E-8

LowInactivePartitionAvailableDiskSpace E-8

LowSwapPartitionAvailableDiskSpace E-9

ServerDown E-9

SparePartitionHighWaterMarkExceeded E-10

SparePartitionLowWaterMarkExceeded E-11

SyslogSeverityMatchFound E-11

SyslogStringMatchFound E-12

SystemVersionMismatched E-13

TotalProcessesAndThreadsExceededThreshold E-13

APPENDIX F **CallManager Alert Descriptions and Default Configurations** F-1

CallProcessingNodeCpuPegging F-3

CDRAgentSendFileFailed F-3

CDRFileDeliveryFailed F-4

CDRHighWaterMarkExceeded F-5

CDRMaximumDiskSpaceExceeded F-5

CodeYellow F-6

DBChangeNotifyFailure F-7

DBReplicationFailure F-7
DDRBlockPrevention F-8
DDRDown F-9
ExcessiveVoiceQualityReports F-9
IMEDistributedCacheInactive F-10
IMEOverQuota F-10
IMEQualityAlert F-11
InsufficientFallbackIdentifiers F-12
IMEServiceStatus F-13
InvalidCredentials F-14
LowCallManagerHeartbeatRate F-14
LowTFTPServerHeartbeatRate F-15
MaliciousCallTrace F-16
MediaListExhausted F-16
MgcpDChannelOutOfService F-17
NumberOfRegisteredDevicesExceeded F-17
NumberOfRegisteredGatewaysDecreased F-18
NumberOfRegisteredGatewaysIncreased F-19
NumberOfRegisteredMediaDevicesDecreased F-19
NumberOfRegisteredMediaDevicesIncreased F-20
NumberOfRegisteredPhonesDropped F-20
RouteListExhausted F-21
SDLLinkOutOfService F-21
TCPSetupToIMEFailed F-22
TLSConnectionToIMEFailed F-23

APPENDIX G **Cisco Unity Connection Alert Descriptions and Default Configurations** G-1
NoConnectionToPeer G-1
AutoFailoverSucceeded G-2
AutoFailoverFailed G-3
AutoFailbackSucceeded G-4
AutoFailbackFailed G-4
SbrFailed (Split Brain Resolution Failed) G-5
DiskConsumptionCloseToCapacityThreshold G-6
DiskConsumptionExceedsCapacityThreshold G-6
LicenseExpirationWarning G-7

LicenseExpired G-8

APPENDIX H **Cisco Intercompany Media Engine Alert Descriptions and Default Configurations** H-1

BannedFromNetwork H-1

IMEDistributedCacheCertificateExpiring H-2

IMEDistributedCacheFailure H-3

IMESdlLinkOutOfService H-3

InvalidCertificate H-4

InvalidCredentials H-5

MessageOfTheDay H-5

SWUpdateRequired H-6

TicketPasswordChanged H-7

ValidationsPendingExceeded H-7

INDEX

Preface

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

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

For Cisco Unified Communications Manager:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

For Cisco Unified Communications Manager Business Edition 5000:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

For Cisco Unity Connection:

http://www.cisco.com/en/US/products/ps6509/tsd_products_support_series_home.html

The preface covers these topics:

- Purpose, page xv
- Audience, page xvi
- Organization, page xvi
- Related Documentation, page xviii
- Conventions, page xix
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xx
- Cisco Product Security Overview, page xx

Purpose

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

Use this book with the documentation for your configuration:

Cisco Unified Communications Manager	*Cisco Unified Communications Manager System Guide, Cisco Unified Communications Manager Administration Guide, Cisco Unified Serviceability Administration Guide*, *CDR Analysis and Reporting Administration Guide*, and *Cisco Unified Communications Manager Call Detail Records Administration Guide*
Cisco Unified Communications Manager Business Edition 5000	*Cisco Unified Communications Manager System Guide, Cisco Unified Communications Manager Administration Guide, Cisco Unified Serviceability Administration Guide*, *CDR Analysis and Reporting Administration Guide*, *Cisco Unified Communications Manager Call Detail Records Administration Guide*, *Cisco Unity Connection System Administration Guide*, and *Administration Guide for Cisco Unity Connection Serviceability*
Cisco Unity Connection	*Cisco Unity Connection System Administration Guide* and *Administration Guide for Cisco Unity Connection Serviceability*

These documents provide the following information:

- Instructions for administering Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, and Cisco Unity Connection.
- Descriptions of procedural tasks that you complete by using the administration interface.

Audience

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* provides information for network administrators who are responsible for managing and supporting Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, and Cisco Unity Connection. 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
Real-Time Monitoring Tool	
Chapter 1, "Understanding Cisco Unified Real-Time Monitoring Tool"	Provides a brief description of the Cisco Unified Real-Time Monitoring Tool (RTMT).

Chapter	Description
Chapter 2, "Installing and Configuring Cisco Unified Real-Time Monitoring Tool"	Provides procedures for installing, upgrading, and uninstalling RTMT. Also provides information on how to navigate within RTMT and how to configure profiles.
Performance Monitoring	
Chapter 3, "Understanding Performance Monitoring"	Provides an overview of performance counters.
Chapter 4, "Monitoring Predefined System Objects"	Provides information on working with predefined system objects.
Chapter 5, "Monitoring Predefined Cisco Unified Communications Manager Objects"	Provides information on working with predefined Cisco Unified Communications Manager objects.
Chapter 6, "Working with Performance Queries"	Provides procedures for working with performance monitors, including viewing performance counters and counter descriptions, and perfmon logs.
Chapter 7, "Viewing and Troubleshooting Perfmon Logs"	Provides information about how to download perfmon logs or view them locally.
Chapter 8, "Using Cisco Unity Connection Port Monitor"	Provides information on the Port Monitor for Cisco Unity Connection.
Alerts	
Chapter 9, "Understanding Alerts"	Provides an overview of alerts, including a description of preconfigured alerts. Describes fields that you use to configure alerts and alert actions.
Chapter 10, "Working with Alerts"	Provides procedures for working with Alerts.
Tools for Traces, Logs, and Plug-Ins	
Chapter 11, "Working with Trace and Log Central"	Provides information on configuring on-demand trace collection and crash dump files for system services as well as on viewing the trace files in the appropriate viewer.
Chapter 12, "Using SysLog Viewer"	Provides information on using the SysLog Viewer.
Chapter 13, "Using Plug-ins"	Provides information on installing and using plug-ins in the Real-Time Monitoring tool.
Analysis Manager	
Chapter 14, "Understanding Cisco Unified Analysis Manager"	Provides information on Cisco Unified Analysis Manager.
Chapter 15, "Installing and Configuring Cisco Unified Analysis Manager "	Provides steps and procedure to install and configure Analysis Manager.
Chapter 16, "Identifying and Adding Nodes to Cisco Unified Analysis Manager"	Provides information on identifying and adding nodes that the Analysis Manager can diagnose.
Chapter 17, "Using the Cisco Unified Analysis Manager Tools"	Provides information on the Analysis Manager tools that allow you to perform management tasks for specific devices and groups of devices.

Chapter	Description
Chapter 18, "Cisco Unified Analysis Manager Troubleshooting and Limitations"	Provides troubleshooting and limitations information of the Cisco Unified Analysis Manager.
Cisco Intercompany Media Engine	
Chapter 19, "Cisco Intercompany Media Engine"	Provides information on Cisco Intercompany Media Engine.
Appendixes: Performance Counter and Alerts Descriptions	
Appendix A, "System Performance Objects and Counters"	Provides a list of performance objects and their associated counters for the system
Appendix B, "Performance Objects and Counters for Cisco Unified Communications Manager"	Provides a complete list of performance objects and their associated counters. Provides tables with related information about Cisco Unified Communications Manager perfmon counters, the Cisco Unified Real-Time Monitoring Tool, and CCM_SNMP_MIB.
Appendix C, "Cisco Unity Connection Performance Objects and Counters"	Provides a list of performance objects and their associated counters for Cisco Unity Connection.
Appendix D, "Performance Objects and Counters for Cisco Intercompany Media Engine"	Provides a list of performance objects and their associated counters for Cisco Intercompany Media Engine.
Appendix E, "System Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of system alerts.
Appendix F, "CallManager Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of CallManager alerts.
Appendix G, "Cisco Unity Connection Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of Cisco Unity Connection alerts.
Appendix H, "Cisco Intercompany Media Engine Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of Cisco Intercompany Media Engine Alert.

Related Documentation

For additional documentation on Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager Documentation Guide* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

For additional documentation on Cisco Unified Communications Manager Business Edition 5000, refer to the *Cisco Unified Communications Manager Business Edition Documentation Guide* at the following URL:

http://www.cisco.com/en/US/products/ps7273/products_documentation_roadmaps_list.html

For additional documentation on Cisco Unity Connection, refer to the *Cisco Unity Connection Documentation Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html

Conventions

This document uses the following conventions:

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

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

Cisco Product Security Overview

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

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

Related Documentation

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

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

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

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

Cisco Unified Communications Manager Documentation Guide

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

PART 1

Cisco Unified Real-Time Monitoring Tool Basics

CHAPTER 1

Understanding Cisco Unified Real-Time Monitoring Tool

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

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

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

RTMT allows you to perform the following tasks:

- Monitor a set of predefined management objects that monitor the health of the system.
- Generate various alerts, in the form of e-mails, for objects when values go over/below user-configured thresholds.
- Collect and view traces in various default viewers that exist in RTMT.
- *Unified CM and Unified CM BE 5000 only:* Translate Q931 messages.
- View syslog messages in SysLog Viewer.
- Work with performance-monitoring counters.

This chapter contains information on the following topics:

- Services, Servlets, and Service Parameters on the Server, page 1-2
- Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter), page 1-3
- Where to Find More Information, page 1-5

Services, Servlets, and Service Parameters on the Server

To support the RTMT client, several services need to be active and running on the server. RTMT uses the following services/servlets:

- Cisco AMC service—This service starts up automatically after the installation and allows RTMT to retrieve real-time information from the server or from a server in a cluster (if applicable).

Caution *Unified CM clusters only:* You must configure a second server as the failover collector in Cisco Unified Communications Manager Administration, so RTMT can continue to retrieve information if the primary collector fails. Otherwise, RTMT cannot retrieve information if the primary collector has failed.

The following list comprises some Cisco AMC service parameters that are associated with RTMT:

  - Primary Collector
  - Failover Collector
  - Data Collection Enabled
  - Data Collection Polling Rate
  - Server Synchronization Period
  - RMI Registry Port Number
  - RMI Object Port Number
  - *Unified CM and Unified CM BE 5000 only:* Alert Manager Enabled
  - *Unified CM BE 5000 and Connection only:* AlertMgr Enabled
  - Logger Enabled
  - *Unified CM and Unified CM BE 5000 only:* Alarm Enabled
  - *Unified CM BE 5000 and Connection only:* PerfMon Log Deletion Age

Note For the latest list of parameters, go to the Service Parameters window of the Cisco Unified CM Administration interface; then, choose Cisco AMC service.

Note For information on these service parameters, see the service parameter Help.

- Cisco Communications Manager servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which supports the Cisco Unified Real-Time Monitoring Tool (RTMT), starts up automatically after the installation.
- Cisco RIS Data Collector (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Real-time Information Server (RIS) maintains real-time information such as performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Cisco Unified Real-Time Monitoring Tool (RTMT), SOAP applications, and AlertMgrCollector (AMC) to retrieve the information that is stored on the server.

- Cisco Tomcat Stats Servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the Command Line Interface. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.
- Cisco Trace Collection Servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Trace Collection Service (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Log Partition Monitoring Tool (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, monitors the disk usage of the log partition on a server.
- Cisco SOAP-Real-Time Service APIs (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco SOAP-Real-Time Service APIs, which start up automatically after the installation, allow you to collect real-time information for devices and CTI applications.
- Cisco SOAP-Performance Monitoring APIs (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, allows you to use performance monitoring counters for various applications through SOAP APIs.
- Cisco RTMT Reporter servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, allows you to publish reports for RTMT.
- Cisco Serviceability Reporter (in the Control Center—Feature Services window in Cisco Unified Serviceability)—The Cisco Serviceability Reporter service allows you to publish reports for RTMT.

Additional Information

See the "Related Topics" section on page 1-5.

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

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

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

Tip *Unified CM clusters only:* Although they require no configuration tasks to run, RTMT Collector and Alert Manager support redundancy. If the primary collector or manager fails for any reason, the secondary collector and manager perform the tasks until primary support becomes available. RTMT Collector, Alert Manager, and RTMT Reporter run on the first server to minimize call-processing interruptions.

The locally written log files appear in the primary collector server at cm/log/amc. For Cisco Unified Communications Manager clusters, the log files can exist on more than one server in the cluster because the primary collector changes in failover and fallback scenarios.

You can display log files, except an alert log file, by using the Performance log viewer in RTMT or by using the native Microsoft Performance viewer. For more information on using the Performance log viewer in RTMT, refer to "Where to Find More Information" section on page 6-11. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace and Log Central in RTMT. For more information on downloading log files by using the collect files option, refer to "Collecting Trace Files" section on page 11-3.

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

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

- Call Activity Status—Number of calls attempted and number of calls completed for each Cisco Unified Communications Manager, each gateway, trunk, and overall cluster (if applicable). Number of channels available, in-service for each gateway.
- Device Status—Number of registered phones, gateways, and trunks per each server and overall cluster (if applicable).
- Server Status—% CPU load,% memory used,% disk space used per server.
- Service Status —*(Unified CM and Unified CM BE 5000 only)* For each CTI Manager, number of opened devices and lines. For each TFTP server, number attempted and failed requests.
- Alert Status—Number of alerts per server. For Cisco Unified Communications Manager clusters, number of alerts per severity level for the cluster, including the top 10 alerts in the cluster.
- Performance Protection Report—Trend analysis information on default monitoring objects that allows you to track overall system health. The report includes information for the last 7 days for each server.

Tip The RTMT reports display in English only.

The following service parameters apply to RTMT report generation: RTMT Reporter Designated server, RTMT Report Generation Time, and RTMT Report Deletion Age. For information on these parameters, go to the service parameter Help for your configuration:

Cisco Unified Communications Manager	Choose Cisco Serviceability Reporter in the Service Parameter window in Cisco Unified Communications Manager Administration and click the ? button.

Cisco Unified Communications Manager Business Edition 5000	Choose Cisco Serviceability Reporter in the Service Parameter window in Cisco Unified Communications Manager Administration and click the ? button.
Connection	On the Service Parameters window, in the Service drop-down list box, click a service and click **Help > This Page**.

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

Additional Information

See the "Related Topics" section on page 1-5.

Where to Find More Information

Related Topics

- Services, Servlets, and Service Parameters on the Server, page 1-2
- Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter), page 1-3

CHAPTER 2

Installing and Configuring Cisco Unified Real-Time Monitoring Tool

You can install Cisco Unified Real-Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 98, Windows XP, Windows 2000, Windows Vista, or Linux with KDE and/or Gnome client.

Note RTMT requires at least 128 MB in memory to run on a Windows OS platform.

Note RTMT requires at least 300 MB of disk space to run on a Windows/Linux OS platform.

This chapter contains information on the following topics:

- Installing RTMT, page 2-1
- Uninstalling RTMT, page 2-3
- Launching RTMT, page 2-3
- Navigating RTMT, page 2-5
- Working with Configuration Profiles, page 2-6
- Where to Find More Information, page 2-8

Installing RTMT

A single copy of RTMT that is installed on your computer lets you monitor one server or one cluster at a time. For example, you can monitor either of the following entities:

- A Cisco Unified Communications Manager product on one server.
- A server on a cluster to monitor the health of the cluster.

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

Consider the following, before you install RTMT:

- On a client machine, you can install RTMT client downloaded from only one product type—Unified Communication Manager or Unified Presence or Unity Connection or Unified Contact Center Express. Installing RTMT client from different product types on the same client machine is not supported.
- The current RTMT download may not support earlier releases of Cisco Unified Communications Manager or Cisco Unity Connection. Some releases of Cisco Unified Communications Manager may require different versions of RTMT to be installed on your computer (one version per Cisco Unified Communications Manager release). Verify that the RTMT version that you install is compatible with the Cisco Unified Communications Manager that you are monitoring. If the RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and RTMT frame size, from the RTMT client that last exits.

To install the tool, perform the following procedure:

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

Note For information on installing RTMT on a Cisco Intercompany Media Engine server, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Procedure

Step 1 Go to the Plug-ins window of the administration interface for your configuration:

Cisco Unified Communications Manager	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Cisco Unified Communications Manager Business Edition 5000	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Unity Connection	From Cisco Unity Connection Administration, choose **System Settings > Plugins**.

Step 2 Click the **Find** button.

Step 3 To install the RTMT tool on a client that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified CM Real-Time Monitoring Tool-Windows.

To install the RTMT tool on a client that is running the Linux operating system, click the **Download** link for the Cisco Unified CM Real-Time Monitoring Tool-Linux.

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

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

The extraction process begins.

Step 6 To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**

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

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

Step 9 Choose the location where you want to install RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Default installation paths are:

- Windows—C:\Program Files\Cisco\Unified-Communications-Manager Serviceability\JRtmt
- Linux—/opt/ Cisco/Unified-Communications-Manager_Serviceability/JRtmt

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

The Setup Status window displays. Do not click Cancel.

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

Additional Information

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

Uninstalling RTMT

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

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

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

Note When you uninstall RTMT on a Windows Vista machine, the following User Account Control pop-up message displays: "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Additional Information

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

Launching RTMT

Caution *Unified CM clusters only:* You must configure a second server as the failover collector in Cisco Unified Communications Manager Administration, so RTMT can continue to retrieve information if the primary collector fails. Otherwise, RTMT cannot retrieve information if the primary collector has failed.

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

Note When you launch RTMT, log into the same product type from which you downloaded the RTMT client application. If you log into a different product type, RTMT will not launch or work properly.

Procedure

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

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

The Real-Time Monitoring Tool Login window displays.

Step 2 In the Host IP Address field, enter either the IP address or host name of the server or (if applicable) first server in a cluster.

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

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

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

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

Note The Trace and Log Central tool in RTMT uses the port number that you specify to communicate with all the nodes in a cluster. If your system uses port mapping and all Cisco CallManager nodes do not map to the same port number, then some RTMT tools can not connect to those nodes. The tools that will fail to connect include Trace and Log Central, Job Status, SyslogViewer, Perfmon Log Viewer, and FTP/SFTP Configuration.

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

Step 7 Click **OK**.

Step 8 When prompted, add the certificate store by clicking **Yes**.

Real-Time Monitoring Tool RTMT starts.

Creating an RTMT-Only User

Cisco Unified Communications Manager supports the creation of an RTMT user with restricted access to Cisco Unified Communications Manager Administration. You can create a user with a profile that is limited to Cisco Unified Communications Manager RTMT usage only. The user will have full access to RTMT but will not have permission to administer a Cisco Unified Communications Manager server.

You can create an RTMT user by adding a new application user in Cisco Unified Communications Manager Administration and adding the user to the predefined Standard RealtimeAndTraceCollection group.

For complete instructions on adding users and user groups, refer the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

Additional Information

- For complete instructions on configuring an application user, see the "Application User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*
- For information on adding an application user to a user group, see the "User Group Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*
- Also see the "Related Topics" section on page 2-8.

Navigating RTMT

The RTMT window comprises the following main components:

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

Note The RTMT menu option **File > Cisco Unified Reporting** lets you access Cisco Unified Reporting from RTMT. You can use the Cisco Unified Reporting application to snapshot Cisco Unified Communications Manager cluster data for inspection or troubleshooting. Refer to the *Cisco Unified Reporting Administration Guide* for more information.

  - System—Allows you to monitor system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view syslog messages.
  - Communications Manager—Allows you to view Cisco Unified Communications Manager summary information on the server; monitor call-processing information; and view and search for devices, monitor services, and CTI.
  - Unity Connection—Allows you to view the Port Monitor tool.
  - IME Service—Allows you monitor server and network activity of the Cisco Intercompany Media Engine server.
  - Edit—Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.
  - Window—Allows you to close a single RTMT window or all RTMT windows.

  - Application—Depending on your configuration, allows you to browse the applicable web pages for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unity Connection Administration, and Cisco Unity Connection Serviceability.
  - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—You can click this pane with tabs on the left side of the RTMT window to display information about the server or information about the applications. The tab contains groups of icons that you can click to monitor various objects.
- Monitor pane—Pane where monitoring results display.

Additional Information

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

Working with Configuration Profiles

You can use RTMT to connect to a server or to any server in a Cisco Unified Communications Manager cluster (if applicable). After you log in to a server, RTMT launches the monitoring module from the local cache or from a remote server when the local cache does not contain a monitoring module that matches the backend version.

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

Unified CM clusters only: Default profile also dynamically monitors all registered phones for all Cisco Unified Communications Manager servers in a cluster. If your cluster contains five configured Cisco Unified Communications Manager servers, CM-Default displays the registered phones for each server in the cluster, as well as calls in progress and active gateway ports and channels.

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

Note If you are running the RTMT client and monitoring performance counters during a Cisco Unified Communications Manager upgrade, the performance counters will not update during and after the upgrade. To continue monitoring performance counters accurately after the Cisco Unified Communications Manager upgrade completes, you must either reload the RTMT profile or restart the RTMT client.

This section provides information on the following topics:

- Using the Default Configuration Profile, page 2-7
- Adding Configuration Profiles, page 2-7
- Restoring Profiles, page 2-7
- Deleting Configuration Profiles, page 2-8

Using the Default Configuration Profile

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

Unified CM clusters only: Default monitors all registered phones dynamically in all the Cisco Unified Communications Manager servers in a cluster. If your cluster includes five Cisco Unified Communications Manager-configured servers, Default displays all registered phones for each server in the cluster, as well as calls in progress and active gateway ports and channels.

Adding Configuration Profiles

With RTMT, you can customize your monitoring window by monitoring different performance counters, then create your own configuration profiles, so you can restore these monitoring windows in a single step rather than opening each window again. You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

The following procedure describes how to create a profile.

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click **Save**.

The Save Current Configuration dialog box displays.

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

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

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

Note *Unified CM clusters only:* Profiles apply to all servers within a cluster, but the profile cannot be saved and applied to a different cluster.

The system creates the new configuration profile.

Restoring Profiles

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

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to restore.

Step 3 Click **Restore**.

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

Deleting Configuration Profiles

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

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Close**.

Additional Information

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

Where to Find More Information

Related Topics

- Installing RTMT, page 2-1
- Uninstalling RTMT, page 2-3
- Launching RTMT, page 2-3
- Navigating RTMT, page 2-5
- Working with Configuration Profiles, page 2-6

PART 2

Performance Monitoring

CHAPTER 3

Understanding Performance Monitoring

Cisco Unified Communications Manager and Cisco Unity Connection directly update Performance counters (called PerfMon counters). The counters contain simple, useful information on the system and devices on the system, such as number of registered phones, number of active calls, number of available conference bridge resources, and voice messaging port usage.

For Cisco Unified Communications Manager, the Cisco CallManager object contains most of the Cisco Unified Communications Manager performance counters, and these counters have only one instance. The instance-based counters that belong to the other objects can have zero or more instances. For example, if two phones are registered to Cisco Unified Communications Manager, two instances of each counter that belong to the Cisco phones object exist.

You can monitor the performance of the components of the system and the components for the application on the system by choosing the counters for any object by using RTMT. The counters for each object display when the folder expands.

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

This chapter contains information on the following topics:

- Using RTMT for Performance Monitoring, page 3-1
- Understanding the Performance Counter Interface, page 3-2
- Understanding Perfmon Logs, page 3-5
- Where to Find More Information, page 3-12

Using RTMT for Performance Monitoring

RTMT integrates with existing software for performance monitoring:

- RTMT integrates with the administration and serviceability software for both Cisco Unified Communications Manager and Cisco Unity Connection.
- RTMT displays performance information for all Cisco Unified Communications Manager and Connection components.

RTMT provides alert notifications for troubleshooting performance. It also periodically polls performance counter to display data for that counter. Refer to "Displaying a Counter Description" section on page 6-8 for examples on displaying perfmon counters in a chart or table format.

Performance monitoring allows you to perform the following tasks:

- *Unified CM and Unified CM BE 5000 only:* Monitor performance counters including all the Cisco Unified Communications Manager servers in a cluster (if applicable), TFTP servers, and database servers.
- Continuously monitor a set of preconfigured objects AND receive notification in the form of an e-mail message.
- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.
- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.
- Use performance queries to add a counter to monitor. See "Working with Performance Queries" section on page 6-1 for more information.

Understanding the Performance Counter Interface

RTMT contains ready-to-view, predefined performance counters. You can also select and add counters to monitor in RTMT.

- To view predefined system counters, see "Monitoring Predefined System Objects" section on page 4-1.
- To view predefined Cisco Unified Communications Manager counters, see "Monitoring Predefined Cisco Unified Communications Manager Objects" section on page 5-1.
- To add a counter to monitor, see "Working with Performance Queries" section on page 6-1.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. You can display a particular counter by double clicking the counter in the perfmon monitoring pane.

Attributes for predefined performance counters, such as format and category, remain fixed. You can define attributes for counters that you configure in RTMT. Because chart view represents the default, you configure the performance counters to display in table format when you create a category.

This section contains the following topics:

- Category Tabs, page 3-3
- Sample Rate, page 3-3
- Zoom Feature, page 3-3
- Highlight Feature, page 3-4
- Counter Properties, page 3-4
- Alert Notification for Counters, page 3-5

Category Tabs

A category comprises a group of monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. RTMT displays any categories that you access during a RTMT session in the bottom toolbar.

The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

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

Sample Rate

The application polls the counters, devices, and gateway ports to gather status information.

The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart. For more information on Service Parameters, refer to *Cisco Unified Communications Manager Administration Guide* or *Cisco Unity Connection System Administration Guide*.

In the RTMT monitoring pane, you configure the polling intervals for the applicable performance counters, devices, and gateway ports for each category tab that you create.

Note High-frequency polling rate affects the performance on the server. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default for both specifies 10 seconds.

Zoom Feature

To get a closer look at perfmon counters, you can zoom a perfmon monitor counter in the RTMT. See also Highlight Feature, page 3-4.

Procedure

Step 1 To zoom in a counter, perform one of the following tasks:

- To zoom predefined objects, such as System Summary, perform one of the following tasks:
  - Drag the mouse over the plot area in the counter to frame the data and release the mouse button. The counter zooms in the chart.
  - Click the counter. The counter zooms in.

- To zoom counters in the Performance pane, perform one of the following tasks (and resize the window, if necessary):
  - Double-click the counter that you want to zoom. The box with the counter appears highlighted and the Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.
  - Click the counter to select the counter to zoom. The box with the counter appears highlighted. Right-click the counter and select **Zoom Chart** or choose **System > Performance > Zoom Chart**. The Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

Step 2 To zoom out a counter, perform one of the following tasks:

- To zoom out predefined objects, such as System Summary, click the counter and press **Z** in the active counter to return the counter to original size.
- To zoom out counters in the Performance pane, click **OK** to close the Zoom window.

Highlight Feature

The highlight feature helps to distinguish hosts and counters when multiple nodes or counters display on color-coded graphs. This feature is active in the System Summary, CPU and Memory, Disk Usage, and Performance Log Viewer windows. See also "Zoom Feature" section on page 3-3.

Procedure

Step 1 To highlight charts and graphs, perform one of the following tasks:

- To highlight charts and graphs for predefined objects, such as System Summary, right-click in a plot area to highlight the nearest data series or point.
- To highlight charts and graphs in the performance log viewer, perform one of the following tasks
  - Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Highlight** to highlight the data series for that counter.
  - Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Change Color** to select a different color for the counter.

Step 2 To return a highlighted item to its original appearance in the Performance Log Viewer, select another item to highlight.

Counter Properties

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

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the

number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view all the data that a perfmon counter collected.

Additional Information

See the "Related Topics" section on page 3-12.

Alert Notification for Counters

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

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

Understanding Perfmon Logs

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

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer.

See "Viewing Perfmon Log Files" section on page 7-1 for more information.

Understanding Troubleshooting Perfmon Data Logging

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

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

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

- Enable and disable the trace filter for Troubleshooting perfmon data logging.

- Monitor the applicable set of predefined System, Cisco Unified Communications Manager, and Cisco Unity Connection performance objects and counters on each server.
- Log the monitored performance data in CSV file format on the server in the active log partition in the var/log/active/cm/log/ris/csv directory. The log file uses the following naming convention: PerfMon_<server>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv. Specify the polling rate. This rate specifies the rate at which performance data gets gathered and logged. You can configure the polling rate down to 5 seconds. Default polling rate equals 15 seconds.
- View the log file in graphical format by using the Microsoft Windows performance tool or by using the Performance Log viewer in the RTMT.
- Specify the maximum number of log files that will be stored on disk. Log files exceeding this limit get purged automatically by removal of the oldest log file. The default specifies 50 files.
- Specify the rollover criteria of the log file based on the maximum size of the file in megabytes. The default value specifies 5 MB.
- Collect the Cisco RIS Data Collector PerfMonLog log file by using the Trace & Log Central feature of the RTMT or Command Line Interface.

For more information on configuring Troubleshooting Perfmon Data Logging, see "Configuring Troubleshooting Perfmon Data Logging" section on page 7-4.

The troubleshooting perfmon data-logging feature collects information from the following counters within the following perfmon objects.

Refer to the System Performance Objects and Counters for a description of the system counters:

- Database Change Notification Server Object
  - Clients
  - CNProcessed
  - QueueDelay
  - QueuedRequestsInDB
  - QueuedRequestsInMemory
- Database Local DSN Object
  - CcmDbSpace_Used
  - CcmtempDbSpace_Used
  - CNDbSpace_Used
  - LocalDSN
  - RootDbSpace_Used
  - SharedMemory_Free
  - SharedMemory_Used
- Enterprise Replication DBSpace Monitors Object
  - ERDbSpace_Used
  - ERSBDbSpace_Used
- IP Object
  - In Receives
  - In HdrErrors

  - In UnknownProtos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- Memory Object
  - % Page Usage
  - % VM Used
  - % Mem Used
  - Buffers Kbytes
  - Cached Kbytes
  - Free Kbytes
  - Free Swap Kbytes
  - HighFree
  - HighTotal
  - Low Total
  - Low Free
  - Page Faults Per Sec
  - Page Major Faults Per Sec
  - Pages
  - Pages Input
  - Pages Input Per Sec
  - Pages Output
  - Pages Output Per Sec
  - SlabCache
  - SwapCached
  - Shared Kbytes
  - Total Kbytes
  - Total Swap Kbytes
  - Total VM Kbytes
  - Used Kbytes

  - Used Swap Kbytes
  - Used VM Kbytes
- Network Interface Object
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
- Number of Replicates Created and State of Replication Object
  - Replicate_State
- Partition Object
  - % CPU Time
  - %Used
  - Await Read Time
  - Await Time
  - Await Write Time
  - Queue Length
  - Read Bytes Per Sec
  - Total Mbytes
  - Used Mbytes
  - Write Bytes Per Sec
- Process Object
  - % Memory Usage
  - Data Stack Size
  - Nice
  - PID
  - STime
  - % CPU Time
  - Page Fault Count
  - Process Status
  - Shared Memory Size

  - VmData
  - VmRSS
  - VmSize
  - Thread Count
  - Total CPU Time Used
- Processor Object
  - Irq Percentage
  - Softirq Percentage
  - IOwait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time
- System Object
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes
  - Total Threads
  - Total CPU Time
- TCP Object
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs
  - InOut Segs
- Thread Object—Troubleshooting Perfmon Data Logger only logs Cisco Unified Communications Manager threads.
  - %CPU Time

Refer to the Performance Objects and Counters for Cisco Unified Communications Manager for a description of the counters:

- Cisco CallManager Object

  - CallManagerHeartBeat
  - CallsActive
  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
- Cisco SIP Stack Object
  - CCBsAllocated
  - SCBsAllocated
  - SIPHandlerSDLQueueSignalsPresent
- Cisco CallManager System Performance Object
  - AverageExpectedDelay
  - CallsRejectedDueToThrottling
  - CodeRedEntryExit
  - CodeYellowEntryExit
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total
  - SkinnyDevicesThrottled
  - ThrottlingSampleActivity
  - TotalCodeYellowEntry
- Cisco TFTP Server Object
  - BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftkeyCount
  - BuildUnitCount
  - ChangeNotifications

- DeviceChangeNotifications
- DialruleChangeNotifications
- EncryptCount
- GKFoundCount
- GKNotFoundCount
- HeartBeat
- HttpConnectRequests
- HttpRequests
- HttpRequestsAborted
- HttpRequestsNotFound
- HttpRequestsOverflow
- HttpRequestsProcessed
- HttpServedFromDisk
- LDFoundCount
- LDNotFoundCount
- MaxServingCount
- Requests
- RequestsAborted
- RequestsInProgress
- RequestsNotFound
- RequestsOverflow
- RequestsProcessed
- SegmentsAcknowledged
- SegmentsFromDisk
- SegmentsSent
- SEPFoundCount
- SEPNotFoundCount
- SIPFoundCount
- SIPNotFoundCount
- SoftkeyChangeNotifications
- UnitChangeNotifications

No Cisco Unity Connection counters get logged to the troubleshooting perfmon data log. Refer to the "Cisco Unity Connection Performance Objects and Counters" appendix for a description of the Cisco Unity Connection counters.

Where to Find More Information

Related Topics

- Using RTMT for Performance Monitoring, page 3-1
- Configuring Troubleshooting Perfmon Data Logging, page 7-4
- Viewing Alerts, page 9-2
- Working with Performance Queries, page 6-1
- System Performance Objects and Counters, page A-1
- Performance Objects and Counters for Cisco Unified Communications Manager, page B-1
- Cisco Unity Connection Performance Objects and Counters, page C-1

CHAPTER 4

Monitoring Predefined System Objects

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

The system logs data every 5 minutes for predefined system counters.

This chapter contains information on the following topics:

- Predefined System Objects Overview, page 4-1
- Viewing the System Summary, page 4-3
- Monitoring Server Status, page 4-3
- Understanding Server Logs, page 4-4
- Where to Find More Information, page 4-5

Predefined System Objects Overview

RTMT displays information on predefined system objects in the monitoring pane.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

For more information on service parameters, refer to *Cisco Unified Communications Manager Administration Guide* or *Cisco Unity Connection System Administration Guide*.

Table 4-1 provides information on the predefined objects that RTMT monitors.

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

Table 4-1 System Categories

Category	Description
System Summary	Displays information on Virtual Memory usage, CPU usage, Common Partition Usage, and the alert history log. To display information on predefined system objects, choose **System > System Summary.**
Server	• CPU and Memory—Displays information on CPU usage and Virtual memory usage for the server. To display information on CPU and Virtual memory usage, choose **System > Server > CPU and Memory**.To monitor CPU and memory usage for specific server, choose the server from the host drop-down list box. • Process—Displays information on the processes that are running on the server. To display information on processes running on the system, choose **System > Server > Process**. To monitor process usage for specific server, choose the server from the Host drop-down list box. • Disk Usage—Displays information on disk usage on the server. To display information on disk usage on the system, choose **System > Server > Disk Usage**. To monitor disk usage for specific server, choose the server from the host drop-down list box. • Critical Services—Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the server or for a particular server in a cluster (if applicable). To display information on critical services, choose **System > Server > Critical Services**, then click the applicable tab: – To display system critical services, click the System tab. – To display Cisco Unified Communications Manager critical services, click the CallManager tab. – To display Cisco Unity Connection critical services, click the Cisco Unity Connection tab. – To monitor critical services for specific server on the tab, choose the server from the host drop-down list box and click the critical services tab in which you are interested. If the critical service status indicates that the administrator stopped the service, the administrator performed a task that intentionally stopped the service; for example, the service stopped because the administrator backed up or restored Cisco Unified Communications Manager, performed an upgrade, stopped the service in Cisco Unified CallManager Serviceability or the Command Line Interface (CLI), and so on. If the critical service status displays as unknown state, the system cannot determine the state of the service. For more information on the critical service states, refer to Monitoring Server Status, page 4-3.

Additional Information

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

Viewing the System Summary

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

- Virtual Memory usage
- CPU usage
- Common Partition Usage
- Alert History Log

For more information about the data these monitors provide, see "Monitoring Server Status" section on page 4-3.

For more information about the Alert History Log, see Understanding Alerts, page 9-1.

Additional Information

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

Monitoring Server Status

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

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

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

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

Note If more than one logical disk drive is available in your system, the system stores CTI Manager traces in the 'spare' partition on the first logical disk and CiscoCallManager traces on the second logical disk. RTMT monitors the disk usage for the 'spare' partition in the Disk Usage window.

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

For a specific description of each state, see Table 4-2.

Table 4-2 Status of Critical Services

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

Additional Information

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

Understanding Server Logs

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

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

The Cisco AMC service logs the server data in csv format. The header of the log comprises the time zone information and a set of columns with the previous counters for a server. These sets of columns repeat for every server in a cluster, if applicable.

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

To download the server logs for viewing on your local computer, refer to Working with Trace and Log Central, page 11-1.

Additional Information

See the "Where to Find More Information" section on page 4-5.

Where to Find More Information

Related Topics

- Predefined System Objects Overview, page 4-1
- Viewing the System Summary, page 4-3
- Monitoring Server Status, page 4-3
- Understanding Server Logs, page 4-4

CHAPTER 5

Monitoring Predefined Cisco Unified Communications Manager Objects

RTMT provides a set of default monitoring objects that assist you in monitoring the health of the Cisco Unified Communications Manager application. Default objects include performance counters for call processing activity and other supported services.

The system logs data every 5 minutes for predefined Cisco Unified Communications Manager counters.

This chapter contains information on the following topics:

- Predefined Cisco Unified Communications Manager Objects Overview, page 5-2
- Viewing the Cisco Unified Communications Manager Summary, page 5-5
- Monitoring Call-Processing Activity, page 5-6
- Understanding Call-Processing Logs, page 5-7
- Understanding Session Trace, page 5-8
- Monitoring Services, page 5-13
- Understanding Service Logs, page 5-13
- Monitoring Devices, page 5-14
- Understanding Device Logs, page 5-16
- Working with Devices, page 5-17
- Monitoring CTI Applications, Devices, and Lines, page 5-20
- Working with CTI Applications, Devices, and Lines, page 5-21
- Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature, page 5-25
- Monitoring Intercompany Media Services, page 5-27
- Where to Find More Information, page 5-28

Predefined Cisco Unified Communications Manager Objects Overview

RTMT displays information on predefined Cisco Unified Communications Manager objects in the monitoring pane when you select Communications Manager in the quick launch channel. The tool monitors the predefined objects on all servers in an cluster, if applicable.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

For more information on Service Parameters, refer to *Cisco Unified Communications Manager Administration Guide* or *Cisco Unity Connection System Administration Guide*.

Table 5-1 provides information on the predefined object that RTMT monitors.

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

Table 5-1 Cisco Unified Communications Manager Categories

Category	Description
CallManager Summary	Displays registered phones, calls in progress, and active gateway ports and channels. To display information on predefined Cisco Unified Communications Manager objects, choose **CallManager > CallManager Summary**.
Call Process	• Call Activity—Displays the call activity on Cisco Unified Communications Manager, including calls completed, calls attempted, calls in progress, and logical partition total failures. This includes all servers in the cluster, if applicable. To display information on call activities, choose **CallManager > Call Process > Call Activity**. • Gateway Activity—Displays gateway activity on Cisco Unified Communications Manager, including active ports, ports in service, and calls completed. This includes all servers in the cluster, if applicable. To display information on gateway activities, choose **CallManager > Call Process > Gateway Activity**. Select the type of gateway interface from the **Gateway Type** drop-down box. • Trunk Activity—Displays the trunk activity on Cisco Unified Communications Manager, including calls in progress and calls completed. This includes all servers in the cluster, if applicable. To display information on trunk activities, choose **CallManager > Call Process > Trunk Activity**. Select the trunk type in the **Trunk Type** drop-down box. • SDL Queue—Displays SDL queue information, including number of signals in queue and number of processed signals. To display information on the SDL Queue, choose **CallManager > Call Process > SDL Queue**. Select the type from the **SDL Queue Type** drop-down list box. • SIP Activity—Displays SIP activity on Cisco Unified Communications Manager, including summary requests, summary responses, summary of failure responses in, summary of failure responses out, retry requests out, and retry responses out. This includes all servers in the cluster, if applicable. To display information on SIP activities, choose **CallManager > Call Process > SIP Activity**. • Session Trace—Displays all SIP message activity: specifically, the incoming and outgoing calls and sessions that pass through the Cisco Unified Communications Manager. Provides associated call flow diagram for each SIP transaction. To display information on Session Trace, choose **CallManager > Call Process > Session Trace**. For more information, see "Understanding Session Trace" section on page 5-8.

Table 5-1 Cisco Unified Communications Manager Categories (continued)

Category	Description
Device	Device Summary displays information on the Cisco Unified Communications Manager server, including the number of registered phone devices, registered gateway devices, and registered media resource devices. This includes all servers in the cluster, if applicable. Device Search displays cluster name and device types in a tree hierarchy and allows you to query for information on phones and devices. Phone Summary displays information on the Cisco Unified Communications Manager server, including the number of registered phones, registered SIP phones, registered SCCP phones, partially registered phones, and the number of failed registration attempts. This includes all servers in the cluster, if applicable. To display information on the number of registered phones, gateways, and media resource devices on Cisco Unified Communications Manager, choose **CallManager > Device > Device Summary**. **Tip** To monitor other devices, you must perform additional configuration steps, as described in the "Finding Specific Devices to Monitor" section on page 5-17.
Service	• Cisco TFTP—Displays Cisco TFTP status on the Cisco Unified Communications Manager server, including total TFTP requests, total TFTP requests found, and total TFTP requests aborted. This includes all servers in the cluster, if applicable. To display information on the Cisco TFTP service, choose **CallManager > Service > Cisco TFTP**. • Heartbeat—Displays heartbeat information for the Cisco Unified Communications Manager, Cisco TFTP service. To display the heartbeat status of Cisco Unified Communications Manager servers, Cisco TFTP servers, choose **CallManager > Service > Heartbeat**. • Database Summary—Provides connection information for the server, such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, the number of replicates that have been created, and the status of the replication. To display information on the database, choose **CallManager > Service > Database Summary.**

Table 5-1 Cisco Unified Communications Manager Categories (continued)

Category	Description
CTI Manager	Displays information on the devices and applications that interfaces with the CTI Manager. To display information on CTI Applications, choose **CallManager > CTI > CTI Manager**. To monitor specific CTI types, you must perform additional configuration steps, as described in the following sections: • Finding CTI Applications to Monitor, page 5-21 • Finding CTI Devices to Monitor, page 5-22 • Finding CTI Lines to Monitor, page 5-23 You cannot choose CTI Manager by using the menu bar. To monitor the number of open devices, lines, and CTI connections in a single window on Cisco Unified Communications Manager, see the "Working with Devices" section on page 5-17.
Intercompany Media Services	• Routing—Displays the total number of Cisco Intercompany Media Engine routes maintained by Cisco Unified Communications Manager. To display information on call activities, choose **CallManager > Intercompany Media Services > Routing**. • Call Activities—Displays the Cisco Intercompany Media Engine call activity, including the number of calls that were accepted, busy, no answer, and failed. To display information on call activities, choose **CallManager > Intercompany Media Services > Call Activities**. For more information, see the "Monitoring Intercompany Media Services" section on page 5-27.

Additional Information

See the Related Topics, page 5-28.

Viewing the Cisco Unified Communications Manager Summary

In a single monitoring pane, RTMT allows you to monitor information about a Cisco Unified Communications Manager server or about all servers in a cluster (if applicable). In the callmanager summary window, you can view information on the following predefined object:

- Registered Phones
- Calls in Progress
- Active Gateway, Ports & Channels

Additional Information

See the "Related Topics" section on page 5-28.

Monitoring Call-Processing Activity

The Call Process monitoring category monitors the following items:

- Call Activity—You can monitor the number of calls that were attempted, calls that were completed, calls in progress, and logical partition total failures for a particular server or for an entire cluster (if applicable).
- Gateway Activity—You can monitor gateway activity for each gateway type. Gateway activity monitoring includes the number of active ports, the number of ports in service, and the number of calls that were completed for each gateway type for a particular server or for an entire cluster (if applicable).
- Trunk Activity—The system monitors trunk activity by trunk type for a particular server or for an entire cluster (if applicable). Trunk activity monitoring includes the number of calls in progress and the number of calls that were completed for a particular trunk type.
- SDL Queue—SDL queue monitoring monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).
- SIP Activity—The system displays a summary of SIP requests, SIP responses, total number of failed incoming responses (4xx, 5xx, and 6xx), total number of failed outgoing responses (4xx, 5xx, and 6xx), number of retry requests, and number of retry responses.
- Session Trace—You can search or trace the calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. RTMT downloads the Call Log file that includes the Start Time and Duration, searches for the matching calls, lists the matching call records, and provides the Call Flow Diagram.

Table 5-2 provides information about the call processing objects that RTMT monitors, the alert, thresholds, and defaults. For information on Cisco Unified Communications Manager call activity daily reports, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-2 Call Processing Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, CallsInProgress, and Logical Partition Failures Total for each server and cluster (if applicable).	N/A
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each server and cluster (if applicable).	N/A
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	N/A
SDL Queue activity on each server.	N/A
MGCP FXS Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted

Table 5-2 Call Processing Category (continued)

Monitored Objects (displayed)	Alert/Threshold/Default
MGCP FXO Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted
MGCP PRI Gateway—Number of In-Service and Active channels for each server and cluster (if applicable).	• D-Channel out of service • Route List exhausted
MGCP T1CAS Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route List exhausted

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Call-Processing Logs

The system accumulates call-processing data in the memory whenever RTMT calls the LogCall API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters on the basis of the following calculation:

- cmCallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsInProgress—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXO_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_PRI_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_T1_CAS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsInProgress—Average of all the values that were collected in last 5 minutes
- gwH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsInProgress—Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

- trunkSIP_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress—Average of all the values that were collected in last 5 minutes
- trunkSIP_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXS_PortsInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService—Average of all the values that were collected in lasts 5 minutes
- gwMGCP_PRI_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels—Average of all the values that were collected in last 5 minutes

The AMC service logs the call data in windows Performance tool-compatible csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for the server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Call Log applies: CallLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Session Trace

The Cisco Unified Communications Manager captures and logs all SIP message activities, which comprise the incoming and outgoing calls or sessions that pass through the Cisco Unified Communications Manager. The Cisco Unified Communications Manager stores the messages on a per-transaction basis in a new Call Log file, which can be downloaded through RTMT for post-processing activity.

RTMT users can search or trace the calls based on the following criteria:

- Calling Number/URI
- Called Number/URI
- Start Time
- Duration

RTMT downloads the Call Log file that includes the Start Time and Duration. The tool searches for the matching calls, lists the matching call records, and provides the SIP message Call Flow Diagram.

Before you Begin

Perform the following task:

- Use the enterprise parameter, Enable Call Trace Log, to enable or disable Call Tracing. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.
- The default value for maximum number of Call Trace log files specifies 2000 and the default value for maximum Call Trace log file size specifies 2 MB.

Procedure

Step 1 To display information on Session Trace, from the RTMT menus, choose **CallManager > Call Process > Session Trace**.

The Session Trace screen displays.

Step 2 Enter the search criteria and Click **Run**.

Note You can search calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. The search applies to the entire Unified CM cluster, not just the local node. If any node fails to collect the trace files, the system displays an error message in the bottom panel and pops up the message prompt to the user.

Click **Yes** to ignore the error and generate the table, based on the input.

Note In Calling Number/URI, Called Number/URI, you can use wild character "*" to match any number of characters. For example, a search for 123* fetches numbers like "123", "123456", "123*", "1234", etc.
If you want to search for numbers with a "*" in them, use "*". For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, and Termination Cause Code. The Termination Cause Code helps to identify the failure calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parenthesis followed by description.

Consider the following scenario:

- If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

Note If cause code description is missing or if you want more information on the Termination Cause Codes, refer the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

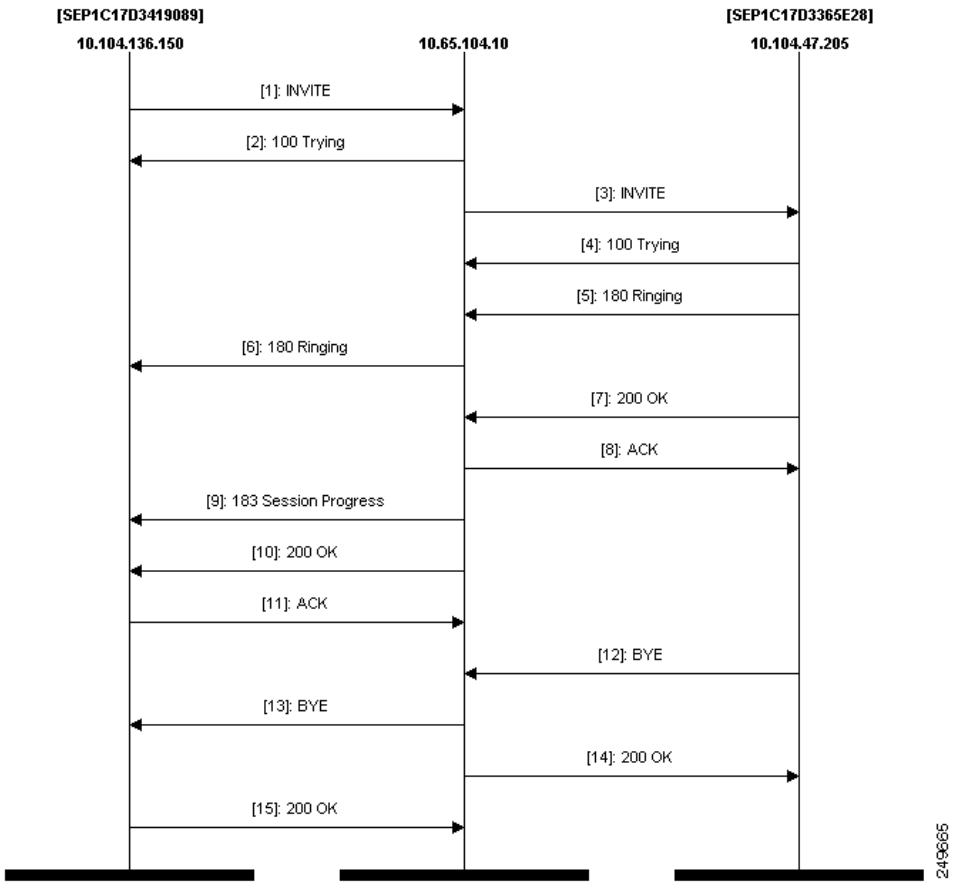
Step 3 Select a call (a row) to trace.

By default, **Include SIP Message** check box is selected to view the associated SIP protocol messages or call transactions.

Step 4 To generate the SIP Message Call Flow Diagram, click **Trace Call**. If you want to stop the generation of the session information, click **Cancel** on the progress window.

The Analyze Call Diagram window displays the corresponding SIP messages in the Call Flow Diagram.

Figure 5-1 Call Flow Diagram for Simple Call Scenario



Step 5 Click the tabs that you want to view. The following tabs are available:

- Call Flow Diagram—Displays the corresponding SIP messages in the Call Flow Diagram.
- Log File—Displays the entire log file.
- SIP Message—Appears only when the **Include SIP Message** check box is checked. Displays the actual SIP message that gets logged into the SDI log file.

Step 6 The following table lists the messages that display when you move your mouse on each SIP message in the Call Flow Diagram:

Displayed Messages	Description
Sender	Displays the IP address of the originating call.
SIP Call ID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or180 Ringing.

Displayed Messages	Description
Receiver	Displays the IP address of the destination call.
Device Name	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

- Click the **See message in log file** link to view the subset of call logs that can be downloaded and analyzed.
- Click the **See SIP Message** link. A new **SIP Message** tab displays adjacent to the **Log File** tab. Click the **SIP message** tab to display the actual SIP message that gets logged into the SDI log file.

  To view the SIP messages that get logged into the SDI log file, do the following:

  – check the **Enable SIP Call Processing Trace** check box in the Trace Configuration window of Cisco Unified Serviceability (**Trace > Configuration**). See *Cisco Unified Serviceability Administration Guide* for more information.

  – set the trace level to any one of the following—State Transition, Significant, Arbitrary or Detailed.

Note You can view the **See SIP Message** link only when the **Include SIP Message** check box is checked.

Step 7 Click **Save.**

The call flow diagram gets saved as index.html in the specified folder along with the SIP messages. You can email the files to the Technical Assistance Center (TAC).

Note If the files are zipped, extract the zipped files to a local folder and open them to view the images.

You can do the following:

a. To view the online help, click **Help**.

b. To exit the Analyze Call Diagram screen, click **Close**.

c. To navigate to the previous page, click **Previous Messages**.

d. To navigate to the next page, click **Next Messages**.

Note **Previous Messages** or **Next Messages** is enabled only when the message size exceeds a threshold.

Call Log files

The Session Manager logs the call data in new log files. These new log files are located in the following folder: /var/log/active/cm/trace/ccm/calllogs/.

The Call Log name has the following file name pattern: calllogs_dddddddd.txt.gz.

The Call Logs include the following message types:

- Call Control—Writes call information at call setup, split, join and release.

  ```
  Timestamp|MessageType (CC)|Operation (SETUP/SPLI/JOIN/RELEASE)|CI for one leg (aCI)|CI for other leg (bCI)|calling DN|Orig Called DN|Final Called DN
  ```

- Device Layer—Writes metadata information that relates to message from or to the device.

  ```
  Timestamp|MessageType (SIPL/SIPT)|My leg CI|Protocol(tcp/ucp)|Direction (IN/OUT)|local ip|local port|device name|device ip|device port|Correlation id|Message Tag|SIP Call ID|SIP method
  ```

Scenarios while Uninstalling RTMT

Consider the following scenarios, while uninstalling RTMT:

1. User saves the call flow diagram files in a folder (created by the user under **user.dir** directory)—All the files in **user.dir** are deleted except the newly created folder and the **user.dir** directory.
2. User saves the call flow diagram files in a folder (created during RTMT installation) under **user.dir** directory—All the files in **user.dir** are deleted including the **user.dir** directory.
3. User directly saves the call flow diagram files under **user.dir** directory—All the files in **user.dir** are deleted except the newly created files and the **user.dir** directory.
4. User saves the call flow diagram files in a folder which is outside **user.dir** directory—**user.dir** and its contents are removed. The folder created by the user is not deleted.

Limitations

The following limitations apply when the Call Flow Diagram gets generated:

- Search does not show incomplete calls.

  Example:

  When the user picks up the handset and hangs up without dialing the complete DN, it will not be listed in the search results.

- The Call Flow Diagram does not show some SIP messages in the following scenarios:
  - Conference calls involving more than three parties.
  - A call leg is used to invoke a feature alone.

  Example:

  Phone B and Phone C are in the same pickup group.

  1. User A calls Phone B.
  2. User C lifts up the Phone C handset.
  3. User C presses the PickUp softkey to pickup the call.

  SIP messages exchanged in Step 2 are not displayed in the Call Flow Diagram.

  In these cases, a RELEASE message is logged in the call logs without a corresponding SETUP message.

Monitoring Services

The Service monitoring category monitors the activities of Cisco TFTP requests, database activities, and heartbeat of the server or of different servers in a cluster (if applicable).

The Cisco TFTP service builds and serves files that are consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. You can view the total Cisco TFTP requests, requests not found, and requests that were aborted.

The tool (RTMT) monitors the heartbeat of Cisco Unified Communications Manager and Cisco TFTP services for the server or for different servers in a cluster (if applicable). The heartbeat acts as an indicator of the life of whatever it is monitoring. When the heartbeat is lost, a blinking icon appears in the lower, right corner of the RTMT window. To find when the heartbeat loss was detected, click the blinking icon. An email can notify you of the heartbeat loss, if you configure the system to do so.

The database summary provides connection information for the server or for each server in a cluster (if applicable), such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, replicates created, and replication status.

Table 5-3 provides information about the service objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily reports for CTI and Cisco TFTP usage statistics, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-3 Services Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of open devices, lines, CTI connections, and active Cisco Unified Communications Manager links for each CTI Manager.	N/A
TotalTftpRequests and TotalTftpRequestsAborted for each Cisco TFTP server.	N/A
Connection and replication status for each Directory server.	• Connection failed. • Replication failed.
Heartbeat rate for each Cisco CallManager, Cisco TFTP services.	• Cisco Unified Communications Manager heartbeat rate specifies <0.x. Default specifies 0.5. • Cisco TFTP heartbeat rate specifies <0.x. Default specifies 0.5.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Service Logs

The service data accumulates in the memory whenever RTMT calls the LogService API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters, based on the following calculation:

- ctiOpenDevices—Average of all the values that were collected in last 5 minutes
- ctiLines—Average of all the values that were collected in last 5 minutes
- ctiConnections—Average of all the values that were collected in last 5 minutes
- ctiActiveCMLinks—Average of all the values that were collected in last 5 minutes
- tftpRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- tftpAbortedRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

The AMC service logs the service data in csv format. The header of the log comprises the time zone information and a set of columns with the counters that were previously listed for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Service Log applies: ServiceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Monitoring Devices

The Device monitoring category provides a summary of devices, device search capability, and a summary of phones.

Table 5-4 provides information about the device objects that RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that RTMT generates for those devices. For information on daily reports on number of registered devices, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-4 Devices Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered phones for each server or for all servers in a cluster (if applicable).	Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.

Table 5-4 Devices Category (continued)

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered gateways on each server or for all servers in a cluster (if applicable).	For Cisco Unified Communications Manager: • (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls. For Cisco Unified Communications Manager Business Edition 5000: • (Warning) Total number of registered gateways decreased in consecutive polls. • (Informational) Total number of registered gateways increased in consecutive polls.
Number of registered media devices on each server or for all servers in a cluster (if applicable).	For Cisco Unified Communications Manager: • (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted. For Cisco Unified Communications Manager Business Edition 5000: • (Warning) Total number of registered media devices decreased in consecutive polls. • (Informational) Total number of registered media devices increased in consecutive polls. • Media List exhausted.

The Device Search menu comprises the following items on which you can search: phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and SIP trunks.

You can search on any device in the Cisco Unified Communications Manager system and choose the status of the devices, including registered, unregistered, rejected, any status, and devices that are only configured in the database. You can also search by any model, or a specific device model, and set up criteria that include several different attributes. Within the phone search, you can also search on the basis of phone protocol.

RTMT queries RIS to find the matching device. Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

If you have Cisco Unified Communications Manager clusters and you search for a device by choosing the any status option, RTMT does not display a snapshot of the matched device type, but rather it displays data for that device type from the RIS database for all specified Cisco Unified Communications Manager servers for a period of time. As a result, you may see multiple entries of a device with multiple statuses (Registered, Unregistered, and so on) in RTMT.

When you see multiple entries of a device, the current status of the device reflects the entry that has the latest time stamp. By configuring the RIS Unused Cisco CallManager Device Store Period service parameter for the Cisco RIS Data Collector service in Cisco Unified Communications Manager Administration, you can configure the period of time that the RIS database keeps information on unregistered or rejected device. Refer to *Cisco Unified Communications Manager Administration Guide* for more information on configuring service parameter.

Tip To find the matching item, RTMT requires that you activate the Cisco RIS Data Collector service in the Service Activation window.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

The phone summary provides information on the number of registered phones, phones that are running SIP, phones that are running SCCP, partially registered phones, and the number of failed registration attempts.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Device Logs

The device data accumulates in the memory whenever RTMT calls the LogDevice API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The data gets logged every 5 minutes for the following counters based on the following calculation:

- gatewayDevicesFXS—Average of all the values that were collected in last 5 minutes
- gatewayDevicesFXO—Average of all the values that were collected in last 5 minutes
- gatewayDevicesPRI—Average of all the values that were collected in last 5 minutes
- gatewayDevicesT1—Average of all the values that were collected in last 5 minutes
- gatewayDevicesH323—Average of all the values that were collected in last 5 minutes

The AMC service logs the device data in csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Device Log applies: DeviceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Working with Devices

This section contains information on the following topics:

- Finding Specific Devices to Monitor, page 5-17
- Viewing Phone Information, page 5-19
- Viewing Device Properties, page 5-19
- Configuring Polling Rate for Devices and Performance Monitoring Counters, page 5-20

Finding Specific Devices to Monitor

By performing the following procedure, you can monitor data for the following device types:

- Phones
- Gateway Devices
- H.323 Devices
- CTI Devices
- Voice Mail Devices
- Media Resources
- Hunt List
- SIP Trunk

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **CallManager.**
  - In the tree hierarchy, double-click **Device.**
  - Click the Device Search icon.
- Choose **CallManager > Device > Device Search > Open Device Search** > <device type; for example, Phone, Gateway, Hunt List, and so on>. A device selection window displays where you enter the search criteria. Go to Step 4.

The Device Search window displays the cluster names (if applicable) and tree hierarchy that lists all device types that you can monitor.

Tip After you display the Device Search or CTI Search panes, you can right-click a device type and choose **CCMAdmin** to go to Cisco Unified Communications Manager Administration.

Step 2 To find all devices or to view a complete list of device models from which you can choose, right-click the cluster name and choose **Monitor**.

Step 3 To monitor a specific device type, right-click or double-click the device type from the tree hierarchy.

Tip If you right-click the device type, you must choose **Monitor** for the device selection window to display.

Step 4 In the Select device with status window, click the radio button that applies.

Step 5 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Cisco Unified Communications Manager server for which you want the device information to display.

Tip In the remaining steps, you can choose the **< Back**, **Next >**, **Finish**, or **Cancel** buttons.

Step 6 Click the **Next >** button.

Step 7 In the Select Device with Download Status pane, click the radio button that applies, and click **Next**.

Step 8 In the Search by device model pane, click the radio button that applies.

Tip If you chose **Device Model**, choose the device type for which you want the device information to display.

Step 9 Click **Next**.

Step 10 In the Search with name pane, click the radio button that applies and enter the appropriate information in the corresponding fields, if required.

Tip If you enter the IPv6 address, the IP Subnet does not apply. Cisco Unified Communications Manager Business Edition 5000 does not support IPv6.

Step 11 Click **Next**.

Step 12 In the Monitor following attributes pane, check one or all of the search attributes.

Tip If you check the Ipv6Address check box, be aware that Cisco Unified Communications Manager Business Edition 5000 does not support IPv6.

Step 13 Click **Finish**.

Tip Some devices may not provide information for all search criteria. For example, if you select to monitor a phone for active load, inactive load, download status, or download reason, the download status results display Unknown for phone models that cannot provide this information.

Additional Information

See the Related Topics, page 5-28.

Viewing Phone Information

You can view information about phones that display in the RTMT device monitoring pane. This section describes how to view phone information.

Procedure

Step 1 To display the phone in the RTMT device monitoring pane, see the "Finding Specific Devices to Monitor" section on page 5-17.

Step 2 Perform one of the following tasks:

- Right-click the phone for which you want information to display and choose **Open**.
- Click the phone and choose **Device > Open**.

The Device Information Window displays.

Step 3 In the Select Device with Status pane, click the radio button that applies.

Step 4 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specificCisco Unified Communications Manager server for which you want the device information to display.

Step 5 In the Search By Device Model pane, choose the phone protocol that you want to display.

Step 6 Click the **Any Model or Device Model** radio button. If you click the Device Model radio button, choose a particular phone model that you want to display.

Step 7 Click **Next**.

Step 8 In the Search With Name pane, click the radio button that applies and enter the appropriate information in the corresponding fields.

Step 9 In the Monitor following attributes pane, check one or all of the search attributes.

Step 10 Click **Finish**.

The Device Information window displays. For more information on the device, choose any field that displays in the left pane of the window.

Additional Information

See the Related Topics, page 5-28.

Viewing Device Properties

You can view the properties of devices that display in the RTMT device monitoring pane. This section describes how to view device properties.

Procedure

Step 1 Display the device in the RTMT device monitoring pane. See the "Finding Specific Devices to Monitor" section on page 5-17.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want property information and choose **Properties**.

- Click the device for which you want property information and choose **Device > Properties**.

Step 3 To display the device description information, click the **Description** tab.

Step 4 To display other device information, click the **Other Info** tab.

Additional Information

See the Related Topics, page 5-28.

Configuring Polling Rate for Devices and Performance Monitoring Counters

Cisco Unified Communications Manager polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance monitoring counters and devices.

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

The default value for devices specifies 10 minutes.

Perform the following procedure to update the polling rate:

Procedure

Step 1 Display the device or 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 5-28.

Monitoring CTI Applications, Devices, and Lines

The CTI category monitors CTI Manager activities and provides CTI search capability. With CTI Manager, you can monitor the number of open devices, lines, and CTI connections.

You can specify criteria for the CTI applications, devices, and lines that include CTI status, device name, application pattern, and attributes.

Tip To find the matching item, RTMT requires that you activate the Cisco RIS Data Collector service in the Service Activation window inCisco Unified Serviceability.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a timestamp of the device that has been opened/closed and the application that controls the device media.

Working with CTI Applications, Devices, and Lines

This section contains information on the following topics:

- Viewing CTI Manager Information, page 5-21
- Finding CTI Applications to Monitor, page 5-21
- Finding CTI Devices to Monitor, page 5-22
- Finding CTI Lines to Monitor, page 5-23
- Viewing Application Information, page 5-24

Viewing CTI Manager Information

To display a chart of open devices, lines, and CTI connections for each server or for each server in a cluster (if applicable), click **CallManager** in the quick launch channel; double-click **CTI**, and then click the **CTI Manager** icon.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Applications to Monitor

Perform the following procedure to find specific CTI applications to monitor:

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Applications**. The selection window displays where you can enter the search criteria.

Step 2 From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the Applications Status drop-down list box, choose the application status.

Step 4 Click **Next**.

Step 5 In the Application Pattern pane, click the radio button that applies.

Step 6 Enter the information in the field for the radio button that you clicked; for example, if you clicked the IP Subnet radio button, enter the IP address and the subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 7 Click **Next**.

Step 8 In the Monitor following attributes window, check one or all of the check boxes for the attributes that you want to monitor.

Step 9 Click **Finish**.

The applications monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Devices to Monitor

Perform the following procedure to find specific CTI devices to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Devices**. The selection window displays where you can enter the search criteria. Go to Step 2.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the Devices Status drop-down list box, choose the device status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 Click **Next**.

Step 6 In the Application Pattern window, click the radio button that applies.

Step 7 Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 8 Click **Next**.

Step 9 In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.

Step 10 Click **Finish**.

The devices monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Lines to Monitor

Perform the following procedure to find specific CTI lines to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Lines**. The selection window displays where you can enter the search criteria. Go to Step 2.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the CTI Manager & Status drop-down list box, choose the CTI manager that you want to monitor.

Step 3 From the Lines Status drop-down list box, choose the status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 In the Lines pane, click the radio button that applies:

Note If you chose **Directory Number**, enter the directory number in the field.

Step 6 Click **Next**.

Step 7 In the Application Pattern pane, click the radio buttons apply:

Step 8 Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 9 Click **Next**.

Step 10 In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.

Step 11 Click **Finish**.

The lines monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Viewing Application Information

You can view the application information for selected devices such as the Cisco Unified IP Phone, CTI port, and CTI route point. This section describes how to view application information.

Procedure

Step 1 Display the devices in the RTMT monitoring pane, as described in the "Finding CTI Devices to Monitor" section on page 5-22.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want application information; for example, CTI; then, choose **App Info**.
- Click the device for which you want application information and choose **Device > App Info**.

The Application Information window displays the CTI manager server name, application ID, user ID, application IP address, application status, app time stamp, device time stamp, device name, and CTI device open status.

Step 3 To view updated information, click **Refresh**. To close the window, click **OK**.

Additional Information

See the Related Topics, page 5-28.

Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature

Learned pattern reports and SAF forwarder reports support the call control discovery feature. When you configure the call control discovery feature, Cisco Unified Communications Manager advertises itself and its hosted DN patterns to other remote call-control entities that use the SAF network. Likewise, these remote call-control entities advertise their hosted DN patterns, which Cisco Unified Communications Manager can learn and insert in digit analysis. For more information on the call control discovery feature, refer to the "Call Control Discovery" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Learned Pattern reports include such information as learned pattern name, time stamp, reachability status for the pattern, remote call-control entity that hosts the pattern, the PSTN failover configuration, and the destination IP address and port. RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

SAF Forwarder reports display information such as authentication status, registration status of SAF forwarders, and so on.

To access the Learned Patterns or SAF Forwarders reports in RTMT, perform the following procedure:

Procedure

Step 1 To access the report, perform one of the following tasks:

- For Learned Patterns—From the RTMT menus, choose **CallManager > Report > Learned Pattern**. Or, Click the **CallManager** tab; then, click **Learned Pattern**.
- For SAF Forwarders—From the RTMT menus, choose **CallManager > Report > SAF Forwarders**. Or, click the **CallManager** tab; then, click **SAF Forwarders**.

Step 2 Choose the node from the Select a Node drop-down list box.

For learned pattern reports, if the Cisco CallManager service is running but the CCD requesting service is not running on that node, a message displays that the CCD Report Service is not working after you choose the node. If the CCD requesting service is not active on the node that you choose, the report displays as empty.

Step 3 Review the data in the report, as described in Table 5-5 (for learned patterns) or Table 5-6 (for SAF forwarders).

Be aware that the learned pattern may be repeated in the report because the learned pattern may be coming from a different source; for example, it may be coming from a different IP address.

Table 5-5 Data from Learned Pattern Report

Column	Description
Pattern	Displays the name of the learned pattern from the remote call-control entity.
TimeStamp	Displays the date and time that the local Cisco Unified Communications Manager marked the pattern as a learned pattern.
Status	Indicates whether the learned pattern was reachable or unreachable

Table 5-5 Data from Learned Pattern Report (continued)

Column	Description
Protocol	Displays the protocol for the SAF-enabled trunk that was used for the outgoing call to the learned pattern; if the remote call-control entity has QSIG tunneling configured for the SAF-enabled trunk, the data indicates that QSIG tunneling was used; for example, EMCA is listed along with H.323 in this column.
AgentID	Displays the name of the remote call-control entity that advertised the learned pattern
IP Address	Displays the IP address for the call control entity that advertised the learned pattern; Displays the port number that the call-control entity uses to listen for the call.
ToDID	Displays the PSTN failover configuration for the learned pattern.
CUCMNodeId	Displays the ID from the local Cisco Unified Communications Manager node.

Table 5-6 Data from SAF Forwarder Report

Column	Description
Name	Displays the name of the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Description	Displays the description for the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration. If None displays, you did not enter a description for the SAF forwarder.
IP Address	Displays the IP address for the SAF forwarder, as configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Port	Indicates the port number that Cisco Unified Communications Manager uses to connect to the SAF forwarder; by default, Cisco Unified Communications Manager uses 5050.
Type	Indicates whether the SAF forwarder is classified as the primary or backup SAF forwarder.
Connection Status	Indicates whether Cisco Unified Communications Manager can connect to the SAF forwarder.

Table 5-6 Data from SAF Forwarder Report (continued)

Column	Description
Authentication Type	Indicates that Cisco Unified Communications Manager used digest authentication to connect to the SAF forwarder.
Registration Status	Indicates whether the Cisco Unified Communications Manager is registered to the SAF forwarder.
Time Last Registered	Displays the date and time when the Cisco Unified Communications Manager last registered with the SAF forwarder.
No of Registered Applications	Displays the total number of CCD advertising and requesting services that are registered to the SAF forwarder.
No of Connection Re-Attempts	Displays the number of times that the call-control entity, in this case, the Cisco Unified Communications Manager, has attempted to connect to the SAF forwarder.

Step 4 After the data displays, if you want to filter the results based on specific criteria, click the **Filter** button; specific the criteria that you want to search, click **Apply** and then **OK**.

Step 5 To display the most current results, click **Refresh**.

Step 6 If you want to search on a specific string in the data, click the **Find** button, enter the string, then, click **Find Next**.

Step 7 If you want to save the results, click **Save**, and choose either **XML** or **Text**, depending on how you want to save the results. Browse to the location where you want to save the data, name the file that you want to save; then, click **Save**.

Monitoring Intercompany Media Services

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application, not the backend server time, provides the basis for the time stamp in each chart.

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

The Intercompany Media Services monitoring category monitors the following items:

- Routing—Displays the total number of Cisco Intercompany Media Engine routes that Cisco Unified Communications Manager maintains. This total includes the following routes:
  - Learned routes that represent the phone numbers that the Cisco Intercompany Media Engine client learned and that exist in the Cisco Unified Communications Manager routing tables
  - Unique domains of peer enterprises for which Cisco Intercompany Media Engine routes exist
  - Published routes that represent the number of direct inward dialing numbers (DIDs) that were published successfully to the IME distributed hash table across all Cisco Intercompany Media Engine services
  - Rejected routes that represent the number of learned routes that got rejected because the administrator blocked them.

  These charts represent the following performance counters for the Cisco IME Client performance object: RoutesLearned, DomainsUnique, RoutesPublished, and RoutesRejected.

  To display information on routing, choose **CallManager > Cisco IME Client > Routing**.
- Call Activities—Allows you to monitor the total number of Cisco Intercompany Media Engine calls. This total includes the following types of calls:
  - Calls that were attempted (including calls that were accepted, busy, no answer, and failed)
  - Calls that were received
  - Calls that were set up (that is, made by Cisco Unified Communications Manager and accepted by the remote party)
  - Calls that were accepted (that is, received by Cisco Unified Communications Manager and answered by the called party)
  - Calls that completed fallback to the PSTN
  - Calls that did not successfully fallback to the PSTN.

  These charts represent the following performance counters for the Cisco IME Client performance object: CallsAttempted, CallAccepted, CallsReceived, CallsSetup, IMESetupsFailed, and FallbackCallsFailed.

  To display information on call activities, choose **CallManager > Cisco IME Client > Call Activities**.

Additional Information

See the Related Topics, page 5-28.

Where to Find More Information

Related Topics

- Predefined Cisco Unified Communications Manager Objects Overview, page 5-2
- Viewing the Cisco Unified Communications Manager Summary, page 5-5
- Monitoring Call-Processing Activity, page 5-6
- Understanding Call-Processing Logs, page 5-7
- Monitoring Services, page 5-13
- Understanding Service Logs, page 5-13

- Monitoring Devices, page 5-14
- Understanding Device Logs, page 5-16
- Working with Devices, page 5-17
- Monitoring CTI Applications, Devices, and Lines, page 5-20
- Working with CTI Applications, Devices, and Lines, page 5-21
- Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature, page 5-25
- Understanding Alerts, page 9-1
- Working with Alerts, page 10-1
- Understanding Performance Monitoring, page 3-1
- Working with Performance Queries, page 6-1
- Viewing Perfmon Log Files, page 7-1
- Working with Trace and Log Central, page 11-1

CHAPTER 6

Working with Performance Queries

To troubleshoot system performance problems, you add a counter (query) that is associated with the perfmon object to the Performance monitor, which displays a chart for the counter.

This chapter contains information on the following topics:

- Working with Categories, page 6-1
- Using Performance Queries to Add a Counter, page 6-3
- Removing a Counter from the Performance Monitoring Pane, page 6-4
- Adding a Counter Instance, page 6-5
- Configuring Alert Notification for a Counter, page 6-5
- Displaying a Counter Description, page 6-8
- Configuring a Data Sample, page 6-9
- Viewing Counter Data, page 6-10
- Local Logging of Perfmon Counters Data, page 6-10
- Where to Find More Information, page 6-11

Working with Categories

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

If you perform various searches for devices, for example, for phones, gateways, and so on, you can create a category for each search and save the results in the category.

Adding a Category

To add a category, perform the following procedure:

Procedure

Step 1 Go to applicable window for your configuration:

Cisco Unified Communications Manager	Display Performance Monitoring under the system tab or Devices/CTIs in the Search window under the Communications Manager tab.
Cisco Unified Communications Manager Business Edition 5000	Display Performance Monitoring under the system tab or Devices/CTIs in the Search window under the Communications Manager tab.
Connection	Choose **System > Performance > Open Performance Monitoring**.

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 "Where to Find More Information" section on page 6-11.

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 "Where to Find More Information" section on page 6-11.

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 "Where to Find More Information" section on page 6-11.

Using Performance Queries to Add a Counter

You can use queries to select and display perfmon counters. You can organize the perfmon counters to display a set of feature-based counters and save it in a category. See "Working with Categories" section on page 6-1 for more information. After you save your RTMT profile, you can quickly access the counters in which you are interested.

RTMT displays perfmon counters in chart or table format. The chart format displays the perfmon counter information by using line charts. For each category tab that you create, you can display up to six charts in the RTMT Perfmon Monitoring pane with up to three counters in one chart. After you create a category, you cannot change the display from a chart format to a table format, or vice versa.

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

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

Before you add counters, see the "Category Tabs" section on page 3-3. To zoom a counter, see "Zoom Feature" section on page 3-3.

Procedure

Step 1 Perform one of the following tasks:

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

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

The tree hierarchy expands and displays all the perfmon objects.

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

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

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

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

Step 7 Click **OK**.

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

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

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

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

Step 9 To monitor a counter in chart format, perform the following tasks:

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

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

The counter chart displays in the RTMT Perfmon Monitoring pane.

Additional Information

See the Related Topics, page 6-11.

Removing a Counter from the Performance Monitoring Pane

You can remove a counter chart (table entry) with the Remove Chart/Table Entry menu item in the Perfmon menu in the menu bar.

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

Perform one of the following tasks:

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

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

Additional Information

See the Related Topics, page 6-11.

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 "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 Perform one of the following tasks:

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

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

The counter displays.

Additional Information

See the Related Topics, page 6-11.

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 "Using RTMT for Performance Monitoring" section on page 3-1.

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

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

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

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

Step 6 Click **Next**.

Step 7 Use Table 6-1 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 6-1 Counter Alert Configuration Parameters

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

Table 6-1 Counter Alert Configuration Parameters (continued)

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

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

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

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

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

The Alert Action dialog box displays.

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

The Action Configuration dialog box displays.

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

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

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

The Input dialog box displays.

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

Step 16 Click **OK**.

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

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

Step 17 Click **OK**.

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

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

Step 19 Click **Close**.

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

Step 21 Click **Activate**.

Additional Information

See the Related Topics, page 6-11.

Displaying a Counter Description

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

Procedure

Step 1 Perform one of the following tasks:

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

Tip To display the counter description and to configure data-sampling parameters, see the "Configuring a Data Sample" section on page 6-9.

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

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

Additional Information

See the Related Topics, page 6-11.

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 6-10.

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

Procedure

Step 1 Display the counter, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 Perform one of the following tasks:

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

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

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

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

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

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

Table 6-2 Data Sample Parameters

Parameter	Description
Absolute	Because some counter values are accumulative, choose Absolute to display the data at its current status.
Delta	Choose Delta to display the difference between the current counter value and the previous counter value.
Delta Percentage	Choose Delta Percentage to display the counter performance changes in percentage.

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

Additional Information

See the Related Topics, page 6-11.

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 6-9 procedure for configuring data samples.

Additional Information

See the Related Topics, page 6-11.

Local Logging of Perfmon Counters Data

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer. See "Viewing Perfmon Log Files" section on page 7-1.

Starting the Counter Logs

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

Procedure

Step 1 Display the performance monitoring counters, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

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

The Counter Logging Configuration dialog box displays.

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

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

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

Stopping the Counter Logs

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

Procedure

Step 1 Display the performance monitoring counters, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

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

Additional Information

See the Related Topics, page 6-11.

Where to Find More Information

Related Topics

- Working with Categories, page 6-1
- Using Performance Queries to Add a Counter, page 6-3
- Removing a Counter from the Performance Monitoring Pane, page 6-4
- Adding a Counter Instance, page 6-5
- Configuring Alert Notification for a Counter, page 6-5
- Displaying a Counter Description, page 6-8
- Configuring a Data Sample, page 6-9
- Viewing Counter Data, page 6-10
- Local Logging of Perfmon Counters Data, page 6-10
- Viewing Perfmon Log Files, page 7-1
- Understanding Performance Monitoring, page 3-1
- System Performance Objects and Counters, page A-1

- Performance Objects and Counters for Cisco Unified Communications Manager, page B-1
- Cisco Unity Connection Performance Objects and Counters, page C-1

CHAPTER 7

Viewing and Troubleshooting Perfmon Logs

To view perfmon logs, you can download the logs or view them locally.

This chapter contains information on the following topics:

- Viewing Perfmon Log Files, page 7-1
- Working with Troubleshooting Perfmon Data Logging, page 7-4
- Where to Find More Information, page 7-6

Viewing Perfmon Log Files

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

Viewing Log Files on the Performance Log Viewer

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

The local perfmon logs comprise data from counters that you choose and store locally on your computer. For more information on how to choose the counters and how to start and stop local logging, see "Local Logging of Perfmon Counters Data" section on page 6-10.

Procedure

Step 1 Perform one of the following tasks:

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

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

- For RISDC Perfmon Logs, perform the following steps:
  a. Click on RISDC Perfmon Logs and choose a server 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 7-1 describes the functions of different buttons that are available on the performance log viewer.

Table 7-1 Performance Log Viewer

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

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

Additional Information

See the Related Topics, page 7-6.

Zooming In and Out

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

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

Additional Information

See the Related Topics, page 7-6.

Viewing the Perfmon Log Files with the Microsoft Performance Tool

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

Procedure

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

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

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

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

Step 5 Click **Apply.**

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

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

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

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

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

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

Additional Information

See the Related Topics, page 7-6.

Working with Troubleshooting Perfmon Data Logging

When you enable RISDC perfmon logs, information gets collected for the system in logs that are written on the server. You can enable or disable RISDC perfmon logs by going to the Service Parameter window of the administration interface for your configuration:

Cisco Unified Communications Manager	On Cisco Unified Communications Manager Administration, choose **System > Service Parameters** and select the Cisco RIS Data Collector Service from the Service drop-down menu.
Cisco Unified Communications Manager Business Edition 5000	On Cisco Unified Communications Manager Administration, choose **System > Service Parameters** and select the Cisco RIS Data Collector Service from the Service drop-down menu.
Connection	On Cisco Unity Connection Administration, choose **System Settings > Service Parameters** and select the Cisco RIS Data Collector from the Service drop-down menu.

By default, RISDC perfmon logging remains enabled. Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects performance data that are used to troubleshoot problems.

You can collect the log files for Cisco RIS Data Collector service on the server by using RTMT to download the log files. If you want to download the log files by using the CLI, refer to *Command Line Interface Reference Guide for Cisco Unified Solutions*. After you collect the log files, you can view the log file by using the Performance Log Viewer in RTMT or by using the Microsoft Windows performance tool. See "Viewing Log Files on the Performance Log Viewer" section on page 7-1 or "Viewing the Perfmon Log Files with the Microsoft Performance Tool" section on page 7-3.

Configuring Troubleshooting Perfmon Data Logging

The following procedure describes how to configure the troubleshooting perfmon data logging feature.

Procedure

Step 1 Go to the Service Parameters window of the administration interface for your configuration:

Cisco Unified Communications Manager	On Cisco Unified Communications Manager Administration, choose **System > Service Parameters**. The Service Parameter Configuration window displays.
Cisco Unified Communications Manager Business Edition 5000	On Cisco Unified Communications Manager Administration, choose **System > Service Parameters**. The Service Parameter Configuration window displays.
Connection	On Cisco Unity Connection Administration, expand **System Settings**, then click **Service Parameters**. The Service Parameter Configuration window displays.

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

Step 3 From the Service drop-down list box, choose Cisco RIS Data Collector.

Step 4 Enter the appropriate settings as described in Table 7-2.

Step 5 Click **Save**.

Troubleshooting Perfmon Data-Logging Configuration Settings

Table 7-2 describes the available settings to enable and disable troubleshooting perfmon data logging.

Table 7-2 Troubleshooting Perfmon Data-Logging Parameters

Field	Description
Enable Logging	From the drop-down box, choose **True** to enable or **False** to disable troubleshooting perfmon data logging. The default value specifies True.
Polling Rate	Enter the polling rate interval (in seconds). You can enter a value from 5 (minimum) to 300 (maximum). The default value specifies 15.
Maximum No. of Files	Enter the maximum number of Troubleshooting Perfmon Data Logging files that you want to store on disk. You can enter a value from 1 (minimum) up to 100 (maximum). The default value specifies 50. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value. When the number of files exceeds the maximum number of files that you specified in this field, the system will delete log files with the oldest timestamp. ⚠ **Caution** If you do not save the log files on another machine before you change this parameter, you risk losing the log files.

Table 7-2 Troubleshooting Perfmon Data-Logging Parameters (continued)

Field	Description
Maximum File Size	Enter the maximum file size (in megabytes) that you want to store in a perfmon log file before a new file is started. You can enter a value from 1 (minimum) to 500 (maximum). The default value specifies 5 MB. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value.

Where to Find More Information

Related Topics

- Using RTMT for Performance Monitoring, page 3-1
- Working with Troubleshooting Perfmon Data Logging, page 7-4
- Working with Performance Queries, page 6-1
- System Performance Objects and Counters, page A-1
- Performance Objects and Counters for Cisco Unified Communications Manager, page B-1
- Cisco Unity Connection Performance Objects and Counters, page C-1

CHAPTER 8

Using Cisco Unity Connection Port Monitor

This chapter describes how to use the Port Monitor for Cisco Unified Communications Manager Business Edition 5000 and for Cisco Unity Connection. It contains the following sections:

- Port Monitor Overview, page 8-1
- Using Cisco Unity Connection Port Monitor, page 8-2
- Where to Find More Information, page 8-2

Port Monitor Overview

The Port Monitor lets you monitor the activity of each Cisco Unity Connection voice messaging port in real time. This information can help you determine whether they system has too many or too few ports.

The Port Monitor provides information about each Cisco Unity Connection voice messaging port in real time. This information can help you determine the activity of each port and whether the system has too many or too few ports. The Port Monitor displays the information for each port as described in Table 8-1.

Table 8-1 Fields and Descriptions in the Port Monitor

Field	Description
Port Name	The display name of the port in Cisco Unity Connection Administration.
Caller	For incoming calls, the phone number of the caller.
Called	For incoming calls, the phone number that was dialed.
Reason	If applicable, the reason why the call was redirected.
Redir	The extension that redirected the call. If the call was redirected by more than one extension, this field shows the extension prior to the last extension.
Last Redir	The last extension that redirected the call.
Application Status	The name of the conversation that Cisco Unity Connection is playing for the caller. When the port is not handling a call, the status displays Idle.
Display Status	The action that the conversation is currently performing. When the port is not handling a call, the status displays Idle.

Table 8-1 Fields and Descriptions in the Port Monitor (continued)

Field	Description
Conversation Status	Specific details about the action that the conversation is performing. When the port is not handling a call, the status displays Idle.
Port Ext	The extension of the port.
Connected To	For Cisco Unified Communications Manager SCCP integrations, the IP address and port of the Cisco Unified Communications Manager server to which the ports are registered.

Note Depending on the information that the phone system integration provided and the status of the call, some fields in Table 8-1 may remain blank.

Using Cisco Unity Connection Port Monitor

Perform the following steps to use the Port Monitor.

Procedure

Step 1 In Unified CM Real Time Monitoring Tool, access Unity Connection and click **Port Monitor**. The Port Monitor window displays.

Step 2 In the Node drop-down box, choose a Cisco Unity Connection server.

Step 3 In the Polling Rate field, accept the default or enter the number of seconds between updates in the data on the Port Monitor tab; then, click **Set Polling Rate**.

Step 4 Click **Start Polling**. The Port Monitor window displays the status of all voice messaging ports on Cisco Unity Connection.

Note Setting a low polling rate may impact system performance.

Where to Find More Information

- Port Monitor Overview, page 8-1
- Using Cisco Unity Connection Port Monitor, page 8-2

PART 3

Alerts

CHAPTER 9

Understanding Alerts

This chapter contains information on the following topics:

- Using RTMT for Alerts, page 9-1
- Viewing Alerts, page 9-2
- Alert Fields, page 9-5
- Alert Action Configuration, page 9-7
- Enabling Trace Download, page 9-8
- Understanding Alert Logs, page 9-9
- Log Partition Monitoring, page 9-9

Using RTMT for Alerts

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

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

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

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

- Set Alert/Properties—This menu category allows you to set alerts and alert properties.
- Remove Alert—This menu category allows you to remove an alert.
- Enable Alert—With this menu category, you can enable alerts.
- Disable Alert—You can disable an alert with this category.
- Suspend cluster/node Alerts—This menu category allows you to temporarily suspend alerts on a particular server or on an entire cluster (if applicable).
- Clear Alerts—This menu category allows you to reset an alert (change the color of an alert item to black) to signal that an alert has been handled. After an alert has been raised, its color will automatically change in RTMT and will stay that way until you manually clear the alert.

Note The manual clear alert action does not update the System cleared timestamp column in Alert Central. This column is updated only if alert condition is automatically cleared.

- Clear All Alerts—This menu category allows you to clear all alerts.
- Reset all Alerts to Default Config—This menu category allows you to reset all the alerts to the default configuration.
- Alert Detail—This menu category provides detailed information on alert events.
- Config Email Server—In this category, you can configure your e-mail server to enable alerts.

Note To configure RTMT to send alerts via e-mail, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco Unified Communications Manager Server Configuration, see the "DHCP Server Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

- Config Alert Action—This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired e-mail recipients.

In RTMT, you configure alert notification for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on. RTMT predefined alerts are configured for perfom counter value thresholds as wells as event (alarms) notifications.

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

Additional Information

See the Related Topics, page 9-10.

Viewing Alerts

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under the applicable tabs—System, CallManager, Cisco Unity Connection, and Custom.

Stand-alone Cisco Unified CM installation will not include Cisco Unity Connection tab and vice- versa. However, Cisco Unified CM Business Edition 5000 will have all the above tabs.

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

- System Alerts, page 9-2
- CallManager Alerts, page 9-3
- Cisco Unity Connection Alerts, page 9-5

System Alerts

Note For alert descriptions and default configurations, see "System Alert Descriptions and Default Configurations" section on page E-1.

The following list comprises the preconfigured system alerts.

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalAuditEventGenerated
- CriticalServiceDown
- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (*Unified CM clusters only*)
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Note Since none of the audit events are alert worthy, there is no way to trigger the CriticalAuditEventGenerated alert.

CallManager Alerts

The following list comprises the preconfigured CallManager alerts.

Note For alert descriptions and default configurations, see "CallManager Alert Descriptions and Default Configurations" section on page F-1.

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSchedulerJobFailed

- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CodeYellow
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutOfSync
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports
- IMEDistributedCacheInactive
- IMEOverQuota
- IMEQualityAlert
- InsufficientFallbackIdentifiers
- IMEServiceStatus
- InvalidCredentials
- LowTFTPServerHeartbeatRate
- MaliciousCallTrace
- MediaListExhausted
- MgcpDChannelOutOfService
- NumberOfRegisteredDevicesExceeded
- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RouteListExhausted
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure

Cisco Unity Connection Alerts

The following list comprises the preconfigured Cisco Unity Connection alerts. These alerts apply only to Cisco Unity Connection and Cisco Unified Communications Manager Business Edition 5000.

Note For alert descriptions and default configurations, see "Cisco Unity Connection Alert Descriptions and Default Configurations" section on page G-1.

- NoConnectionToPeer *(Cisco Unity Connection cluster configuration only)*
- AutoFailoverSucceeded *(Cisco Unity Connection cluster configuration only)*
- AutoFailoverFailed *(Cisco Unity Connection cluster configuration only)*
- AutoFailbackSucceeded *(Cisco Unity Connection cluster configuration only)*
- AutoFailbackFailed *(Cisco Unity Connection cluster configuration only)*
- SbrFailed (Split Brain Resolution Failed) *(Cisco Unity Connection cluster configuration only)*
- DiskConsumptionCloseToCapacityThreshold
- DiskConsumptionExceedsCapacityThreshold
- LicenseExpirationWarning
- LicenseExpired

Note The first six alerts apply to Cisco Unity Connection cluster configurations only. Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster configuration.

Additional Information

See the Related Topics, page 9-10.

Alert Fields

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

Note Severity levels for Syslog entries match the severity level for all RTMT alerts. If RTMT issues a critical alert, the corresponding Syslog entry also specifies critical.

Table 9-1 provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 9-1 Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which RTMT associates an alert	Descriptive name. For preconfigured alerts, you cannot change this field. For a list of preconfigured alerts, see the "Viewing Alerts" section on page 9-2.
Description	Description of the alert	You cannot edit this field for preconfigured alerts. For a list of preconfigured alerts, see the "Viewing Alerts" section on page 9-2.
Performance Counter(s)	Source of the performance counter	You cannot change this field. You can associate only one instance of the performance counter with an alert.
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than #, %, rate greater than #, %, rate. This field is applicable only for alerts based on performance counters.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta. This field is applicable only for alerts based on performance counters.
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sending the alert immediately or after a specified time that the alert has persisted. This field is applicable only for alerts based on performance counters.
Number of Events Threshold	Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes).	For ExcessiveVoiceQualityReports, the default thresholds equal 10 to 60 minutes. For RouteListExhausted and MediaListExhausted, the defaults equal 0 to 60 minutes. This field is applicable only for event based alerts.
Node IDs *(Unified CM clusters only)*	Cluster or list of servers to monitor	Cisco Unified Communications Manager servers, Cisco TFTP server, or first server. This field is applicable only for non-clusterwide alerts. **Note** When you deactivate both the Cisco CallManager and Cisco TFTP services of a server, the system considers that server as removed from the currently monitored server list. When you reactivate both Cisco CallManager and Cisco TFTP services, that server is added back, and its settings are restored to default values.

Table 9-1 Alert Customization (continued)

Field	Description	Comment
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action gets defined first (see the "Additional Information" section on page 9-7). If this field is blank, that indicates that e-mail is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disabled.
Clear Alert	Resets alert (change the color of an alert item from to black) to signal that the alert has been resolved	After an alert has been raised, its color will automatically change to and stay that way until you manually clear the alert. Use Clear All to clear all alerts.
Alert Details *(Unified CM clusters only)*	Displays the detail of an alert (not configurable)	For ExcessiveVoiceQualityReports, RouteListExhausted, and MediaListExhausted, up to 30 current event details display in the current monitoring interval if an alert has been raised in the current interval. Otherwise, the previous 30 event details in the previous interval displays. For DChannel OOS alert, the list of outstanding OOS devices at the time the alert was raised displays.
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Raise alert once every X minutes if condition persists.) Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	N/A
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts.

Additional Information

See the Related Topics, page 9-10.

Alert Action Configuration

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

Table 9-2 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 9-2 Alert Action Configuration

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

Additional Information

See the Related Topics, page 9-10.

Enabling Trace Download

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

- CriticalServiceDown - CriticalServiceDown alert gets generated when any service is down.

Note The RTMT backend service checks status (by default) every 30 seconds. If service goes down and comes back up within that period, CriticalServiceDown alert may not get generated.

Note CriticalServiceDown alert monitors only those services that are listed in RTMT Critical Services.

- CodeYellow - This alarm indicates that Cisco Unified Communications Manager initiated call throttling due to unacceptably high delay in handling calls.
- CoreDumpFileFound - CoreDumpFileFound alert gets generated when RTMT backend service detects a new Core Dump file.

Note You can configure both CriticalServiceDown and CoreDumpFileFound alerts to download corresponding trace files for troubleshooting purposes. This helps preserve trace files at the time of crash.

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

Additional Information

See the Related Topics, page 9-10.

Understanding Alert Logs

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

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes in the Alert Central log history. Alert log periodically gets updated, and new logs get inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

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

The alert log includes the following attributes:

- Time Stamp—Time when RTMT logs the data
- Alert Name—Descriptive name of the alert
- Node—Server name for where RTMT raised the alert
- Alert Message—Detailed description about the alert
- Type—Type of the alert
- Description—Description of the monitored object
- Severity—Severity of the alert
- PollValue—Value of the monitored object where the alert condition occurred
- Action—Alert action taken
- Group ID—Identifies the source of the alert

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

Additional Information

See the Related Topics, page 9-10.

Log Partition Monitoring

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

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

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

- SparePartitionLowWaterMarkExceeded (% 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.
- SparePartitionHighWaterMarkExceeded (% disk space)—When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central.

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

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

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

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central. For more information, see "Setting Alert Properties" section on page 10-3.

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

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

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

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

Where to Find More Information

Related Topics

- Using RTMT for Alerts, page 9-1
- Viewing Alerts, page 9-2
- Alert Fields, page 9-5
- Alert Action Configuration, page 9-7
- Enabling Trace Download, page 9-8

- Understanding Alert Logs, page 9-9
- Working with Alerts, page 10-1
- Setting Alert Properties, page 10-3
- Suspending Alerts, page 10-5
- Configuring E-mails for Alert Notification, page 10-6
- Configuring Alert Actions, page 10-6

CHAPTER 10

Working with Alerts

This chapter contains information on the following topics:

- Working with Alerts, page 10-1
- Setting Alert Properties, page 10-3
- Suspending Alerts, page 10-5
- Configuring E-mails for Alert Notification, page 10-6
- Configuring Alert Actions, page 10-6
- Configuring a Global E-Mail List for Alert Notifications, page 10-7

Working with Alerts

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

Procedure

Step 1 Perform one of the following tasks:

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

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

Step 2 Perform one of the following tasks:

- To set alert properties, see the "Setting Alert Properties" section on page 10-3.
- To suspend alerts, see the "Suspending Alerts" section on page 10-5.
- To configure e-mails for alert notification, see the "Configuring E-mails for Alert Notification" section on page 10-6.
- To configure alert actions, see the "Configuring Alert Actions" section on page 10-6.

- 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 In Safe Range column.

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

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

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

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

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

- To reset alerts to default configuration, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Reset Alert to Default Config,** to reset that alert to the default configuration.
  - Choose **System > Tools > Alert > Reset all Alerts to Default Config,** to reset all the alerts to the default configuration.

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

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

Additional Information

See the "Related Topics" section on page 10-8.

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 10-1.

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

Step 3 Perform one of the following tasks:

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

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

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

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

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

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

Step 7 Click **Next**.

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

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

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

Step 10 Click **Next**.

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

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

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

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

Step 13 Click **Next**.

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

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

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

Step 17 To add a new alert action, continue to Step 18. To edit an existing alert action, skip to Step 25.

Step 18 Click **Add**.

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

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

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

Step 22 In the Enter email/epage address field, enter an e-mail or e-page address of the recipient that you want to receive the alert action.

Step 23 Click **OK**.

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

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

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

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

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

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

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

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

a. Click **Next**.

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

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

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

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

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

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

Additional Information

See the "Related Topics" section on page 10-8.

Suspending Alerts

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

Procedure

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

Note Per server suspend states do not apply to Cisco Unified Communications Manager or Cisco Unity Connection clusterwide alerts.

Step 2 Do one of the following:

To suspend all alerts in the cluster	Choose the Cluster Wide radio button and check the suspend all alerts check box.
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 3 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" section on page 10-8.

Configuring E-mails for Alert Notification

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

Note To configure RTMT to send alerts via e-mail, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco Unified Communications Manager Server Configuration, see the DHCP Server Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*.

(Unified CM Clusters only) Because Cisco Unified Communications Manager generates the e-mail notifications, you can verify that the mail server that you configure can be reached from the Cisco Unified Communications Manager platform with the CLI command: **utils network ping** <mail server>

Procedure

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

The Mail Server Configuration window displays.

Step 2 Enter the address of the mail server in the Mail Server field.

Step 3 Enter the port number of the mail server in the Port field.

Step 4 Enter the address of the intended recipient in the Enter e-mail/epage address field.

Repeat Step 4 as necessary to enter all intended e-mail recipients.

By default, RTMT_Admin@domain will be used, where domain is the domain of the host server.

Step 5 Click **OK**.

Additional Information

See the "Related Topics" section on page 10-8.

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 10-1.

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

Step 3 Perform Step 17 through in the "Setting Alert Properties" section on page 10-3 to add, edit, or delete alert actions.

Additional Information

See the "Related Topics" section on page 10-8

Configuring a Global E-Mail List for Alert Notifications

The following procedure describes how to configure all precanned alerts at once for sending to one or more e-mail destinations. This procedure uses the initial "Default" alert action setting that is assigned to all alerts by default at installation.

Follow this procedure to configure a recipient list for all precanned alerts without having to set an alert action for each alert. When you add e-mail destinations to the Default alert action list, all pre-canned alerts get sent to those recipients, as long as all alerts continue to use the Default alert action.

Note To configure a new alert action for a specific alert, you can use the Set Alerts/Properties option,which displays when you right-click an alert. You can also reconfigure existing alert actions with this option.

Any time you update an alert action, the changes apply to all alerts that are configured with that alert action. For example, if all alerts use the "Default" alert action, updating the alert action "Default" will impact all alerts.

You cannot remove the "Default" alert action. For all other alert actions, the system allows you to delete an alert action only when it is not associated with other alerts. If an alert action is associated with multiple alerts, you must reassign a new alert action to those alerts before you can delete the alert action.

Procedure

Step 1 Click **Alert Central** in the QuickLaunch Channel.

The Alert Central window displays.

Step 2 Click **System > Tools > Alert > Config Alert Action**.

The Alert Action box displays.

Step 3 Select Default (highlight the item) in the Alert Action list and click **Edit**.

The Action Configuration box displays.

Step 4 (Optional) Enter the description of the default list.

Step 5 Click **Add** to add a recipient. The Input box displays.

Step 6 Enter an e-mail destination that is to receive all alerts. Click **OK**.

The e-mail address displays in the Recipients list in the Action Configuration box; the destination is enabled by default.

Note You can disable an e-mail destination at any time by clicking the check box next to the destination to disable it. To completely remove a recipient from the list, highlight the recipient in the list and click **Delete**.

Step 7 Return to Step 5 to add additional e-mail destinations, as required.

Note You can disable e-mails for an alert at any time by highlighting the alert in the Alert Central window, right-clicking the alert, and using the Set Alert/Properties selections to deselect Enable Email.

Additional Information

See the "Related Topics" section on page 10-8.

Where to Find More Information

Related Topics

- Working with Alerts, page 10-1
- Setting Alert Properties, page 10-3
- Suspending Alerts, page 10-5
- Configuring E-mails for Alert Notification, page 10-6
- Configuring Alert Actions, page 10-6
- Configuring a Global E-Mail List for Alert Notifications, page 10-7
- Configuring Alert Notification for a Counter, page 6-5
- Understanding Alerts, page 9-1

PART 4

Tools for Traces, Logs, and Plug-Ins

CHAPTER 11

Working with Trace and Log Central

The trace and log central feature in the Cisco Unified 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 a SFTP or FTP server on your network, or collect a crash dump file.

After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Note From RTMT, you can also edit the trace setting for the traces on the server 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 directly access the server or all of the servers in a cluster without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the server(s) 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 11-2
- Displaying Trace and Log Central Options in RTMT, page 11-2
- Collecting Trace Files, page 11-3
- Collecting Installation Logs, page 11-7
- Using the Query Wizard, page 11-8
- Scheduling Trace Collection, page 11-12
- Viewing Trace Collection Status and Deleting Scheduled Collections, page 11-15
- Collecting a Crash Dump, page 11-16
- Collecting Audit Logs, page 11-19

- Using Local Browse, page 11-22
- Using Remote Browse, page 11-23
- Displaying QRT Report Information, page 11-27
- Using Real-Time Trace, page 11-28
- Updating the Trace Configuration Setting for RTMT, page 11-32
- Log Compression, page 11-32

Importing Certificates

You can import the server authentication certificate that the certificate authority provides for the server or 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 the server(s) each time that you log in to 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**.

Additional Information

See the Related Topics, page 11-33.

Displaying Trace and 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 11-2.

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

- In the Quick Launch Channel, click **System**; then, click the **Trace & Log Central** icon.
- Choose **Tools > Trace & 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 and Log Central options in the real-time monitoring tool, perform one of the following tasks:

Note Cisco Unified Serviceability supports only these options on Windows servers: Collect Files and Schedule Collection.

- Collect traces for services, applications, and system logs on the server or on one or more servers in the cluster. See "Collecting Trace Files" section on page 11-3
- 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 11-8

- Schedule a recurring trace collection and download the trace files to a SFTP or FTP server on your network. See "Scheduling Trace Collection" section on page 11-12
- Collect a crash dump file for one or more servers on your network. See "Collecting a Crash Dump" section on page 11-16.
- Collect audit log files and download the audit logs to a SFTP or FTP server on your network. See "Collecting Audit Logs" section on page 11-19.
- View the trace files that you have collected. See the "Using Local Browse" section on page 11-22.
- View all of the trace files on the server. See the "Using Remote Browse" section on page 11-23.
- 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 11-28.

Additional Information

- See Related Topics, page 11-33.

Collecting Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on the server or 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 11-8.

RTMT Trace and Log Central Disk IO and CPU Throttling

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

When you make a request for an on-demand operation when the call processing node is running under high IO conditions, the system displays a warning that gives you the opportunity to abort the operation. You can configure the IO rate threshold values that control when the warning displays with the following service parameters (in Cisco RIS Data Collector service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

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

Trace Compression Support

This feature enables the ROS (Recoverable Outstream) library to support the compressed output of tracefiles. The files get compressed as they are being generated. The benefits of tracefile compression include

- Reduces the capacity that is required to store tracefiles.
- Reduces the disk head movement, which results in significantly improved disk I/O wait. This may prove of value when tracefile demand is high.

Use the enterprise parameter, Trace Compression, to enable or disable trace compression. The default value for this parameter specifies Disabled. For information on setting the values of enterprise parameters, see the "Enterprise Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Caution Compressing files adds additional CPU cycles. Enabling the Trace Compression enterprise parameter can negatively impact overall call throughput by as much as 10 percent.

You can recognize compressed files by their .gz extension (.gzo if the file is still being written to). To open a compressed file, double click the file name, and the file opens in the log viewer.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window in Cisco Unified Serviceability. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window in Cisco Unified Serviceability. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- Configure the throttling of critical Trace and Log Central operations and jobs by setting the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service). For more information on configuring service parameters, refer to the *Cisco Unified Communications Manager Administration Guide.*
- Optionally, enable trace compression by setting the value of the Trace Compression enterprise parameter to Enabled. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide.*

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

The Trace Collection wizard displays.

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

Note *Unified CM clusters and Connection clusters only:* 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 and Log Central windows.

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

Step 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE 5000*, perform one of the following actions in the Select CCM Services/Application tab:

- To collect traces for all services and applications for all servers in a cluster, check the **Select All Services on All Servers** check box and click **Next**.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications on a particular server (or for particular system logs on the server for Connection), check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To go to the next tab without collecting traces for services or applications, click **Next**.

Go to Step 4 for *Unified CM BE* 5000 or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To go to the next tab without collecting traces for system logs, click **Next.** *Connection* users go to Step 6.

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

- To collect all system logs for all servers in a cluster, check the **Select All Services on all Servers** check box and click **Next**.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the trace collection wizard without collecting traces for system logs, click **Next**.

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

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

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

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

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

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

Note RTMT returns logs of a different timestamp, than that configured through the wizard. This occurs specifically, when the specified timestamp is lesser than that of the existing log files. For example:
Log files exist on the server for a specific service from 11/24/09, and you have given the time range from 11/23/09 5:50 to 11/23/09 7:50; RTMT still returns the existing log files.

Step 7 In the Download File option group box, specify the options that you want for downloading traces. From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

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

This means that when you upgrade from one version of Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, or Cisco Unity Connection that is running on an appliance server to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log back in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Cisco Unified Communications Manager or Cisco Unity Connection versions that ran on the Windows platform.

Step 8 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 9 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 10 To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.

Step 11 Click **Finish** or, to abort the settings**,** click **Cancel**.

If you clicked Finish, the window shows the progress of the trace collection.

When the trace collection process is complete, the message “Completed downloading for node <Server name or IP address>” displays at the bottom of the window.

Step 12 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 11-22.

Note You will see a message if the service parameter values are exceeded or if the system is in code yellow.

Additional Information

- For more information about setting the values of enterprise parameters, see the "Enterprise Parameters Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*
- For information about setting the values of service parameters, see the "Service Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*
- Also see Related Topics, page 11-33.

Collecting Installation Logs

The following procedure describes how to collect installation and upgrade logs in trace and log central.

Procedure

Step 1 Perform one of the following tasks:

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

The Trace & Log Central window displays.

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

The Collect Install Logs wizard displays

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

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

Step 5 Click **Finish**.

Using the Query Wizard

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

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

Before You Begin

Perform one or more of the following tasks:

- From the Trace Configuration window in Cisco Unified Serviceability, configure the information that you want to include in the trace files for the various services. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window. For more information, refer to *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

The Query wizard displays.

Step 3 In the Query Wizard Options window, click one of the following radio buttons:

- Saved Query

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

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

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

  To run the query without any modifications, click **Run Query** and go to Step 22. To modify the query, go to Step 4.

- Create Query

Step 4 Click **Next**.

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

Tip To collect traces for all services and applications on a particular server, check the check box next to the server name or server IP address. To collect traces for all services and applications for all servers in a Cisco Unified Communications Manager cluster, check the **Select All Services on All Servers** check box. To collect traces for particular system logs on the server, check the check boxes that apply

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

Note If you have a cluster configuration, you can install some of the listed services/applications only on a particular server 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 *Connection* users go to Step 8. For *Unified CM* or *Unified CM BE 5000*, choose the services and application logs in which you are interested by checking all check boxes that apply in the Select CallManager Services/Applications tab.

Step 7 Click **Next**. *Unified CM* users go to Step 10.

Step 8 In the Select CUC Services/Application tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 9 Click **Next**.

Step 10 In the Select System Logs tab, choose the logs in which you are interested by checking all check boxes that apply.

Step 11 Click **Next**.

Step 12 In the Query Time Options box, specify the time range for which you want to collect traces. Choose one of the following options:

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

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

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

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

Step 13 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box.

Step 14 In the Call Processing Impact Options box, specify the level of impact you want the string search activity to have on call processing. From the Select Impact Level drop down list box, select Low, Medium, or 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 15 Click **Next**.

Step 16 In the Action Options window, choose one of the following actions:

- Trace Browse
- On Demand Trace Collection
  - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.
- Schedule Download

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

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 17 Choose one of the following options:

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

  The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **Close** and continue with Step 22.
- To save the query, click the **Save Query** button and continue with Step 18.
- To download the trace, click the **Download Trace** button. This option is only available if you selected On Demand Trace Collection or Schedule Download from the Action Options window.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 11-22.

Step 18 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 servers other than the one on which it was created. You can create a generic query only if the services that you chose exist on that server. If you chose services on more than one server in a cluster, a message displays.

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

  - For Cisco Unified Communications Manager clusters, the trace collection tool chooses all the servers in the cluster by default when you execute the query.
  - For Cisco Unified Communications Manager Business Edition 5000, the trace collection tool chooses the server on which you created the query when you executed the query.
  - For Cisco Unity Connection, the trace collection tool chooses the server on which you created the query when you executed 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 server or cluster (if applicable) on which you created the query.

Step 19 Click **Finish**.

Step 20 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 21 Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with Step 22.
- To exit the query wizard without running the query that you created, click **Cancel**.

Step 22 After the query execution completes, perform one or more of the following tasks:

- To view a file that you collected, navigate to the file by double-clicking Query Results, double-clicking the <node> folder, where <node> equals the IP address or host name for the server that you specified in the wizard, and double-clicking the folder that contains the file that you want to view.

  After you have located the file, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer. The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

Note *Unified CM and Unified CM BE 5000 only:* To view reports that the QRT Quality Report Tool (QRT) generates, see the "Displaying QRT Report Information" section on page 11-27.

- Download the trace files and the result file that contains a list of the trace files that your query collected by choosing the files that you want to download, clicking the **Download** button, specifying the criteria for the download, and clicking **Finish**.
  - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 11-22.

- To save the query, click **Save Query** button and complete Step 18 through Step 20.

Note You will see a message if the service parameter values are exceeded or if the system is in code yellow.

Additional Information

See the Related Topics, page 11-33.

Scheduling Trace Collection

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

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

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window of Cisco Unified Serviceability. For more information, refer to the *Cisco Unified Serviceability Administration Guide*.
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window. For more information, refer to the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

The Schedule Collection wizard displays.

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

Note *Unified CM clusters and Connection clusters only:* 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 and Log Central windows.

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

Step 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE 5000*, perform one of the following actions in the Select CCM Services/Application tab:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for services or applications, click **Next.**

Go to Step 4 for *Unified CM BE* 5000 or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

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

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 6 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 7 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 8 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 9 From the Scheduler Frequency drop-down list box, choose how often you want to run the configured trace collection.

Step 10 From the Collect Files that are 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 11 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. The tool searches for a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box

Step 12 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 13 To delete collected log files from the server, check the **Delete Collected Log Files from the Server** check box.

Step 14 Choose one or more of the following actions:

- Download Files. If you chose Download Files or Run Another Query, continue with Step 15.
- Run Another Query
- Generate Syslog. If you chose Generate Syslog, go to Step 17.

Step 15 In the SFTP/FTP 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 or FTP 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 or FTP parameters fields: /home/<user>/Trace.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 16 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 17 Click **Finish**.

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

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

Step 18 Click **OK**.

Step 19 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

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

Additional Information

See the Related Topics, page 11-33.

Viewing Trace Collection Status and Deleting Scheduled Collections

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

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

The Job Status Window displays.

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

This list of scheduled trace collections displays.

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

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

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

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

Additional Information

See the Related Topics, page 11-33.

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 and Log Central Options in RTMT" section on page 11-2.

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

The Collect Crash Dump wizard displays.

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

Note *Unified CM clusters and Connection clusters only:* 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 and Log Central windows.

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

Step 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE 5000*, perform one of the following actions in the Select CCM Services/Application tab:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

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

Go to Step 4 for *Unified CM BE 5000* or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the servers, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

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

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

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

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

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

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

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

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

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

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

This means that when you upgrade from one version of Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition 5000, or Cisco Unity Connection that is running on the Linux platform to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of 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, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Cisco Unified Communications Manager and Cisco Unity Connection versions that ran on the Windows platform.

Step 8 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

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

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

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

Step 11 Click **Finish**.

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

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

Additional Information

See the Related Topics, page 11-33.

Collecting Audit Logs

The audit user can collect, view, and delete the audit logs. The end user can view the audit logs.

Note Only a user with an audit role can delete the audit logs.

Perform the following procedure to collect audit logs:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard displays.

Step 3 *P*erform one of the following actions in the Action Options window:

- To browse audit logs, check the **Browse Audit Logs** check box.
- To download audit logs, check the **Download Audit Logs** check box.
- To schedule a download of audit logs, check the **Schedule Download of Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard displays.

Step 5 Perform one of the following actions in the Action Options window:

Note If you have a standalone server and check the **Select All Servers** check box, the system will browse, download, or schedule a download of all audit logs for your standalone server.

- To browse, download, or schedule a download of audit logs for all servers, check the **Select All Servers** check box.
- To browse, download, or schedule a download of audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Proceed with one of the following selections:

- Browse Audit Logs, go to Step 7.
- Download Audit Logs, go to Step 12.
- Schedule Download of Audit Logs, go to Step 17.

Step 7 The Remote Browse is Ready window displays. Click the **Close** button.

Step 8 The Nodes pane displays.

Step 9 On the left side of the Nodes pane, double-click on the **Nodes** folder. Navigate through the tree hierarchy until the Audit App folder displays.

Step 10 After the audit log file names display in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view each file or double-click the selected file to display the file in the default viewer.

Step 11 Select an audit log file and perform one of the following actions:

- To download the selected audit log file, click the **Download** button.

  The Select Download Options wizard displays.

a. To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <\Program Files\Cisco\CallManager Serviceability\JRtmt>.

b. To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

c. To delete collected audit log files from the server, check the **Delete Files on Server** check box.

d. Click **Finish**.

- To delete the selected audit log file, click the **Delete** button.
- To refresh the selected audit log file, click the **Refresh** button.
- To refresh all of the audit log files, click the **Refresh All** button.

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

You have completed the steps for Browse Audit Logs.

Step 12 To download audit logs, click **Next**. The Download Audit Logs window displays.

Step 13 In the Nodes Selection Options pane, select one of the following:

- Check the **Select All Servers** checkbox.
- Check a specific node checkbox.

Step 14 In the Collection Time pane, select one of the following radio buttons:

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

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

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

- Relative Range—Specify the length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect audit logs based on the values from the following table:

Period of Time	Range
Minutes	5 - 60
Hours	2 - 24
Days	1 - 31
Weeks	1 - 4
Months	1 -12

Step 15 In the Download File Options pane, select one of the following options:

a. To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <\Program Files\Cisco\CallManager Serviceability\JRtmt>.

b. To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

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

Step 16 Click **Finish**. You have completed the steps for the download of audit logs.

Step 17 The Schedule Download of Audit Logs window displays.

a. In the Nodes Selection Options pane, select one of the following options:

- Check the **Select All Servers** checkbox.
- Check a specific node checkbox.

b. In the Schedule Time pane, perform the following actions:

- Highlight the **Select Reference Server Time Zone**.
- Use the calendar and highlight a **Start Date/Time**.
- Use the calendar and highlight an **End Date/Time**.
- Select the Scheduler Frequency. You may choose Hourly, Daily, Weekly, or Monthly.
- Check the **Zip All Files** checkbox if you want to zip the audit log files.
- Check the **Delete Collected Log Files From Server** checkbox if you want to delete the collected audit log files from the server.

c. In the Action Options pane, check the **Download Files** checkbox.

The Trace Download Configuration Dialog window displays. Enter the following information:

- Protocol—Select FTP (default) or SFTP.

- Host IP Address—Enter the IP address of the host server.
- User Name—Enter your user name.
- Password—Enter your password.
- Port—Enter the FTP or SFTP port information.
- Download Directory Path—Enter the complete directory path where the files get downloaded.
- Click on **Test Connection**. When the connection has been tested, the files are downloaded.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Additional Information

See the Related Topics, page 11-33.

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.

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

Before You Begin

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

- “Collecting Trace Files” section on page 11-3
- “Using the Query Wizard” section on page 11-8
- “Scheduling Trace Collection” section on page 11-12

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

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

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

Step 5 If the file type has a viewer that is already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box displays. Click the program (viewer) that you would like to use to view the file. If your preferred program is not on the list, choose another program by clicking the **Other** button.

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

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

Unified CM and Unified CM BE 5000 only: For more information on using the QRT Viewer, see the "Displaying QRT Report Information" section on page 11-27.

Additional Information

See the Related Topics, page 11-33.

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.

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

Before You Begin

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

- "Collecting Trace Files" section on page 11-3
- "Using the Query Wizard" section on page 11-8
- "Scheduling Trace Collection" section on page 11-12

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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 7.

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

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

Note *Unified CM clusters and Connection clusters only:* You can install some of the listed services/applications only on a particular server in the cluster. To choose traces for those services/applications, make sure that you choose traces from the server on which you have activated the service/application.

Step 4 *Connection* users go to Step 5. For *Unified CM* or *Unified CM BE 5000*, perform one of the following actions in the Select CCM Services/Application tab:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for services or applications, click **Next.**

Go to Step 5 for *Unified CM BE* 5000 or go to Step 6 for *Unified CM*.

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

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.

- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

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

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects system logs for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.
- Go to Step Step 10.

Step 7 *Connection* users go to Step 8. For *Unified CM* or *Unified CM BE 5000*, perform one of the following actions in the Select CCM Services/Application tab:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone server.

- To choose crash dump files for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To choose crash dump files for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To choose crash dump files for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Go to Step 8 for *Unified CM BE* 5000 or go to Step 9 for *Unified CM*.

Step 8 In the Select CUC Services/Application tab, perform one of the following tasks:

- To choose crash dump files for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To choose crash dump files for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

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

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone server.

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

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

Step 10 Click **Finish**.

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

Step 12 Perform one of the following tasks:

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

Tip To sort the files that display 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.

Unified CM and Unified CM BE 5000 only: For more information on using the QRT Viewer, see the "Displaying QRT Report Information" section on page 11-27.

- 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 <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Files on server** check box.
- To delete trace files from the server, click the file that displays in the pane on the right side of the window; then, click the **Delete** button.
- To refresh a specific service or a specific server in a cluster, click the service or server name; then, click the **Refresh** button. After a message states that the remote browse is ready, click **Close**.
- To refresh all services or all servers in a cluster 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 11-22.

Additional Information

See the Related Topics, page 11-33.

Displaying QRT Report Information

Note This section applies only to Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000.

You can view the IP phone problem reports that the Quality Report Tool (QRT) generates by using the QRT viewer. QRT serves as a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. After you collect the QRT log files, you can use the following procedure to list and view Cisco Unified Communications Manager IP Phone problem reports by using the QRT viewer. The QRT viewer allows you to filter, format, and view phone problem reports that are generated. For detailed information about how to configure and use QRT, refer to the *Cisco Unified Communications Manager Features and Services Guide*.

Before You Begin

You can view the QRT log files by either viewing the files on the server or by downloading the files onto your computer.

Collect or View the QRT log files as described in one of the following sections:

- "Collecting Trace Files" section on page 11-3
- "Using the Query Wizard" section on page 11-8
- "Scheduling Trace Collection" section on page 11-12
- "Using Remote Browse" section on page 11-23

After you download the files onto your computer, you can use the Local Browse option in the trace and log central feature as described in the "Using Local Browse" section on page 11-22.

Procedure

Step 1 Display the log file entries by using the Query Wizard, the Remote Browse or the Local Browse option in trace and log central.

The QRT Viewer window displays.

Note Only log files from the Cisco Extended Functions service contain QRT information. The following format for the log file name that contains QRT data applies: qrtXXX.xml.

Step 2 From the Extension drop-down list box, choose the extension(s) that you want the report to include.

Step 3 From the Device drop-down list box, choose the device(s) that you want the report to include.

Step 4 From the Category drop-down list box, choose the problem category that you want the report to include.

Step 5 From the Select Fields drop-down list box, choose the fields that you want the report to include.

Note The order in which you choose the fields determines the order in which they appear in the QRT Report Result pane.

Step 6 To view the report in the QRT Report Result pane, click **Display Records**.

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 11-28
- Monitor User Event, page 11-29

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, with a limit of 3 concurrent sessions on a single server. The log viewer refreshes every 5 seconds. As the traces get rolled into a new file, the generic log viewer appends the content in the viewer.

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

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

Note *Unified CM clusters and Connection clusters only:* 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 and Log Central windows.

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

The View Real Time Data wizard displays.

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

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

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

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

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

Step 7 Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear. Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.

Step 8 Repeat this procedure to view data for additional services.The following limitations apply for your configuration:

Cisco Unified Communications Manager	You can view data for up to 10 services, 5 of which can exist on a single server.
Cisco Unified Communications Manager Business Edition 5000	You can view data for 5 services.
Connection	You can view data for 5 services.

A message displays if you attempt to view data for too many services or too many services on a single server.

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

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

Additional Information

See the Related Topics, page 11-33.

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 performs the action only once. The following limitations apply for your configuration:

Cisco Unified Communications Manager	For each event, you can monitor one service on one server.
Cisco Unified Communications Manager Business Edition 5000	You can monitor one service for each event.
Connection	You can monitor one service for each event.

Before you Begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 10-3.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

Note *Unified CM clusters and Connection clusters only:* 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 and 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 that are configured for the server that you choose display.

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

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

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

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

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

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

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

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

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

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

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

- Alert—Choose this option to generate an alarm when the system encounters the specified search string. For the system to generate the alarm, you must enable the enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 10-3.
- 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.

Note By default, audit events are not sent to the remote syslog server, unless the severity is lowered to Warning, Notice or Informational.

- Download File—Choose this option to download the trace files that contain the specified search string. In the SFTP/FTP Server Parameters group box, choose either FTP or SFTP, enter the server credentials for the server where you want to download the trace files, and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

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

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

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

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

Step 10 Click **Finish**.

Additional Information

See the Related Topics, page 11-33.

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

Tip The Error radio button equals the default setting.

Additional Information

See the Related Topics, page 11-33.

Log Compression

In previous releases of Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000, there were trace service parameters that enabled and disabled log file compression to the hard disk. The service parameters have been deprecated along with that feature.

There is a new implementation of log compression in 8.0, and is not configurable.

The new log compression feature only compresses the following log files:

- cm/trace/cti/sdl
- cm/trace/cti/sdi
- cm/trace/ccm/sdl
- cm/trace/ccm/sdi

The other log files are not compressed and are written directly to the hard disk.

The compressed files have a .gz extension. The file that is being actively written to the disk will have a .gzo extension.

All the CLI commands used to view and tail the files will work on the compressed files and will automatically uncompress them for viewing or tailing. The only difference is in specifying file names with the .gz and .gzo extension.

There is a new option available with the file tail command as follows:

```
file tail activelog cm/trace/cti/sdl recent
```

The recent option, when used with a compressed directory, will continually tail the most recent log file. It is not necessary to switch to a newer log file when the currently written-to log file is closed, so it is an infinite and ongoing tail. This option is only available with the compressed log files.

The log files are compressed in the gzip format. For uncompressing the log files, the open source program 7-Zip is available at http://www.7-zip.org, and works on all Windows platforms. You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip. On a linux platform, you can use the gzip or gunzip commands.

Where to Find More Information

Related Topics

- Using the Query Wizard, page 11-8
- Using Local Browse, page 11-22
- Collecting Trace Files, page 11-3
- Scheduling Trace Collection, page 11-12
- Displaying Trace and Log Central Options in RTMT, page 11-2
- Collecting a Crash Dump, page 11-16
- Using Local Browse, page 11-22

Additional Cisco Documentation

- *Cisco Unified Serviceability Administration Guide*

CHAPTER 12

Using SysLog Viewer

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

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the Syslog Viewer icon.
- Choose **System >Tools > SysLog Viewer> Open SysLog Viewer**.

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

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

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

Tip If some syslog messages do not appear in the window, scrolling the mouse pointer over the missing syslog messages refreshes the display.

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.

Tip CiscoSyslog messages also display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

You can also use the following buttons that are described in Table 12-1 to view the syslog messages:

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

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

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

Table 12-1 Syslog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the syslog viewer. **Tip** You can enable the syslog viewer to automatically update the syslog messages every 5 seconds by checking the Auto Refresh check box.
Clear	Clears the display of the current log.
Filter	Limits the messages that displayed base on the set of options that you select.
Clear Filter	Removes the filter that limits the type of messages that display.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC

Additional Information

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

Where to Find More Information

Related Topics

- Installing and Configuring Cisco Unified Real-Time Monitoring Tool, page 2-1

CHAPTER 13

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 Voice Tools Download**.

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:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the icon of the application in which you are interested.
- Under **System > Tools > Plugin**, choose the plug-in that you want to launch.

The application displays in the plugin window.

Refer to the application document for usage information.

Where to Find More Information

Additional Cisco Documentation

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

PART 5

Analysis Manager

CHAPTER 14

Understanding Cisco Unified Analysis Manager

The Cisco Unified Analysis Manager (Unified Analysis Manager), a tool included with the Cisco Unified Real-Time Monitoring Tool (RTMT), is used to perform troubleshooting operations. When the Unified Analysis Manager is launched, it collects troubleshooting information from your system and provides an analysis of that information. You can use this information to perform your own troubleshooting operation or to send the information to Cisco Technical Assistance for analysis.

The Analysis Manager application is installed as an option when you install the RTMT software. The Analysis Manager interface is accessed from the RTMT main menu and quick launch channel.

Once it is installed, the application can identify the supported UC products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files.

The Unified Analysis Manager will support the following products:

- Cisco Unified Communications Manager (Unified Communications Manager) Release 8.0 (1)
- Cisco Unified Contact Center Enterprise (Unified CCE) Release 8.0(1)
- Cisco Unified Contact Center Express (Unified CCX) Release 8.0(1)
- Cisco IOS Voice Gateways (37xx, 28xx, 38xx, 5350XM, 5400XM) IOS Release PI 11
- Cisco Unity Connection (Unity Connection) Release 8.0(1)
- Cisco Unified Presence (Unified Presence) Release 8.0(2)

The three primary components of the Unified Analysis Manager interface are

- Administration—The system component lets you import device and group configuration from an external file and provide a status of jobs run by the Unified Analysis Manager.
- Inventory —The inventory component is used to identify all of the devices in your system that can be accessed and analyzed by the Unified Analysis Manager.
- Tools —The tools component contains all of the functions that Unified Analysis Manager supports. This includes configuring traces settings, collecting logs and viewing configurations.

How the Unified Analysis Manager Works

The Unified Analysis Manager application is installed as part of the RTMT installation. So once you complete the RTMT installation, you have access to the Unified Analysis Manager features.

The Unified Analysis Manager application is not displayed when RTMT is connected to a Cisco Unity Connection or Cisco Unified Presence server.

When you use RTMT to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition 5000 server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in Unified Analysis Manager.

Where to Find More Information

For more information about RTMT and Cisco Unified Communications Manager, refer to:

- Cisco Unified Communications Manager Release 8.0(1)
- Cisco Unified Communications Manager Business Edition Release 8.0(1)

For more information about products that can be managed with Unified Analysis Manager, refer to:

- Cisco Unified Contact Center Enterprise Release 8.0(1)
- Cisco Unified Contact Center Express Release 8.0(1)
- Cisco Unity Connection Release 8.0(1)
- Cisco Unified Presence Release 8.0(2)

CHAPTER 15

Installing and Configuring Cisco Unified Analysis Manager

You can install Cisco Unified Real-Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 98, Windows XP, Windows 2000, Windows Vista, or Linux with KDE and/or Gnome client.

Note RTMT requires at least 128 MB in memory to run on a Windows operating system platform.

This chapter contains information on the following topics:

- Installing Cisco Unified Real-Time Monitoring Tool, page 15-1
- Uninstalling Cisco Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager, page 15-2
- Launching Cisco Unified Analysis Manager, page 15-3
- Configuring Cisco Unified Analysis Manager, page 15-4
- Importing Configurations, page 15-4
- Displaying Job Status , page 15-4
- Uploading Configuration Files, page 15-5
- Cisco Unified Analysis Manager Preferences, page 15-5

Installing Cisco Unified Real-Time Monitoring Tool

To install the tool, perform the following procedure:

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

Procedure

Step 1 Go to the **Plug-ins** window of the administration interface for your configuration:

Cisco Unified Communications Manager	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Cisco Unified Communications Manager Business Edition 5000	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Cisco Unity Connection	From Cisco Unity Connection Administration, choose **System Settings > Plugins**.

Step 2 Click the **Find** button.

Step 3 To install the Cisco Unified Real-Time Monitoring Tool on a client that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Communications Manager Real-Time Monitoring Tool-Windows.

Step 4 To install the Cisco Unified Real-Time Monitoring Tool on a client that is running the Linux operating system, click the **Download** link for the Cisco Unified Communications Manager Real-Time Monitoring Tool-Linux.

Step 5 Download the executable to the preferred location on your client.

Step 6 To install the Windows version, double-click the Cisco Unified Real-Time Monitoring Tool icon that displays on the desktop or locate the directory where you downloaded the file and run the Cisco Unified Real-Time Monitoring Tool installation file.

Step 7 The extraction process begins.

Step 8 To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: chmod +x CcmServRtmtPlugin.bin

Step 9 After the Unified Real-Time Monitoring Tool welcome window displays, click **Next**.

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

Step 10 Choose the location where you want to install Cisco Unified Real-Time Monitoring Tool. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Step 11 To begin the installation, click **Next**.

Step 12 The Setup Status window displays. Do not click **Cancel**.

Step 13 To complete the installation, click **Finish**.

Uninstalling Cisco Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager

On a Windows client, use Add/Remove Programs under the Control Panel to uninstall Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager (Unified Analysis Manager).

Launching Cisco Unified Analysis Manager

Caution *Unified Communications Manager clusters only.* You must configure a second server as the failover collector in Cisco Unified Communications Manager Administration, so Cisco Unified Real-Time Monitoring Tool can continue to retrieve information if the primary collector fails.

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

The Unified Analysis Manager application is not displayed when Cisco Unified Real-Time Monitoring Tool is connected to a Cisco Unity Connection or Cisco Unified Presence server because these products do not have a Call Record database.

When you use Cisco Unified Real-Time Monitoring Tool to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition 5000 server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in the Unified Analysis Manager.

To launch Unified Analysis Manager, do the following procedure:

Procedure

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

- From your Windows desktop, double-click the **Real Time Monitoring Tool 8.5** icon.
- Choose **Start > Programs > Cisco Unified Serviceability > Real-Time Monitoring Tool**.

The Unified Real-Time Monitoring Tool Login window displays.

Step 2 In the IP Host Address field, enter either the IP address or host name of the server, or (if applicable), first server in a cluster.

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

Step 4 in the Password field, enter the Administrator user password that you established for the username.

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

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

Step 7 Click **OK**.

Step 8 When prompted, add the certificate store by clicking **Yes**.

The Cisco Unified Real-Time Monitoring Tool starts.

Configuring Cisco Unified Analysis Manager

The **Administration** option on the Unified Analysis Manager menu allows you to import device and group configurations from a .csv file to the Unified Analysis Manager tool.

Importing Configurations

This option allows you to import device and group configuration from a .csv file into the Unified Analysis Manager.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration > Import**.

Step 2 Use the Import window to select the .csv configuration file that you want to import.

Step 3 Click the **Import** button. The selected file will display.

Displaying Job Status

This function allows you to display status of scheduled trace setting and log collection jobs. Jobs can be scheduled using the Unified Analysis Manager Tools. Once a device is added to a group, you can schedule trace setting and log collections jobs on the device.

A scheduled job is linked to the machine it is configured on, and the job cannot be run on a different machine. If the machine on which a job was scheduled is not usable for any reason, the old job can be cloned and saved as a new job with new parameters to be run on the new machine.

Jobs running on a device can have one of the following states:

- Scheduled—A job is scheduled within Unified Analysis Manager; however it has not started
- Running—A job that is currently either setting traces or collecting logs
- Completed—A job that is done
- Pending—A job that has completed one run of collecting logs and is waiting to start the next run.
- Aborted—A job that has stopped abnormally due to an unexpected error
- Canceled—A job that has stopped due to a cancel operation by the user.

The Job Status screen gives a system view of all the jobs in Unified Analysis Manager. For jobs that have multiple runs, the status and time of the last run is also shown in this page.

The following operations can be performed on a job:

- View Details—Use this option to get more detailed view of the job.
- Cancel—Use this option to cancel a job. The Cancel operation can only be done on the machine that the job is running or scheduled on. This option cannot be used for jobs that are in the Completed/Aborted/Canceled state.
- Clone—Use this option to select any job and save it as a new job. The job being cloned from can be in any state. This option allows you to change any attribute of the job before saving. Cloning a job does not impact the attributes of the job being cloned.

Uploading Configuration Files

This option allows you to transfer files to a configured FTP server and send an email to interested parties. You can use this option to transfer some files to another machine so they can be viewed by others.

This screen allows you to specify the files and folders to be transferred as well as any annotations to accompany those files.

The following procedure explains how to transfer files to an FTP server:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration > Upload Files**.

Step 2 The **Upload Files** screen displays.

Step 3 In the **Case ID** field, enter the number that Cisco TAC has assigned to the case.

Step 4 Use the drop-down list box in the **Send to Server** field to select the FTP server you are sending the file to.

Step 5 Use the **Notes** box to provide any additional information about the file.

Step 6 Use the **Send Email Notifications** checkbox if you want to add the email addresses to send a notification that the file is uploaded. To add multiple email addresses, add the mail ids separated by comma. The mail addresses can be only the <username> or it can be of the format username@domain.com.

Step 7 In the bottom section of the screen, in the **Files to upload** box, select the files you want to transfer. Use the **Add** or **Remove** buttons to select or deselect files from the system. The files selected will be zipped by default and then uploaded. The name of the zipped file will be of the format <case id>_uploadedfile.zip.

Step 8 Click the **OK** button to transfer the file.

Cisco Unified Analysis Manager Preferences

Use the Unified Analysis Manger dropdown menu to set preferences for:

- FTP Server
- Mail Server
- Trace Collection directory

Setting these preferences is described in the following sections:

- Configuring an FTP Server , page 15-6
- Accessing FTP Server Options, page 15-6
- Adding or Editing an FTP Server, page 15-6
- Configuring a Mail Server , page 15-7
- Adding or Editing a Mail Server and Recipients, page 15-7
- Trace Collection Directory, page 15-8

Configuring an FTP Server

This function allows you to configure a FTP Server which you can then use to export information to. These servers can be Cisco TAC FTP servers. This information can include things such as Logs/trace files, system call trace information, etc.

By default, Cisco's TAC FTP server will be pre-populated. You can modify this configuration for this default FTP server.

The FTP Sever option allows you to manage the configured servers. This includes the following operations:

- Adding a new FTP server
- Editing an existing FTP server
- Deleting FTP servers
- Testing the connection of an FTP server

Cisco TAC has two FTP servers you can configure for exporting files:

- ftp-rtp.cisco.com
- ftp-sj.cisco.com

On both servers, files should be uploaded to the **/incoming** directory.

Accessing FTP Server Options

The following procedure explains how to access the FTP Server Options:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Use the buttons to select the option you want.

Adding or Editing an FTP Server

The following procedure explains how to add an FTP Server or edit and exiting configuration:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. The **Add FTP Server** screen displays.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the FTP server you are adding.

Step 5 In the **Protocol** field, select either the FTP or SFTP protocol, depending on the type of server you are connecting to. Use SFTP if you are connecting to a Cisco TAC server.

Step 6 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the server.

Step 7 In the **Port** field, enter the port number on the server that you will be using.

Step 8 In the **Destination Directory** field, enter the path for the directory to which you will be exporting files. If you are adding a Cisco TAC server, use the **/incoming** directory.

Step 9 Click the **OK** button to add the server. You can use the **Cancel** button to end the operation without adding the FTP server.

Configuring a Mail Server

This option allows you to configure a mail server for the purpose of notifying a set of user configured recipients on the status of Unified Analysis Manager operations such as trace and log collections and file transfers.

You must configure at least one mail server in order to be able to send a notification.

Note You can only use mail servers configured with this option for Unified Analysis Manager notifications. For Cisco Unified Real-Time Monitoring Tool notifications, you must configure a separate mail server.

Adding or Editing a Mail Server and Recipients

The following procedure explains how to add a Mail Server and recipient or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **Mail Server**.

Step 2 The **Mail Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server. The bottom part of the screen shows the recipients listed for each server and buttons to **Add**, **Edit**, or **Delete** a recipient.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. The **Add Mail Server** screen displays.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the Mail server you are adding.

Step 5 In the **Port** field, enter the port number on the server that you will be using.

Step 6 Click the **OK** button to add the server. You can use the **Clear** button to clear the field, or the **Cancel** button to end the operation without adding the Mail server.

Step 7 To add or edit a recipient, go back to the Mail Server screen and Click the **Add** button to add a recipient or the **Edit** button to edit an existing configuration. The **Add Mail Server** screen displays.

Step 8 In the **Email address** field, enter the name or the email address of the recipient you are adding.

Step 9 Click the **OK** button to add the recipient. You can use the **Cancel** button to end the operation without adding the recipient.

Trace Collection Directory

The following procedure explains how to use the Trace Collection option under Preferences to set a directory for trace logs:

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **Trace Collection**.

Step 2 The **Trace Collection** screen displays. Enter the directory you want to use for traces logs in the **Download Directory** box, or use the **Browse** button to locate the directory. Optionally, you can click the **Default** button to select the default dirctory.

Step 3 Click the **Save** button.

CHAPTER 16

Identifying and Adding Nodes to Cisco Unified Analysis Manager

This chapter covers the operations involved with identifying which nodes the Unified Analysis Manager can diagnose. This chapter contains the following sections:

- Managing Nodes, page 16-1
- Managing Groups, page 16-3
- Managing the Trace File Repositories, page 16-4
- Managing the Call Record Repositories, page 16-5
- Defining Trace Templates, page 16-6

Managing Nodes

Once configured, a supported node is added to the Unified Analysis Manager database and will appear on the supported Unified Analysis Manager node list. You can identify a Unified Analysis Manager node in one of three ways:

- Importing node and group configuration from a configuration file.
- Manually entering node and group information with the Unified Analysis Manager screens.
- Discovering Unified Analysis Manager nodes from a seed node. A seed node is one that can return information about all the nodes within a deployment. Once discovered, the nodes can then be added to the node inventory. This option saves you from manually entering details of these nodes.

For Cisco Unified Communications Manager, the first node (publisher) is the seed node. For Cisco Unified Customer Voice Portal (Unified CVP), the Cisco Unified CVP OAMP server is the seed node.

This option allows you to perform Add/Edit/Delete and Discover operations on nodes. All configured Unified Analysis Manager nodes (manually entered, imported from a file, or discovered) will be displayed in the list of nodes.

You can use the Nodes option to perform the following functions:

- Add—The Add button allows you to manually enter a new node.
- Edit—The Edit button allows you to edit a node that has already been configured.
- Delete—The Delete button allows you to delete one or more nodes.

- Discover—You can use the Discover option, which applies only to a seed node. Use the Discover button to send a query to the seed node, which then returns information about all the nodes within that deployment that the seed node is aware of. Once discovered, the nodes are automatically added to the node inventory.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to the node using the configured access information.

Node Summary

The Node summary screen displays all of the nodes currently configured with the Unified Analysis Manager application. Use the following procedure to access the Node summary screen.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Nodes.**

Step 2 The **Node** summary screen displays with a list of configured nodes and buttons to **Add**, **Edit**, **Delete, Discover**. The **Test Connection** button allows you to test connectivity to a node. Nodes are listed by **Name** and **Product Type**.

Adding or Editing a Node

The following procedure explains how to add a node or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Node**. The Node window displays.

Step 2 Click the **Add** button to add a node or select a node from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Node** screen displays.

Note Fields on this screen that are marked with an asterisk (*) are required fields.

Step 3 Use the **Product Type** drop-down list box to select a product.

Step 4 In the **IP/Host Name** field, enter the host name or the IP address of the node you are adding or editing.

Step 5 In the **Transport Protocol** field, select the protocol you want to use. Options for this field depend on the **Product Type** you selected.

Step 6 In the **Port Number** field, enter the port number on the node that you will be using.

Step 7 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the node. Reenter the password in the **Confirm Password** field.

Step 8 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 9 In the **Associated Call Record Repositories** and **Associated Trace File Repositories** fields, use the drop down list to select the respective servers you want to use for the node.

Step 10 Use the **Associated Group** checkboxes if you want to add the node to an existing group.

Step 11 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Node-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 12 Click the **Save** button to add the node. You can use the **Cancel** button to end the operation without adding the node.

Managing Groups

Within Unified Analysis Manager, you can create groups and add nodes to these groups. Once the nodes are added to a group, the user can perform a set of functions (for example, Trace Collection and Trace Setting) at a group level. A single node can belong to multiple groups. Nested groups will not be supported. Copying a group will not be supported.

Note The **AllNodes** group is added by default when a node is added in Unified Analysis Manager. Any nodes added to Unified Analysis Manager are part of the AllNodes group by default. The AllNodes group cannot be edited or deleted.

Note The number of groups you can have is limited to 20 and the number of nodes in a group (with the exception of the AllNodes group) is 20.

You can use the Group option to perform the following functions:

- Add—Use the Add button to create a group. Once a Group is created, you can add nodes to the group.
- Edit—Use the Edit button to select and edit group information. The Edit function also allows you add or delete the node members of the group. You can change which nodes belong to a group by adding or deleting nodes from that group.
- Delete—Use the Delete button to delete a Group. This function deletes that group from the Unified Analysis Manager. However, this function does not delete the individual nodes in the group from the Unified Analysis Manager. Nodes must be deleted individually using the Edit button.

For more information, see the "Adding or Editing a Node" section on page 16-2.

Adding or Editing a Group

The following procedure explains how to add a group or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Node Groups**.

Step 2 The **Groups** window displays. Click the **Add** button to add a group or select a group from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Group** screen displays.

Step 3 Use the **Group Name** field to enter the name of the group.

Step 4 Use the **Group Description** field to enter a brief description of the group.

Step 5 The **Select Nodes** section contains a list of each configured node. To add a node to the group, highlight the node in the list and click the **Add** button.

Step 6 When you have finished selecting nodes for the group, click the **Add** button to add the group or the **Update** button if you are editing the group content. You can use the **Cancel** button to end the operation without adding or editing the group.

Managing the Trace File Repositories

This option allows you to perform Add/Edit/Delete operations on trace file repositories for the Unified Analysis Manager. Managed nodes typically use the trace file repository to off load its trace and log files. The Unified Analysis Manager can then connect to the trace file repository to collect logs and traces.

You can use the Trace File Repository option to perform the following functions:

- Add—The Add button allows you to manually enter a new server.
- Edit —The Edit button allows you to edit a server that has already been configured.
- Delete—The Delete button allows you to delete one or more servers.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to a server using the configured access information.

For more information, see the "Adding or Editing a Trace File Repository" section on page 16-4.

Adding or Editing a Trace File Repository

The following procedure explains how to add a Trace File Repository or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory> Trace File Repositories**.

Step 2 The **Trace File Repositories** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 In the **IP/Hostname** field, enter the name or the IP address of the server you are adding.

Step 4 In the **Transport Protocol** field, use the drop-down list box to select the protocol you want to use, either SFTP or FTP.

Step 5 In the **Port Number** field, enter the port number on the server that you will be using.

Step 6 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the server. Reenter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the server you are adding.

Step 8 In the **Associated Nodes** field, use the check boxes to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Trace File Repository-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Managing the Call Record Repositories

This option allows you to perform Add/Edit/Delete operations on call record repositories for the Unified Analysis Manager. Managed nodes typically see the Call Record Repository to store the call data in a database. The Unified Analysis Manager can then connect to the Call Record Repository to get detailed call data.

You can use the Call Record Repository option to perform the following functions:

- Add—The Add button allows you to manually enter a new server.
- Edit—The Edit button allows you to edit a server that has already been configured.
- Delete—The Delete button allows you to delete one or more servers.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to a server using the configured access information.

For more information, see the "Adding or Editing a Call Record Repository" section on page 16-5.

Adding or Editing a Call Record Repository

The following procedure explains how to add a call record repository or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Call Record Repositories**.

Step 2 The **Call Record Repositories** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 Use the **Repository Type** drop down list to select the product type for the node that will be accessing the server.

Step 4 In the **Hostname** field, enter the name of the server you are adding.

Step 5 In the **JDBC Port** field, enter the port number on the server that you will be using.

Step 6 In the **JDBC User Name** and **JDBC Password** fields, enter the user name and password that gives you access to the server. Re-enter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 8 Use the **Nodes Available for Association** to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Call Record Repository-Advanced** screen. Enter the appropriate information in the **Alternate Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Defining Trace Templates

If you have large number of nodes in a group, the Unified Analysis Manager provides templates as a shortcut for selecting components to change trace levels. You can also use templates to establish the new trace levels for nodes. You can also use template for collecting logs and trace files.

You can use the Templates option to perform the following functions:

- Add—The Add button allows you to create a new template. When adding a template you should note that you are doing so for node types and not actual nodes. For a given node type, there is a known fixed set of components and services.
- Edit—The Edit button allows you to edit an existing template.
- Clone—The Clone button allows you to save an existing template as a new template without replacing the original one.
- Delete—The Delete button allows you to delete a template.
- Import—Use the Import button to import predefined templates from a flat file.
- Export—Use the Export button to export a template to a flat file.

For more information, see the "Adding or Editing a Template" section on page 16-6.

Adding or Editing a Template

The following procedure explains how to add a template or edit an existing configuration:

Note Unified Analysis Manager has default templates which cannot be edited or deleted.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory> Templates**.

Step 2 The **Templates** window displays. Click the **Add** button to add a template or select a template from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Template** screen displays.

Step 3 Use the **Name** field to enter the name of the template.

Step 4 Use the **Description** field to enter a brief description of the group.

Step 5 The **Product Types** section contains a list of products supported by the Unified Analysis Manager. When you select a product from this list, the associated components display in the **Component Name** field.

Step 6 For each component displayed, you can apply a trace level by using the drop down list in the **Trace Level** field.

Note Not all components are available for setting trace levels with this screen.

Step 7 You can indicate if you want to collect trace logs for the component by checking the box in the **Collect** field.

Step 8 Click the **Add** button to add the template or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

CHAPTER 17

Using the Cisco Unified Analysis Manager Tools

The Unified Analysis Manager provides a set of tools that allow you to perform management tasks for specific devices and groups of devices. The following sections describe the tasks you can perform with the Unified Analysis Manager tools:

- Analyze Call Path, page 17-1
- Collect Traces Now, page 17-8
- Schedule Trace Collection, page 17-8
- Setting Trace Levels, page 17-9
- Viewing a Configuration, page 17-10

Analyze Call Path

The Analyze Call Path tool allows you to trace a call between multiple Cisco Unified Communications products. In order to trace a call using the Analyze Call Path tool, a node must be defined in Unified Analysis Manager and the node must belong to a group. See Identifying and Adding Nodes to Cisco Unified Analysis Manager for more information about adding nodes and assigning them to groups.

Note All nodes that you define are assigned to the AllNodes group by default. Use the Node Groups function if you want to assign the node to a different group. See Configuration Considerations for Analyze Call Path for more information on configuring a Call Record Repository before using the Analyze Call Path function.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Analyze Call Path**. The Analyze Call Path Information window displays.

Step 2 Click the **Continue** button. The **Search Criteria** window displays

Step 3 Enter the number where the call originated in the **Calling Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 4 Enter the number where the call terminated in the **Called Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 5 Use the **Termination Cause** drop-down list box to select the reason for the call termination; either Abandoned, Dropped, Failed or all three.

Step 6 Use the **Start Time** field to enter the start time for the trace.

Step 7 Use the **Duration** field to indicate the length of the time period you want to trace.

Step 8 Use the **Time Zone** drop-down list box to select the time zone where you are tracing calls.

Step 9 Use the **Filter Nodes by Group** drop-down list box to select the group of nodes that you want to trace.

Step 10 Use the **and Node Type** drop-down list box to select specific types of nodes that you want to trace. When you have selected the Group and Node, information displays for each node. You can then use the checkbox for each node listed to select or deselect the node.

Note The limit for the number of nodes that you can select at a time is 20.

Step 11 Click the **Run** button to begin the trace. The trace results display on the bottom of the window. If you selected multiple nodes, a tab is displayed for each node. Click on the tab to display information for that node.

Step 12 When the call record information displays, you can click the **View Full Path** button to see the complete call path. You can click the **View Record Details** button to see the information about the call. Use the **Save Results** button to save the reports.

Configuration Considerations for Analyze Call Path

When using the Analyze Call Path tool, there are configuration considerations for each product that the Unified Analysis Manager manages. Refer to the following sections for configuration information for these products.

- Cisco Unified Communications Manager/Cisco Unified Communications Manager Business Edition 5000, page 17-2
- Cisco Unified Contact Center Express, page 17-4
- Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise, page 17-4
- Cisco Unified Customer Voice Portal, page 17-5
- Cisco Access Control Server and Cisco IOS Gateway, page 17-6

The Analyze Call Path tool does not include information for Cisco Unity Connection and Cisco Unified Presence servers.

Cisco Unified Communications Manager/Cisco Unified Communications Manager Business Edition 5000

The following information applies when configuring the Analyze Call Path for Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition 5000:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Cisco Unified Communications Manager and Release 8.0(1) and above for Cisco Unified Communications Manager Business Edition 5000.
- Call Record Repository—For Cisco Unified Communications Manager, use the first node (publisher) as the Call Record Repository with the HTTPS protocol and the default port 8443.

- User Group and Access Permissions— Users should belong to a user group whose role contains read and update permissions required to access Call Records for the following resources:
  - SOAP Call Record APIs
  - SOAP Control Center APIs
  - SOAP Diagnostic Portal Database Service
  - SOAP Log Collection API
  - SOAP Performance Informations APIs
  - SOAP Realtime Informations and Control Center APIs

Note New resources "SOAP Diagnostic Portal Database Service" and "SOAP Call Record APIs" added on an upgrade should not have the read and update permissions by default due to security reasons for existing users. Users need to create or copy the role to custom resources and update the required permissions for above mentioned resources as needed. Refer to *Cisco Unified Communications Manager Administration Guide* for additional details.

- Configuring NTP—Each product installed in the solution should be configured to point to same set of external NTP clock sources. NTP is required to be configured on all nodes that involve calls for SCT features. For Cisco Unified Communications Manager, use the **utils ntp config** CLI command to configure NTP.
- Enable Call Record Logging—In Cisco Unified Communications Manager Administration, go to the Service Parameter Configuration window, and choose the **Cisco CallManager Service**. Enable the **CDR Enabled Flag** and the **CDR Log Calls with Zero Duration Flag** parameters. Restart the **Cisco CallManager** service for change-notification to take effect immediately. Repeat this procedure for all nodes in the Cisco Unified Communications Manager cluster.

Note You can verify that flags are set as desired at https://<HOSTNAME:PORT>/ccmadmin/vendorConfigHelp.do

- CDR CAR Loader—Ensure your CDR Analysis and Reporting (CAR) Loader is set to **Continuous Loading 24/7**. To verify this:
  - Go to the Cisco Unified Serviceability and select **Tools > CDR Analysis and Reporting** (CAR) page. The CAR page opens in a new browser.
  - Go to **System > Scheduler > CDR Load** page.
  - Verify if Loader is not disabled and that **Continuous Loading 24/7** is enabled. This allows CDR records that are generated from Cisco Unified Communications Manager nodes to be loaded into the CAR database as soon as they arrive to Cisco Unified Communications Manager first node (publisher).

  If call records are not found on the Cisco Unified Communications Manager, it is possible that the CAR Loader failed or is having a delay loading the latest CDR records. If this occurs, go to the CAR **System > Database > Manual Purge** page and click the **Table Information** button. Check for the oldest and latest CDR records that are available in the CAR database. If records are not set to the latest date, go to **System > Log Screens > Event Log** and select **CDR Load** to check its recent run status to see if there were any Unsuccessful runs. If CDR Load failure is found, collect CAR Scheduler traces to provide to Cisco Support for troubleshooting.

- Raw Call Record Details—For information on Raw Call Record details help for the Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Call Detail Records Administration Guide* for 8.0(1).

Cisco Unified Contact Center Express

The following information applies when configuring the Analyze Call Path for Unified CCX:

- Version Support—Unified Analysis Manager supports Unified CCX version 8.0(1) and later.
- Call Record Repository—The Call Record Repository used for Unified CCX is either (or both in the case of a High Availability system) of the Unified CCX nodes. The database is active on both nodes and the data is replicated. The JDBC user is **uccxsct** and the password is the encrypted version of the TFTP password. The password is typically set by the Unified CCX administrator.
- Default user for adding Unified CCX Call Record Repository—The Informix user for adding (and connecting to) Unified CCX Call Record Repository is**: uccxsct.** You can reset the default install time password for above user in the Unified CCX Application **Administration > Tools > Password Management** page. Typically, the Unified CCX administrator will reset to the desired password and pass it on to the Unified Analysis Manager administrator.
- User Group and Access Permissions—Unified CCX does not require any additional user group and access permission to access Call Records. The access permissions of the uccxsct user is set by Unified CCX install for read access to specific tables. No external settings are required.
- Configuring NTP—To configure NTP for Unified CCX, go to **OS Administration > Settings > NTP Server**.
- Enable Call Record Logging—Unified CCX always generates Call Records by default, so no configuration is required to enable logging of Call Records.

Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise

The following information applies when configuring the Analyze Call Path for Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Unified CCE:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Unified ICME and Unified CCE.
- Call Record Repository—The Call Record Repository used for Unified ICME is either AW-HDS-DDS or HDS-DDS. The server used for Unified CCE is HDS/AW Database (port 1433).
- User Group and Access Permissions—For Release 8.0(1), the recommended user group and access permissions that are required to access Call records are the Windows only Authentication for SQL Server. This is done by using the **User List** tool from the Configuration Manager and creating a user with the right access privileges.
- Configuring NTP—Configuration for Time Synchronization of Unified CCE servers is based on Microsoft Windows Time Services. When setting up the Unified CCE router component, retain the default settings of the “Disable ICM Time Synchronization” box as checked. With the recommended default setting, the time synchronization for Unified CCE servers is provided by the Windows Time Service, which automatically synchronizes the computer's internal clock across the network. The time source for this synchronization varies, depending on whether the computer is in an Active Directory domain or a workgroup. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at: http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx

- Enable Call Record Logging—To check that Call Record logging is enabled, first be sure that the Unified Analysis Manager service on Unified CCE is enabled. Using the web setup, you need to install the AW-HDS-DDS or HDS-DDS servers with Administration and Data Server roles. Once you install these roles using the web setup, the call records are available by default.
- Raw Call Record Details—To find help for the Raw Call Record details, refer to the Schema Help which you can access from the Unified CCE Administration Tool group on either the AW-HDS-DDS or HDS-DDS server. You can also refer to the United CCE Database Schema Handbook for a specific release.

Cisco Unified Customer Voice Portal

The following information applies when configuring the Analyze Call Path for to Unified CVP:

- Version Support—United Analysis Manager supports Unified CVP Release 8.0(1) and above.
- Call Record Repository—Unified CVP uses the Unified CVP Reporting Server for the Call Record Repository.
- User Group and Access Permissions—Unified CVP uses Unified CVP OAMP to set user group and access permissions required to access Call Records:
  - All users trying to access Unified CVP records from the Unified CVP database need to be created via Unified CVP OAMP.
  - Unified CVP Reporting users need to be granted the Unified CVP Reporting role in Unified CVP OAMP.
  - User passwords may expire if security hardening is installed on the Unified CVP Reporting Server. SNMP monitor displays alerts when this happens.
- Configuring NTP—Configuration for Time Synchronization of the Unified CVP servers is based on Microsoft Windows Time Services. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx.
- Enable Call Record Logging—To ensure that Call Record logging is enabled, do the following:
  - Unified CVP Reporting Server is not installed nor configured by default. Customers and Partners will have to install a Unified CVP Reporting Server to use the Analyze Call Path tool with Unified CVP.
  - Unified CVP Database schema needs to be laid down by the Unified CVP_database_config.bat file. This file needs to be run by the user after Unified CVP Reporting Server installation is completed.
  - Once a Unified CVP Reporting Server is installed, it needs to be configured via Unified CVP OAMP and a Unified CVP Call Server needs to be associated with the Unified CVP Reporting Server.
  - Follow the Unified CVP CAG and RPT guidelines for configuring the Unified CVP Reporting Server, Unified CVP VXML Server, and Unified CVP Call Servers.
  - Unified CVP data retention is 30 days, by default. You can customize this value via Unified CVP OAMP. Unless you back up the database, data will be purged at the end of data retention day. Backed up Unified CVP data is not accessible unless it is imported back into the database.
  - Unified CVP VXML Server filters need to be configured on Unified CVP OAMP. Refer to the Unified CVP OAMP guide for configuring these filters.
- Raw Call Record Details—For information relating to Raw Call Record details, refer to the Unified CVP Reporting Guide for version 7.0(2).

Cisco Access Control Server and Cisco IOS Gateway

The following information applies when configuring the Analyze Call Path for Cisco Access Control (ACS) Servers and Cisco IOS Gateways:

- Version Support—Unified Analysis Manager supports ACS Release 5.1.
- Call Record Repository—To assign a Call Record Repository, one of the acs servers can be configured as a "collector" node.
- User Group and Access Permissions—To set user group and access permissions, after the ACS server is installed, in ssh/telnet access, enter **acsadmin** as the username and **default** as the password, You will be prompted to change the password.
- Configuring NTP—To configure an NTP server on an ACS server, use cli: **ntp server <NTP server IP/host>**.
- Enable Web View—Execute the CLI command acs **config-web-interface view enable** to enable web view. It is disabled by default.
- Cisco IOS gateways as ACS network devices or AAA clients—You need to configure ACS network device to have the correct Radius secret, which is the same secret as the one on the IOS gateway.
  - From acsadmin, access **Network Devices Group > Network Devices and AAA clients** to add the Cisco IOS gateway as the ACS network device or AAA client.
- For IOS configurations:
  - Use the CLI to configure NTP server: ntp server <<NTP server IP/host>
  - Configure Cisco IOS gateway as a Radius client of the ACS server. Sample CLIs are below:

```
aaa new-model
!
!
aaa group server radius acs
server 172.27.25.110 auth-port 1812 acct-port 1813
!
aaa authentication login h323 group acs
aaa authorization exec h323 group acs
aaa accounting connection h323 start-stop group acs
aaa session-id common
gw-accounting aaa
radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

- Be sure you have local login access to your Cisco IOS gateways.
- Enable Call Record Logging—To check that Call Records logging is enabled:
  - aaa accounting connection h323 start-stop group acs
    aaa session-id common
    gw-accounting aaa
    radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
    radius-server key cisco
    radius-server vsa send accounting

Call Definitions

Table 17-1 defines the types of call termination.

Table 17-1 Call Definitions

Call Type	Call Termination Explanation
Failed call	The call is not connected for any reason other than user hang-up before the connection is completed.
Abandoned call	The call is not connected because the user hangs up after initiating the call.
Dropped call	The call is disconnected after connection for any reason other than user hanging up.

Table 17-2 Product Support for Call Types

Call Type	Unified CM/ Unified CMBE	Unified CCE	Unified CVP	Unified CCX
Failed Call	Supported	Supported	Supported	Supported
Abandoned call	Supported	Supported	Not Supported	Supported
Dropped Called	Supported	Supported	Not Supported	Supported

Collecting Traces

Unified Analysis Manager allows you to collect log and trace files from services of supported devices. There are three ways you can collect logs and trace files:

- Collect Traces Now— Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.
- Schedule Trace Collection— Schedule Trace Collection option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time in the future.
- Schedule Trace Settings and Collections—Schedule Trace Settings and Collection option allows you to collect trace files from the present into the future and also specify the trace levels to be used during the scheduled time.

The following sections describe each of the above option:

- Collect Traces Now, page 17-8
- Schedule Trace Collection, page 17-8
- Schedule Trace Settings and Collection, page 17-9

Collect Traces Now

The Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Collect Traces Now**. The Collect Traces Now window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 You can optionally click the **View Summary** button to view the Collection Summary window. This window contain a list of the components associated with the node.

Step 7 Click the **OK** button to start the trace. When the trace is completed, the window displays a Status Summary and Status Details for the trace. The Status Details provide the path to the directory to which the log was sent.

Schedule Trace Collection

Use the Schedule Trace Collection option if you want to collect trace files for any period of time from the present into the future.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Schedule Trace Collection. The Schedule Trace Collection** window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** dropdown field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the **Send Email Notification to** checkbox and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the Collection Summary window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Schedule Trace Settings and Collection

Use the Schedule Trace Settings and Collection option if you want to collect trace files for any period of time from the present into the future and, in addition, also specify the trace levels to be used during the scheduled time. If you change trace settings with this option, trace levels are restored to their default settings after the collection period is over.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Schedule Trace Collection. The Schedule Trace Collection** window displays.

Step 2 Select either the Group to display a list of supported groups or Node, for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device. This option also allows you to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** dropdown field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the Send **Email Notification to** checkbox and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the Collection Summary window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Setting Trace Levels

Use the Set Trace Level option to assign trace levels for a group of devices or individual devices. You can assign trace levels using a template or you can customize trace levels. Trace levels can be set for the following Cisco Unified Communications components:

- Cisco Unified Communications Manager—Allows setting trace levels for Cisco Unified Communications Manager and Common Trace Components.
- Cisco Unified Presence—Allows setting trace levels for Unified Presence and Common Trace Components.
- Cisco Unity Connection—Allows setting trace level for Cisco Unity Connection and Common Trace Components.

- Cisco Unified Contact Center Express—Allows setting trace level only for Common Trace Components.

Table 17-3 describes the general trace level settings for the Cisco Unified Communications components that are managed by Unified Analysis Manager.

Table 17-3 Unified Analysis Manager Trace Level Settings

Trace Level	Guidelines	Expected Volume of Traces
Default	This level should include all traces generated in abnormal paths. This level is intended for coding error traces and error s traces that normally should not occur.	Minimum Traces expected
Warning	This level should include traces for system-level operations. This should include all traces generated by "State Transitions" within components.	Medium Volume of Traces Expected when component is used
Informational	This should include traces that can be used in the lab for debugging difficult problems of the component.	High Volume of Traces Expected when component is used
Debug	This level should include detailed debug information or high volume of messages which are primarily used for debugging.	Very High Volume of Traces Expected when component is used

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Set Trace Level. The Set Trace Level** window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize trace levels for the group or device. If you choose the **Customize** option, the Design Preview dialog displays with a list of supported devices. Choose the device you want and use the **Selected Components** fields to set the trace levels.

Step 4 You can click the **View Changes** button to see any changes made to traces levels for the node. Click **OK** to set the level and exit the screen.

Viewing a Configuration

Use the View Configuration option to view configuration information related to a node. You can collect the version and configuration information and view it in a browser or save the results.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > View Configuration**. The **View Configuration** window displays.

Step 2 The window displays a list of nodes. Select a node and click the **Next** button to display the **Selected Components** screen. This screen lists the Version, Platform, License and other category configuration information for the product.

Step 3 Click the **Finish** button to collect the configuration information. The summary window displays. The window has a **View** and a **Save As** button. User can view the collected information in a browser or save the collected configuration information using the **Save As** button.

CHAPTER 18

Cisco Unified Analysis Manager Troubleshooting and Limitations

This chapter contains the following sections:

- Cisco Unified Analysis Manager Limitations, page 18-1
- Cisco Unified Analysis Manager Troubleshooting, page 18-2

Cisco Unified Analysis Manager Limitations

The following are the limitations you should consider when implementing and using the Unified Analysis Manager.

- The maximum number of call records that the Call Search Report can display is 500.
- The maximum number of call records that the Call Track Report can display is 100.
- Since there is no globally unique callID to use, Unified Analysis Manager uses link-by-link approach to trace the call. If any record for a call is missing in one of the products in the call path, the link will be broken for the rest of the chain and the tracking will not be complete.
- Call records are not stored in the database orderly based on any particular column. When running Call Search Report, the number of returned records is limited to 500. The 500 records that are retrieved may not be the earliest (based on originating time, connection time, or disconnect time) in the specified time range. To make sure all of the call records within the specified time range are retrieved, you need to shorten the time range until the returned number of records is less than 500.
- The Unified Analysis Manager option is not displayed when the Cisco Unified Real-Time Monitoring Tool is connected to a Cisco Unity Connection or Cisco Unified Presence server, because these products do not have a Call Record database.

  When you use the Cisco Unified Real-Time Monitoring Tool to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition 5000 server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in the Unified Analysis Manager.
- Call Tracking does not support tracking of SIP Unified Outbound Option calls from Unified CCE and Unified IME to Cisco IOS gateways.
- Call Tracking does not support direct call tracking of call paths using a GED-125 protocol from Unified CCE to Unified CVP.
- Cisco Unified Communications Manager needs to be in the call path for tracking calls from Cisco Unified Communications Manager.

- Call tracking only supports single branch tracking from Cisco Unified Communications Manager.
- No Call Detail Records (CDR) are generated for calls on the MGCP gateway, as the gateway does not implement call control and Q.931 is backhauled/tunneled to the Cisco Unified Communications Manager for signalling. The CDR is available only on the Cisco Unified Communications Manager.
- With ACS servers, Unified Analysis Manager is used only for call tracing, and then used only if you want to include gateway records and information in the tracing data. If you do not have an ACS server or a supported hardware/software version of the ACS server, most of Unified Analysis Manager functions in your deployment will continue to work; however, your gateway information will not be included in your call traces.

Cisco Unified Analysis Manager Troubleshooting

Table 18-1 provides a list of errors that you may see when testing Unified Analysis Manager connectivity to a node and the suggested action for correcting the errors.

Table 18-1 Test Connectivity Errors and Corrective Actions

No.	Error Code	Message	Corrective Action
1	*NOT_AUTHORIZED_CODE*	Username or password is not correct	Enter the correct username and password.
2	*MISSING_SERVICE_CODE*	Missing Service	The requested web service was not found. Check to see if the web service is down on the target application.
3	*SERVER_BUSY_CODE*	Server is busy	Check to see if there are any other ongoing jobs running on the server. If so, wait until the job is done. If not, wait a few minutes and try again.
4	*INVALID_PORT_CODE*	Invalid Port	The specified port may be syntactically incorrect or may be out of range.
5	*CONNECTION_FAILED_CODE*	Not connected to the specified node	Verify that you have entered the correct address for this node. If the address is correct, then verify that the node is up and that it is reachable.
6	*NOT_SUPPORTED_CODE*	Not supported	This version of the specified product is not supported for this release. Upgrade this product to a supported version.

Table 18-1 Test Connectivity Errors and Corrective Actions (continued)

7	*CERTIFICATE_HANDLING_ERROR_CODE*	SSL handshake failed. The client and server could not negotiate desired level of security	Verify that you have accepted the certificate that was sent to the client from the server.
8	*GENERAL_CONNECTION_ERROR_CODE*	An internal error has occurred	Save the recent Unified Analysis Manager log files and contact Unified Analysis Manager support for help.

PART 6

Cisco Intercompany Media Engine

CHAPTER 19

Cisco Intercompany Media Engine

RTMT provides a set of predefined monitoring objects that assist you in monitoring the health of the Cisco Intercompany Media Engine application. On the Cisco Unified Communications Manager server, you can monitor call processing activity and routing activity of Cisco IME calls. On the Cisco Intercompany Media Engine server you can monitor a variety of statistics related to Internet bandwidth and IME distributed cache status. You need objects from both servers to monitor the performance of the Cisco Intercompany Media Engine product.

This chapter contains information on the predefined objects on the Cisco Intercompany Media Engine server. For information on the objects on the Cisco Unified Communications Manager server, see the "Monitoring Intercompany Media Services" section on page 5-27

This chapter contains the following topics:

- Monitoring IME Service, page 19-1
- Monitoring IME System Performance, page 19-2

Monitoring IME Service

The IME Service category monitors the following items:

- Network Activity—Displays the activity on the Cisco Unified Communications Manager that relates to Cisco Intercompany Media Engine. The Network Activity object displays these charts:
  - IME Distributed Cache Health—Displays the health of the IME distributed cache based on the IMEDistributedCacheHealth counter for the IME Server performance object.
  - IME Distributed Node Count—Displays an approximation of the number of nodes in the IME distributed cache, based on the value of the IMEDistributedCacheNodeCount counter for the IME Server performance object. Because each physical Cisco Intercompany Media Engine server contains multiple nodes, the number that displays in the chart does not indicate the number of physical Cisco Intercompany Media Engine servers that participate in the IME distributed cache.
  - Internet BW Received—Displays the amount of bandwidth in Kbits/s that the Cisco IME service uses for incoming Internet traffic and represents the InternetBandwidthRecv counter for the IME Server performance object.
  - Internet BW Send—Displays the amount in Kbits/s that the Cisco IME service uses for outgoing Internet traffic and represents the InternetBandwidthSend counter for the IME Server performance object.

  - IME Distributed Cache Stored Data Records—Displays the number of IME Distributed Cache records that the Cisco Intercompany Media Engine server stores and represents the IMEDistributedCacheStoredData counter for the IME Server performance object.

To display information on network activity, choose **Cisco IME Service > Network Activity**.

- Server Activity—Allows you to monitor the activity on the Cisco Intercompany Media Engine server. The Server Activity object displays these charts:
  - Number of Registered Clients—Displays the current number of clients that connect to the Cisco IME service and represents the value of the ClientsRegistered counter for the IME Server performance object.
  - IME Distributed Cache Quota—Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Cisco Unified CMs attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
  - IME Distributed Cache Quota Used—Indicates the total number of unique DID numbers that have been configured, to be published via enrolled patterns for Intercompany Media Services, by Cisco Unified CMs currently attached to this IME server.
  - Terminating VCRs—Indicates the total number of IME voice call records that are stored on the Cisco IME server for the terminating side of a call. These records can be used for validation of learned routes.
  - Validations Pending—Displays the number of pending validations on the Cisco IME service as well as the threshold for validations. This chart represents the ValidationsPending counter for the Cisco IME Server performance object.

To display information on server activity, choose **Cisco IME Service > Server Activity**.

Monitoring IME System Performance

The IME System Performance monitoring category provides the SDL Queue object that monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).

To display information on the SDL Queue, choose **Cisco IME Service > SDL Queue**. Select the type from the SDL Queue Type drop-down list box.

PART 7

Performance Counters and Alerts

APPENDIX A

System Performance Objects and Counters

This appendix contains the following sections:

- Cisco Tomcat Connector, page A-2
- Cisco Tomcat JVM, page A-3
- Cisco Tomcat Web Application, page A-4
- Database Change Notification Client, page A-5
- Database Change Notification Server, page A-6
- Database Change Notification Subscription, page A-7
- Database Local DSN, page A-7
- DB User Host Information Counters, page A-7
- Enterprise Replication DBSpace Monitors, page A-7
- Enterprise Replication Perfmon Counters, page A-8
- IP, page A-8
- IP6, page A-9
- Memory, page A-10
- Network Interface, page A-12
- Number of Replicates Created and State of Replication, page A-13
- Partition, page A-13
- Process, page A-14
- Processor, page A-16
- System, page A-16
- TCP, page A-17
- Thread, page A-18
- Where to Find More Information, page A-18

Cisco Tomcat Connector

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

Table A-1 Cisco Tomcat Connector

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

Table A-1 Cisco Tomcat Connector (continued)

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

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by Cisco Unified Communications Manager applications such as Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unity Connection Administration. Table A-2 contains information on the Tomcat JVM counters.

Table A-2 Tomcat JVM

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

Cisco Tomcat Web Application

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

Table A-3 Tomcat Web Application

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that a Cisco Unified Communications Manager-related or Cisco Unity Connection-related web application encountered. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified Communications Manager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified Serviceability gets identified by ccmservice, Cisco Unified Communications Manager User Options gets identified by ccmuser, Cisco Unity Connection Administration (https://<IP Address>:8443/cuadmin) gets identified by cuadmin, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
Requests	This counter represents the total number of requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified Communications Manager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified Serviceability gets identified by ccmservice, Cisco Unified Communications Manager User Options gets identified by ccmuser, Cisco Unity Connection Administration (https://<IP Address>:8443/cuadmin) gets identified by cuadmin, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
SessionsActive	This counter represents the number of sessions that the web application currently has active (in use). The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified Communications Manager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified Serviceability gets identified by ccmservice, Cisco Unified Communications Manager User Options gets identified by ccmuser, Cisco Unity Connection Administration (https://<IP Address>:8443/cuadmin) gets identified by cuadmin, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.

Database Change Notification Client

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

Table A-4 Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	This counter represents the number of database change notifications that have been processed. This counter refreshes every 15 seconds.
MessagesProcessing	This counter represents the number of change notification messages that are currently being processed or are waiting to be processed in the change notification queue for this client. This counter refreshes every 15 seconds.

Table A-4 Database Change Notification Client (continued)

Counters	Counter Descriptions
QueueHeadPointer	This counter represents the head pointer to the change notification queue. The head pointer acts as the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds.
QueueMax	This counter represents the largest number of change notification messages that will be processed for this client. This counter remains cumulative since the last restart of the Cisco Database Layer Monitor service.
QueueTailPointer	This counter represents the tail pointer to the change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds
TablesSubscribed	This counter represents the number of tables in which this client has subscribed.

Database Change Notification Server

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

Table A-5 Database Change Notification Server

Counter	Counter Descriptions
Clients	This counter represents the number of change notification clients (services/servlets) that have subscribed for change notification.
CNProcessed	This counter represents the total number of change notification messages processed by server since reboot.
Queue Delay	This counter provides the number of seconds that the change notification process has messages to process but is not processing them. This condition is true if: • either Change Notification Requests Queued in Database (QueuedRequestsInDB) and Change Notification Requests Queued in Memory (QueuedRequestsInMemory) are non-zero, or • the Latest Change Notification Messages Processed count is not changing. This condition gets checked every 15 seconds.
QueuedRequestsInDB	This counter represents the number of change notification records that are in the DBCNQueue (Database Change Notification Queue) table via direct TCP/IP connection (not queued in shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	This counter represents the number of change notification requests that are queued in shared memory.

Database Change Notification Subscription

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

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

Database Local DSN

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

Table A-6 Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	This counter represents the amount of Ccm DbSpace that is being consumed
CcmtempDbSpace_Used	This counter represents the amount of Ccmtemp DbSpace that is being consumed.
CNDbSpace_Used	This counter represents the percentage of CN dbspace consumed.
LocalDSN	This counter represents the data source name (DSN) that is being referenced from the local machine.
SharedMemory_Free	This counter represents total shared memory that is free.
SharedMemory_Used	This counter total shared memory that is used.
RootDbSpace_Used	This counter represents the amount of RootDbSpace that is being consumed.

DB User Host Information Counters

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

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

Enterprise Replication DBSpace Monitors

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

Table A-7 Enterprise Replication DBSpace Monitors

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

Enterprise Replication Perfmon Counters

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

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

IP

The IP object provides information on the IPv4-related statistics on your system. Table A-8 contains information on the IP counters.

Table A-8 IP

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated at this entity.
Frag Fails	This counter represents the number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that were successfully fragmented at this entity.
In Delivers	This counter represents the number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).
In Discards	This counter represents the number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	This counter represents the number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	This counter represents the total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.

Table A-8 IP (continued)

Counters	Counter Descriptions
Reasm Fails	This counter represents the number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that required reassembly at this entity.

IP6

The IP6 object, which supports Cisco Unified Communications Manager, provides information on the IPv6-related statistics on your system. Table A-9 contains information on the IP counters.

Cisco Unified Communications Manager Business Edition 5000 and Cisco Unity Connection do not support IPv6, so these counters do not apply to Cisco Unified Communications Manager Business Edition 5000 and Cisco Unity Connection.

Table A-9 IP6

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated as a result of fragmentation at this entity.
Frag Fails	This counter represents the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not, for example because their Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that have been successfully fragmented at this entity.
In Delivers	This counter represents the total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol [ICMP]).
In Discards	This counter represents the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
In Receives	This counter represents the number of input datagrams received from all network interfaces, including those received with errors.
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.

Table A-9 IP6 (continued)

Counters	Counter Descriptions
InOut Requests	This counter represents the total number of IP datagrams received and the number of IP datagrams sent.
Out Discards	This counter represents the number of output IP datagrams that was not transmitted and was discarded. One reason may be a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams which local IP user-protocols (including Internet Control Message Protocol [ICMP]) supply to IP in requests transmission. This counter does not include any datagrams counted in ForwDatagrams.
Reasm Fails	This counter represents the number of failures detected by the IP reassembly algorithm (for various reasons, for example timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that have been successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments received which needed to be reassembled at this entity.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. Table A-10 contains information on memory counters.

Table A-10 Memory

Counters	Counter Descriptions
% Mem Used	This counter displays the system physical memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes) / Total KBytes, which also corresponds to the Used KBytes/Total KBytes.
% Page Usage	This counter represents the percentage of active pages.
% VM Used	This counter displays the system virtual memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes) / (Total KBytes + Total Swap KBytes), which also corresponds to Used VM KBytes/Total VM KBytes.
Buffers KBytes	This counter represents the capacity of buffers in your system in kilobytes.
Cached KBytes	This counter represents the amount of cached memory in kilobytes.
Free KBytes	This counter represents the total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	This counter represents the amount of free swap space that is available in your system in kilobytes.

Table A-10 Memory (continued)

Counters	Counter Descriptions
HighFree	This counter represents the amount of free memory in the high region. Linux kernel splits the virtual memory address space into memory regions. The high memory is memory above certain physical address, and its amount depends on the total memory and the type of kernel on the system. For the Cisco Unified Communications Manager system with 4GB memory, the high memory is roughly in the address of 896M to 4096M.
HighTotal	This counter represents the total amount of memory in the high region. Linux kernel splits the virtual memory address space into memory regions. The high memory is memory above certain physical address, and its amount depends on the total memory and the type of kernel on the system. For the Cisco Unified Communications Manager system with 4GB memory, the high memory is roughly in the address of 896M to 4096M.
Page Faults Per Sec	This counter represents the number of page faults (both major and minor) that the system made per second (post 2.5 kernels only). This does not necessarily represent a count of page faults that generate I/O because some page faults can get resolved without I/O.
Low Total	This counter represents the total low (non-paged) memory for kernel.
Low Free	This counter represents the total free low (non-paged) memory for kernel.
Page Major Faults Per Sec	This counter represents the number of major faults that the system has made per second that have required loading a memory page from disk (post 2.5 kernels only).
Pages	This counter represents the number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	This counter represents the number of pages that the system paged in from the disk.
Pages Input Per Sec	This counter represents the total number of kilobytes that the system paged in from the disk per second.
Pages Output	This counter represents the number of pages that the system paged out to the disk.
Pages Output Per Sec	This counter represents the total number of kilobytes that the system paged out to the disk per second.
Shared KBytes	This counter represents the amount of shared memory in your system in kilobytes.
SlabCache	This counter represents all memory used by created slabcaches by various kernel components, as a macroscopic counter representing the sum of all the individual entries in the proc's slabinfo.
SwapCached	This counter represents the amount of Swap used as cache memory. Memory that once was swapped out, is swapped back in, but is still in the swapfile.
Total KBytes	This counter represents the total amount of memory in your system in kilobytes.
Total Swap KBytes	This counter represents the total amount of swap space in your system in kilobytes.
Total VM KBytes	This counter represents the total amount of system physical and memory and swap space (Total Kbytes + Total Swap Kbytes) that is in use in your system in kilobytes.

Table A-10 Memory (continued)

Counters	Counter Descriptions
Used KBytes	This counter represents the amount of system physical memory that is in use on the system in kilobytes. The value of the Used KBytes counter equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes. The Used KBytes value differs from the Linux term that displays in the top or free command output. The Used value that displays in the top or free command output equals the difference in Total KBytes - Free KBytes and also includes the sum of Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your system in kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swap space that is in use on your system in kilobytes. The value equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes. This corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. Table A-11 contains information on network interface counters.

Table A-11 Network Interface

Counters	Counter Descriptions
Rx Bytes	This counter represents the number of bytes, including framing characters, that were received on the interface.
Rx Dropped	This counter represents the number of inbound packets that were chosen to be discarded even though no errors had been detected. This prevents the packet from being delivered to a higher layer protocol. Discarding packets to free up buffer space provides one reason.
Rx Errors	This counter represents the number of inbound packets (packet-oriented interfaces) and the number of inbound transmission units (character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.
Rx Multicast	This counter represents the number of multicast packets that were received on this interface.
Rx Packets	This counter represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This counter represents the total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	This counter represents the total number of Rx packets and Tx packets.
Tx Bytes	This counter represents the total number of octets, including framing characters, that were transmitted out from the interface.

Table A-11 Network Interface (continued)

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

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides real-time replication information for the system. Table A-12 contains information on replication counters.

Table A-12 Number of Replicates Created and State of Replication

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

Partition

The partition object provides information about the file system and its usage in the system. Table A-13 contains information on partition counters. These counters are also available for the spare partition, if present.

Table A-13 Partition

Counters	Counter Descriptions
% CPU Time	Percentage of CPU time that is dedicated to handling IO requests that were issued to the disk.
% Used	This counter represents the percentage of disk space that is in use on this file system.
% Wait in Read	Not Used. The Await Read Time counter replaces this counter. This counter is no longer valid with the counter value -1.
% Wait in Write	Not Used. The Await Write Time counter replaces this counter. This counter is no longer valid with the counter value -1.
Await Read Time	Average time measured in milliseconds, for read requests issued to the device to be served.
Await Time	Average time measured in milliseconds, for I/O requests issued to the device to be served. This includes the time spent by the requests in queue and the time spent servicing them.
Await Write Time	Average time measured in milliseconds, for write requests issued to the device to be served.
Queue Length	Average queue length for the requests that were issued to the disk.
Read Bytes Per Sec	This counter represents the amount of data in bytes per second that was read from the disk.
Total Mbytes	This counter represents the amount of total disk space in megabytes that is on this file system.
Used Mbytes	This counter represents the amount of disk space in megabytes that is in use on this file system.
Write Bytes Per Sec	This counter represents the amount of data that was written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. Table A-14 contains information on process counters.

Table A-14 Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total CPU time, represents the tasks share of the elapsed CPU time since the last update.
% MemoryUsage	This counter represents the percentage of physical memory that a task is currently using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.

Table A-14 Process (continued)

Counters	Counter Descriptions
Page Fault Count	This counter represents the number of major page faults that a task encountered that required the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically wraps, but the value will never equal zero.
Process Status	This counter displays the process status: • 0—Running • 1—Sleeping • 2—Uninterruptible disk sleep • 3—Zombie • 4—Stopped • 5— Paging • 6—Unknown
Shared Memory Size	This counter displays the amount of shared memory (KB) that a task is using. Other processes could potentially share the same memory.
STime	This counter displays the system time (STime), measured in jiffies, that this process has scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second comprises 100 jiffies.
Thread Count	This counter displays the number of threads that are currently grouped with a task. A negative value (-1) indicates that this counter is currently not available. This happens when thread statistics (which includes all performance counters in the Thread object as well as the Thread Count counter in the Process object) are turned off because the system total processes and threads exceeded the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user mode and kernel mode since the start of the task. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second comprises 100 jiffies.
UTime	This counter displays the time, measured in jiffies, that a task has scheduled in user mode.
VmData	This counter displays the virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB). This includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in kilobytes (KB). It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.
Wchan	This counter displays the channel (system call) in which the process is waiting.

Processor

The processor object provides information on different processor time usage in percentages. Table A-15 contains information on processor counters.

Table A-15 Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed CPU time, excluding idle time, since the last update. This share gets expressed as a percentage of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idle state and did not have an outstanding disk I/O request.
IOwait Percentage	This counter represents the percentage of time that the processor is in the idle state while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends executing the interrupt request that is assigned to devices, including the time that the processor spends sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends executing at the user level with nice priority.
Softirq Percentage	This counter represents the percentage of time that the processor spends executing the soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is executing processes in system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is executing normal processes in user (application) level.

System

The System object provides information on file descriptors on your system. Table A-16 contains information on system counters.

Table A-16 System

Counters	Counter Descriptions
Allocated FDs	This counter represents the total number of allocated file descriptors.
Being Used FDs	This counter represents the number of file descriptors that are currently in use in the system.
Freed FDs	This counter represents the total number of allocated file descriptors on the system that are freed.
IOPerSecond	Total number of input/output operations on all disk partitions per second on this server. If you experience a system performance issue, use the information in this counter to measure the impact of the aggregate I/O operations on this server.
IOReadReqMergedPerSecond	Total number of read requests merged per second, that were queued to all devices on this server.

Table A-16 System (continued)

Counters	Counter Descriptions
IOWriteReqMergedPerSecond	Total number of write requests merged per second, that were queued to all devices on this server.
IOReadReqPerSecond	Total number of read requests per second, that were issued to all devices on this server.
IOWriteReqPerSecond	Total number of write requests per second, that were issued to all devices on this server.
IOSectorsReadPerSecond	Total number of sectors read per second from all devices on this server.
IOSectorsWrittenPerSecond	Total number of sectors written per second to all devices on this server.
IOKBytesReadPerSecond	Total number of KBytes read per second from all devices on this server.
IOKBytesWrittenPerSecond	Total number of KBytes written per second to all devices on this server.
IOSectorsReqSizeAvg	Average size in sectors of the requests that were issued to all devices on this server.
IOReqQueueSizeAvg	Average queue length of the requests that were issued to all devices on this server.
IOAwait	Average time in milliseconds, for I/O requests issued to all devices to be served. This includes the time spent by the requests in queue and the time spent servicing the requests.
IOServiceTime	Average service time in milliseconds, for I/O requests that were issued to all devices on this server.
IOCpuUtil	Percentage of CPU time during which I/O requests were issued to the device (bandwidth utilization for the device) on this server.
Max FDs	This counter represents the maximum number of file descriptors that are allowed on the system.
Total CPU Time	This counter represents the total time in jiffies that the system has been up and running.
Total Processes	This counter represents the total number of processes on the system.
Total Threads	This counter represents the total number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system. Table A-17 contains information on the TCP counters.

Table A-17 TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state.

Table A-17 TCP (continued)

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

Thread

The Thread object provides a list of running threads on your system. Table A-18 contains information on the Thread counters.

Table A-18 Thread

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

Where to Find More Information

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX B

Performance Objects and Counters for Cisco Unified Communications Manager

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

- Cisco Analog Access, page B-2
- Cisco Annunciator Device, page B-3
- Cisco Call Restriction, page B-3
- Cisco CallManager, page B-4
- Cisco CallManager System Performance, page B-12
- Cisco CTIManager, page B-14
- Cisco Dual-Mode Mobility, page B-15
- Cisco Extension Mobility, page B-16
- Cisco Gatekeeper, page B-17
- Cisco H.323, page B-17
- Cisco Hunt Lists, page B-18
- Cisco HW Conference Bridge Device, page B-19
- Cisco IP Manager Assistant, page B-20
- Cisco Lines, page B-20
- Cisco Locations, page B-21
- Cisco Media Streaming Application, page B-22
- Cisco Messaging Interface, page B-25
- Cisco MGCP BRI Device, page B-25
- Cisco MGCP FXO Device, page B-26
- Cisco MGCP FXS Device, page B-26
- Cisco MGCP Gateways, page B-27
- Cisco MGCP PRI Device, page B-28
- Cisco MGCP T1 CAS Device, page B-28
- Cisco Mobility Manager, page B-29
- Cisco Music On Hold (MOH) Device, page B-30

- Cisco MTP Device, page B-31
- Cisco Phones, page B-31
- Cisco Presence Feature, page B-32
- Cisco QSIG Feature, page B-32
- Cisco Signaling Performance, page B-33
- Cisco SIP, page B-33
- Cisco SIP Normalization, page B-34
- Cisco SIP Stack, page B-41
- Cisco SIP Station, page B-49
- Cisco SW Conf Bridge Device, page B-51
- Cisco TFTP Server, page B-51
- Cisco Transcode Device, page B-55
- Cisco Video Conference Bridge, page B-55
- Cisco Web Dialer, page B-56
- Cisco WSM Connector, page B-57
- IME Client, page B-57
- IME Client Instance, page B-59

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for Cisco Unified Communications Manager, access the performance monitoring counters in the Cisco Unified Real-Time Monitoring Tool. In RTMT, you can review a counter description, as described in the "Using Performance Queries to Add a Counter" section on page 6-3.

Cisco Analog Access

The Cisco Analog Access object provides information about registered Cisco Analog Access gateways. Table B-1 contains information about Cisco Analog Access counters.

Table B-1 Cisco Analog Access

Counters	Counter Description
OutboundBusyAttempts	This counter represents the total number of times that Cisco Unified Communications Manager attempts a call through the analog access gateway when all ports were busy.
PortsActive	This counter represents the number of ports that are currently in use (active). A port appears active when a call is in progress on that port.
PortsOutOfService	This counter represents the number of ports that are currently out of service. Counter applies only to loop-start and ground-start trunks.

Cisco Annunciator Device

The Cisco Annunciator Device object provides information about registered Cisco annunciator devices. Table B-2 contains information about Cisco Annunciator counters.

Table B-2 Cisco Annunciator Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate an annunciator resource from an annunciator device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the total number of annunciator resources that are currently active (in use) for an annunciator device.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used at the current time for the annunciator device.
ResourceTotal	This counter represents the total number of annunciator resources that are configured for an annunciator device.

Cisco Call Restriction

The Cisco Call Restriction object provides information about the number of failures that result due to logical partitioning policy restrictions. Table B-3 contains information about Cisco Call Restriction counters.

Table B-3 Cisco Call Restriction

Counters	Counter Description
AdHocConferenceFailures	This counter represents the number of attempts that failed to add a participant to an Ad Hoc Conference because the call path between the geolocation of the devices already in conference and the device being invited to the conference was restricted due to a logical partition policy.
BasicCallFailures	This counter represents the number of basic calls that have failed because of logical partition policy restrictions between the geolocations of the called and calling parties. A basic call is any call that does not utilize supplementary services such as transfer, forward, and so on.
ForwardingFailures	This counter represents the number of attempts to forward an incoming call which failed because of a logical partition policy restriction between the geolocations of the two parties involved.
LogicalPartitionFailuresTotal	This counter represents the total number of call attempts that have failed because of a restriction of calls between geolocations of the calling and called parties. This includes the number of failures for Transfer, Ad Hoc Conference, Meet-Me Conference, PickUp, Call Park, Shared Lines and Basic Calls.
MeetMeConferenceFailures	This counter represents the number of attempts that failed to add a participant to a Meet-Me conference because the call path between the geolocation of the devices already in conference and the device attempting to join the conference was restricted due to a logical partition policy.

Table B-3 Cisco Call Restriction (continued)

Counters	Counter Description
MidCallFailures	This counter represents the number of calls that have failed because of a restriction between the geolocations of the called or connected parties after the initial policy check.
ParkRetrievalFailures	This counter represents the number of attempts to perform a Call Park operation that failed because the device that was attempting to retrieve the call had a logical partition policy restriction with the geolocation of the parked party.
PickUpFailures	This counter represents the number of attempts to perform a PickUp operation that failed because the device on which the pickup was being attempted had a logical partition policy restriction with the geolocation of the calling device.
SharedLineFailures	This counter represents the number of attempts to use a shared line which failed because the caller or callee has a logical partition policy restriction with the geolocation of the devices having the shared lines.
TransferFailures	This counter represents the number of call transfer attempts that failed due to restriction of calls between the geolocation of the transferred party and the transferred destination.

Cisco CallManager

The Cisco CallManager object provides information about calls, applications, and devices that are registered with the Cisco Unified Communications Manager. Table B-4 contains information about Cisco CallManager counters.

Table B-4 Cisco CallManager

Counters	Counter Description
AnnunciatorOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate an annunciator resource from those that are registered to a Cisco Unified Communications Manager when none were available.
AnnunciatorResourceActive	This counter represents the total number of annunciator resources that are currently in use on all annunciator devices that are registered with a Cisco Unified Communications Manager.
AnnunciatorResourceAvailable	This counter represents the total number of annunciator resources that are not active and are currently available.
AnnunciatorResourceTotal	This counter represents the total number of annunciator resources that are provided by all annunciator devices that are currently registered with Cisco Unified Communications Manager.
AuthenticatedCallsActive	This counter represents the number of authenticated calls that are currently active (in use) on Cisco Unified Communications Manager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the Transport Layer Security (TLS) authenticated Skinny protocol signaling with Cisco Unified Communications Manager.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
AuthenticatedCallsCompleted	This counter represents the number of authenticated calls that connected and subsequently disconnected through Cisco Unified Communications Manager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco Unified Communications Manager.
AuthenticatedPartiallyRegisteredPhone	This counter represents the number of partially registered, authenticated SIP phones.
AuthenticatedRegisteredPhones	This counter represents the total number of authenticated phones that are registered to Cisco Unified Communications Manager. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco Unified Communications Manager.
BRIChannelsActive	This counter represents the number of BRI voice channels that are currently in an active call on this Cisco Unified Communications Manager.
BRISpansInService	This counter represents the number of BRI spans that are currently available for use.
CallManagerHeartBeat	This counter represents the heartbeat of Cisco Unified Communications Manager. This incremental count indicates that Cisco Unified Communications Manager is up and running. If the count does not increment, that indicates that Cisco Unified Communications Manager is down.
CallsActive	This counter represents the number of voice or video streaming connections that are currently in use (active); in other words, the number of calls that actually have a voice path that is connected on Cisco Unified Communications Manager.
CallsAttempted	This counter represents the total number of attempted calls. An attempted call occurs any time that a phone goes off hook and back on hook, regardless of whether any digits were dialed, or whether it connected to a destination. The system considers some call attempts during feature operations (such as transfer and conference) to be attempted calls.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path or video stream was established) through Cisco Unified Communications Manager. This number increases when the call terminates.
CallsInProgress	This counter represents the number of voice or video calls that are currently in progress on Cisco Unified Communications Manager, including all active calls. When a phone that is registered with Skinny Client Control Protocol (SCCP) goes off hook, the CallsInProgress progress counter increments. until it goes back on hook. For Cisco Unified IP Phones 7902, 7905, 7912, 7940, and 7960 that register with SIP, the CallsInProgress counter increments when the dial softkey is pressed. For all other phones that are running SIP, the CallsInProgress counter increments when the first digit is pressed. When all voice or video calls that are in progress are connected, the number of CallsInProgress represents the number of CallsActive. The counter decreases by one when a phone goes back on hook.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
CM_MediaTermPointsRequestsThrottled	This counter represents the total number of media termination point (MTP) resource requests that have been denied due to throttling (a resource from this MTP was not allocated because, as specified by the Cisco CallManager service parameter, MTP and Transcoder Resource Throttling Percentage, the MTP was being utilized beyond the configured throttle percentage). This counter increments each time a request for an MTP on this Cisco Unified Communications Manager (Unified CM) node is requested and denied due to MTP throttling and reflects a running total since the start of the Cisco CallManager service.
CM_TranscoderRequestsThrottled	This counter represents the total number of transcoder resource requests that have been denied due to throttling (a resource from this transcoder was not allocated because, as specified by the Cisco CallManager service parameter MTP and Transcoder Resource Throttling Percentage, the transcoder was being utilized beyond the configured throttle percentage). This counter increments each time a request for a transcoder on this Cisco Unified Communications Manager (Unified CM) node is requested and denied due to transcoder throttling and reflects a running total since the start of the Cisco CallManager service
EncryptedCallsActive	This counter represents the number of encrypted calls that are currently active (in use) on this Cisco Unified Communications Manager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.
EncryptedCallsCompleted	This counter represents the number of encrypted calls that were connected and subsequently disconnected through this Cisco Unified Communications Manager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.
EncryptedPartiallyRegisteredPhones	This counter represents the number of partially registered, encrypted SIP phones.
EncryptedRegisteredPhones	This counter represents the total number of encrypted phones that are registered on this Cisco Unified Communications Manager.
FXOPortsActive	This counter represents the number of FXO ports that are currently in use (active) on a Cisco Unified Communications Manager.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the system.
FXSPortsActive	This counter represents the number of FXS ports that are currently in use (active) on a Cisco Unified Communications Manager.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the system.
HuntListsInService	This counter represents the number of hunt lists that are currently in service on Cisco Unified Communications Manager.
HWConferenceActive	This counter represents the total number of hardware conference resources that are provided by all hardware conference bridge devices that are currently registered with Cisco Unified Communications Manager.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
HWConferenceCompleted	This counter represents the total number of conferences that used a hardware conference bridge (hardware-based conference devices such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that is allocated from Cisco Unified Communications Manager and that have completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
HWConferenceOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate a hardware conference resource from those that are registered to a Cisco Unified Communications Manager when none was available.
HWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all hardware conference devices (such as Cisco Catalyst 6000, Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are registered with Cisco Unified Communications Manager. System considers conference to be active when one or more calls are connected to a bridge.
HWConferenceResourceAvailable	This counter represents the number of hardware conference resources that are not in use and that are available to be allocated on all hardware conference devices (such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are allocated fromCisco Unified Communications Manager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
HWConferenceResourceTotal	This counter represents the number of active conferences on all hardware conference devices that are registered with Cisco Unified Communications Manager.
InitializationState	This counter represents the current initialization state of Cisco Unified Communications Manager. Cisco Unified Communications Manager includes the following initialization state values: 1-Database; 2-Regions; 3-Locations; 4-QoS Policy; 5-Time Of Day; 6-AAR Neighborhoods; 7-Digit Analysis; 8-Route Plan; 9-Call Control; 10-RSVP Session Manager; 11-Supplementary Services; 12-Directory; 13-SDL Link; 14-Device; 100-Initialization Complete. Not all states display when this counter is used. This does not indicate that an error occurred; it simply indicates that the state(s) initialized and completed within the refresh period of the performance monitor.
LocationOutOfResources	This counter represents the total number of times that a call through Locations failed due to the lack of bandwidth.
MOHMulticastResourceActive	This counter represents the total number of multicast MOH resources that are currently in use (active) on all MOH servers that are registered with a Cisco Unified Communications Manager.
MOHMulticastResourceAvailable	This counter represents the total number of active multicast MOH connections that are not being used on all MOH servers that are registered with a Cisco Unified Communications Manager.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco Unified Communications Manager were already active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH resources or connections that are provided by all MOH servers that are currently registered with a Cisco Unified Communications Manager.
MOHTotalUnicastResources	This counter represents the total number of unicast MOH resources or streams that are provided by all MOH servers that are currently registered with Cisco Unified Communications Manager. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the total number of unicast MOH resources that are currently in use (active) on all MOH servers that are registered with Cisco Unified Communications Manager. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the total number of unicast MOH resources that are currently available on all MOH servers that are registered with Cisco Unified Communications Manager. Each MOH unicast resource uses one stream.
MTPOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted but failed to allocate an MTP resource from one MTP device that is registered with Cisco Unified Communications Manager. This also means that no transcoders were available to act as MTPs.
MTPResourceActive	This counter represents the total number of MTP resources that are currently in use (active) on all MTP devices that are registered with a Cisco Unified Communications Manager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
MTPResourceAvailable	This counter represents the total number of MTP resources that are not in use and are available to be allocated on all MTP devices that are registered with Cisco Unified Communications Manager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
MTPResourceTotal	This counter represents the total number of media termination point (MTP) resources that are provided by all MTP devices that are currently registered with Cisco Unified Communications Manager.
MTP_RequestsThrottled	This counter represents the total number of media termination point (MTP) resource requests that have been denied due to throttling (a resource from this MTP was not allocated because, as specified by the Cisco CallManager service parameter MTP and Transcoder Resource Throttling Percentage, the MTP was being utilized beyond the configured throttle percentage). This counter increments each time a resource is requested from this MTP and is denied due to throttling. This counter reflects a running total since the MTP device registered with the Cisco CallManager service.
PartiallyRegisteredPhone	This counter represents the number of partially registered phones that are running SIP.
PRIChannelsActive	This counter represents the number of PRI voice channels that are in an active call on a Cisco Unified Communications Manager.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
RegisteredAnalogAccess	This counter represents the number of registered Cisco analog access gateways that are registered with system. The count does not include the number of Cisco analog access ports.
RegisteredHardwarePhones	This counter represents the number of Cisco hardware IP phones (for example, Cisco Unified IP Phones 7960, 7940, 7910, and so on.) that are currently registered in the system.
RegisteredMGCPGateway	This counter represents the number of MGCP gateways that are currently registered in the system.
RegisteredOtherStationDevices	This counter represents the number of station devices other than Cisco hardware IP phones that are currently registered in the system (for example, Cisco IP SoftPhone, CTI port, CTI route point, Cisco voice-mail port).
SIPLineServerAuthorizationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that the Cisco Unified Communications Manager server issued to phones that are running SIP. An authentication challenge occurs when a phone that is running SIP with Digest Authentication enabled sends a SIP line request to Cisco Unified Communications Manager.
SIPLineServerAuthorizationFailures	This counter represents the number of authentication challenge failures for incoming SIP requests from SIP phones to the Cisco Unified Communications Manager server. An authentication failure occurs when a SIP phone with Digest Authentication enabled sends a SIP line request with bad credentials to Cisco Unified Communications Manager.
SIPTrunkAuthorization	This counter represents the number of application-level authorization checks for incoming SIP requests that Cisco Unified Communications Manager has issued to SIP trunks. An application-level authorization check occurs when Cisco Unified Communications Manager compares an incoming SIP request to the application-level settings on the SIP Trunk Security Profile Configuration window in Cisco Unified Communications Manager Administration.
SIPTrunkAuthorizationFailures	This counter represents the number of application-level authorization failures for incoming SIP requests that have occurred on Cisco Unified Communications Manager SIP trunks. An application-level authorization failure occurs when Cisco Unified Communications Manager compares an incoming SIP request to the application-level authorization settings on the SIP Trunk Security Profile Configuration window in Cisco Unified Communications Manager Administration and finds that authorization for one or more of the SIP features on that window is not allowed.
SIPTrunkServerAuthenticationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that Cisco Unified Communications Manager issued to SIP trunks. An authentication challenge occurs when a SIP trunk with Digest Authentication enabled sends a SIP request to Cisco Unified Communications Manager.
SIPTrunkServerAuthenticationFailures	This counter represents the number of authentication challenge failures that occurred for incoming SIP requests from SIP trunks to Cisco Unified Communications Manager. An authentication failure occurs when a SIP trunk with Digest Authentication enabled sends a SIP request with bad credentials to Cisco Unified Communications Manager.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
SWConferenceActive	This counter represents the number of active conferences on all software conference devices that are registered with Cisco Unified Communications Manager.
SWConferenceCompleted	This counter represents the total number of conferences that used a software conference bridge that was allocated from a Cisco Unified Communications Manager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
SWConferenceOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate a software conference resource from those that are registered to Cisco Unified Communications Manager when none were available. Counter includes failed attempts to add a new participant to an existing conference.
SWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all software conference devices that are registered with Cisco Unified Communications Manager. The system considers a conference to be active when one or more calls connect to a bridge. One resource equals one stream.
SWConferenceResourceAvailable	This counter represents the number of new software-based conferences that can be started at the same time, for Cisco Unified Communications Manager. You must have a minimum of three streams available for each new conference. One resource equals one stream
SWConferenceResourceTotal	This counter represents the total number of software conference resources that are provided by all software conference bridge devices that are currently registered with Cisco Unified Communications Manager.
SystemCallsAttempted	This counter represents the total number of server-originated calls and attempted calls to the Unity message waiting indicator (MWI).
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are in an active call on a Cisco Unified Communications Manager.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use.
TLSConnectedSIPTrunks	This counter represents the number of SIP trunks that are configured and connected via Transport Layer Security (TLS).
TLSConnectedWSM	This counter represents the number of WSM Connectors that is configured and connected to Motorola WSM via Transport Layer Security (TLS).
TranscoderOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate a transcoder resource from a transcoder device that is registered to a Cisco Unified Communications Manager when none was available.
TranscoderResourceActive	This counter represents the total number of transcoders that are in use on all transcoder devices that are registered with Cisco Unified Communications Manager. A transcoder in use represents one transcoder resource that has been allocated for use in a call. Each transcoder resource uses two streams.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
TranscoderResourceAvailable	This counter represents the total number of transcoders that are not in use and that are available to be allocated on all transcoder devices that are registered with Cisco Unified Communications Manager. Each transcoder resource uses two streams.
TranscoderResourceTotal	This counter represents the total number of transcoder resources that are provided by all transcoder devices that are currently registered with Cisco Unified Communications Manager.
VCBConferenceActive	This counter represents the total number of active video conferences on all video conference bridge devices that are registered with Cisco Unified Communications Manager.
VCBConferenceAvailable	This counter represents the total number of new video conferences on all video conference bridge devices that are registered with Cisco Unified Communications Manager.
VCBConferenceCompleted	This counter represents the total number of video conferences that used a video conference bridge that are allocated from Cisco Unified Communications Manager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
VCBConferenceTotal	This counter represents the total number of video conferences that are supported on all video conference bridge devices that are registered with Cisco Unified Communications Manager.
VCBOutOfConferences	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate a video conference resource from those that are registered to Cisco Unified Communications Manager when none was available.
VCBOutOfResources	This counter represents the total number of failed new video conference requests. A conference request can fail because, for example, the configured number of conferences is already in use.
VCBResourceActive	This counter represents the total number of video conference resources that are currently in use on all video conference devices that are registered with Cisco Unified Communications Manager.
VCBResourceAvailable	This counter represents the total number of video conference resources that are not active and are currently available.
VCBResourceTotal	This counter represents the total number of video conference resources that are provided by all video conference bridge devices that are currently registered with Cisco Unified Communications Manager.
VideoCallsActive	This counter represents the number of active video calls with active video streaming connections on all video conference bridge devices that are registered with Cisco Unified Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams and then released.

Table B-4 Cisco CallManager (continued)

Counters	Counter Description
VideoOutOfResources	This counter represents the total number of times that Cisco Unified Communications Manager attempted to allocate a video-streaming resource from one of the video conference bridge devices that is registered to Cisco Unified Communications Manager when none was available.
XCODE_RequestsThrottled	This counter represents the total number of transcoder resource requests that have been denied due to throttling (a resource from this transcoder was not allocated because, as specified by the Cisco CallManager service parameter MTP and Transcoder Resource Throttling Percentage, the transcoder was being utilized beyond the configured throttle percentage). This counter increments each time a resource is requested from this transcoder and is denied due to throttling. This counter reflects a running total since the transcoder device registered with the Cisco CallManager service.

Cisco CallManager System Performance

The Cisco CallManager System Performance object provides system performance information about Cisco Unified Communications Manager. Table B-5 contains information about Cisco CallManager system performance counters.

Table B-5 Cisco CallManager System Performance

Counters	Counter Description
AverageExpectedDelay	This counter represents the current average expected delay before any incoming message gets handled.
CallsRejectedDueToICTThrottling	This counter represents the total number of calls that were rejected since the start of Cisco CallManager service due to Intercluster Trunk (ICT) call throttling. When the threshold limit of 140 calls per 5 seconds is met, the ICT will start throttling (rejecting) new calls. One cause for ICT call throttling occurs when calls across an ICT enter a route loop condition.
CallThrottlingGenericCounter3	This counter represents a generic counter that is used for call-throttling purpose.
CodeRedEntryExit	This counter indicates whether Cisco Unified Communications Manager has entered or exited a Code state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).
CodeYellowEntryExit	This counter indicates whether Cisco Unified Communications Manager has entered or exited a Code Yellow state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).
EngineeringCounter1	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter2	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter3	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter4	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.

Table B-5 Cisco CallManager System Performance (continued)

Counters	Counter Description
EngineeringCounter5	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter6	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter7	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter8	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the Cisco Unified Communications Manager queue. High-priority signals include timeout events, internal Cisco Unified Communications Manager keepalives, certain gatekeeper events, and internal process creation, among other events. A large number of high-priority events will cause degraded performance on Cisco Unified Communications Manager and result in slow call connection or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 1-High counter to determine the processing delay on Cisco Unified Communications Manager.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the Cisco Unified Communications Manager queue. Normal-priority signals include call-processing functions, key presses, on-hook and off-hook notifications, among other events. A large number of normal-priority events will cause degraded performance on Cisco Unified Communications Manager, sometimes resulting in delayed dial tone, slow call connection, or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the call-processing delay on Cisco Unified Communications Manager. Remember that high-priority signals must complete before normal-priority signals begin to process, so check the high-priority counters as well to get an accurate picture of the potential delay.
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the Cisco Unified Communications Manager queue. Low-priority signals include station device registration (except the initial station registration request message), among other events. A large number of signals in this queue could result in delayed device registration, among other events.
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest priority signals in the Cisco Unified Communications Manager queue. Lowest priority signals include the initial station registration request message during device registration, among other events. A large number of signals in this queue could result in delayed device registration, among other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that Cisco Unified Communications Manager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay on this queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that Cisco Unified Communications Manager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 2-Normal counter to determine the processing delay on this queue. Remember that high-priority signals get processed before normal-priority signals.

Table B-5 Cisco CallManager System Performance (continued)

Counters	Counter Description
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that Cisco Unified Communications Manager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 3-Low counter to determine the processing delay on this queue. The number of signals processed gives an indication of how much device registration activity is being processed in this time interval.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest priority signals that Cisco Unified Communications Manager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 4-Lowest counter to determine the processing delay on this queue. The number of signals that are processed gives an indication of how many devices began the Cisco Unified Communications Manager registration process in this time interval.
QueueSignalsProcessed Total	This counter provides a sum total of all queue signals that Cisco Unified Communications Manager processes for each 1-second period for all queue levels: high, normal, low, and lowest.
SkinnyDevicesThrottled	This counter represents the total number of Skinny devices that are being throttled. A Skinny device gets throttled (asked to shut down and reregister) when the total number of events that the Skinny device generated exceeds the configured maximum threshold value (default value specifies 2000 events) within a 5-second interval.
ThrottlingSampleActivity	This counter indicates how many samples, out of the configured sample size, have non-zero averageExpectedDelay values. This counter resets when any sample has an averageExpectedDelay value of zero. This process repeats for each batch of samples. A batch represents the configured sample size.
TotalCodeYellowEntry	This counter indicates the number of times that Cisco Unified Communications Manager call processing enters the code yellow state. This counter remains cumulative from the start of the Cisco Unified Communications Manager process.

Cisco CTIManager

The Cisco CTI Manager object provides information about Cisco CTI Manager. Table B-6 contains information about Cisco CTIManager counters.

Table B-6 Cisco CTI Manager

Counters	Counter Description
CcmLinkActive	This counter represents the total number of active Cisco Unified Communications Manager links. CTI Manager maintains links to all active servers in a cluster, if applicable.
CTIConnectionActive	This counter represents the total number of CTI clients that are currently connected to the CTIManager. This counter increases by one when new connection is established and decreases by one when a connection is released. The CTIManager service parameter MaxCTIConnections determines the maximum number of active connections.

Table B-6 Cisco CTI Manager (continued)

Counters	Counter Description
DevicesOpen	This counter represents the total number of devices that are configured in Cisco Unified Communications Manager that CTI applications control and/or monitor. Devices include hardware IP phones, CTI ports, CTI route points, and so on.
LinesOpen	This counter represents the total number of lines that are configured in Cisco Unified Communications Manager that control and/or monitor CTI applications.
QbeVersion	This counter represents the version number of the Quick Buffer Encoding (QBE) interface that the CTIManager uses.

Cisco Dual-Mode Mobility

The Cisco Dual-Mode Mobility object provides information about the dual-mode mobility application on Cisco Unified Communications Manager. Table B-7 contains information about Cisco Dual-Mode Mobility counters.

Table B-7 Cisco Dual-Mode Mobility

Counters	Counter Description
CallsAnchored	This counter represents the number of calls that are placed or received on dual-mode phones that are anchored in Cisco Unified Communications Manager. The counter increments when a call is received from or placed to a dual-mode phone. The counter increments twice if a dual-mode phone calls another dual-mode phone.
DMMSRegistered	This counter represents the number of Dual-mode Mobile Station (DMMS) subscribers that are registered in the wireless LAN (WLAN).
FollowMeAborted	This counter represents the number of failed follow-me operations.
FollowMeAttempted	This counter represents the number of follow-me operations that Cisco Unified Communications Manager attempted. The counter increments when a SIP 302 - Moved Temporarily message is received from the Wireless Service Manager (WSM) and Cisco Unified Communications Manager redirects the call to the DMMS in WLAN.
FollowMeCompleted	This counter represents the number of follow-me operations that were successfully completed. The counter increments when the DMMS in WLAN answers the call and the media (voice path) is successfully established with the calling device.
FollowMeInProgress	This counter represents the number of follow-me operations that are currently in progress. The counter increments when a follow-me is attempted, and it decrements when the follow-me operation is aborted or completed.
H1HandOutAttempted	This counter represents the number of H1 hand-out operations that dual-mode phones attempt. The counter increments when Cisco Unified Communications Manager processes a call to the H1 number from a DMMS.
H1HandOutCompleted	This counter represents the number of successfully completed H1 hand-out operations The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).

Table B-7 Cisco Dual-Mode Mobility (continued)

Counters	Counter Description
H2HandOutCompleted	This counter represents the number of successfully completed H2 hand-out operations. The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).
H2HandOutsAttempted	This counter represents the number of H2 hand-out operations that dual-mode phones attempt. The counter increments when Cisco Unified Communications Manager receives a call to the H2 number from a DMMS.
HandInAborted	This counter represents the number of hand-in operations that failed.
HandInAttempted	This counter represents the number of hand-in operations that dual-mode phones attempt.
HandInCompleted	This counter represents the number of successfully completed hand-in operations. The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).
HandInInProgress	This counter represents the number of hand-in operations that are currently in progress. The counter increments when a hand-in is attempted, and the counter decrements when the hand-in is aborted or completed.
HandOutAborted	This counter represents the number of hand-out operations that failed.
HandOutInProgress	This counter represents the number of H1 and H2 hand-out operations that are currently in progress. The counter increments when a H1 or H2 hand-out is attempted, and it decrements when the hand-out is aborted or completed.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application. Table B-8 contains information about Cisco Extension Mobility counters.

Table B-8 Cisco Extension Mobility Application

Counters	Counter Description
RequestsHandled	This counter represents the total number of HTTP requests that the extension mobility application handled since the last restart of the Cisco CallManager service. A typical login would constitute two HTTP requests: one to query the initial login state of the device and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
RequestsInProgress	This counter represents the number of HTTP requests that the extension mobility application currently is handling. A typical login would constitute two HTTP requests: one to query the initial login state of the device and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
RequestsThrottled	This counter represents the total number of Login/Logout Requests that failed due to throttling.
LoginsSuccessful	This counter represents the total number of successful login requests that were completed through EM Service.

Table B-8 Cisco Extension Mobility Application (continued)

Counters	Counter Description
LogoutsSuccessful	This counter represents the total number of successful logout requests that were completed through EM Service
Total Login/LogoutRequestsAttempted	This counter represents the total number of Login and Logout requests that were attempted through this EM Service. This number includes both successful and unsuccessful attempts.

Cisco Gatekeeper

The Cisco Gatekeeper object provides information about registered Cisco gatekeeper devices. Table B-9 contains information about Cisco gatekeeper device counters.

Table B-9 Cisco Gatekeeper

Counters	Counter Description
ACFsReceived	This counter represents the total number of RAS Admission Confirm messages that are received from the configured gatekeeper and its alternate gatekeepers.
ARQsAttempted	This counter represents the total number of RAS Admission Request messages that are attempted by using the configured gatekeeper and its alternate gatekeepers.
RasRetries	This counter represents the number of retries due to loss or delay of all RAS acknowledgement messages on the configured gatekeeper and its alternate gatekeepers.
VideoOutOfResources	This counter represents the total number of video-stream requests to the configured gatekeeper or its alternate gatekeepers that failed, most likely due to lack of bandwidth.

Cisco H.323

The Cisco H.323 object provides information about registered Cisco H.323 devices. Table B-10 contains information about Cisco H.323 device counters.

Table B-10 Cisco H.323

Counters	Counter Description
CallsActive	This counter represents the number of streaming connections that are currently active (in use) on the configured H.323 device; in other words, the number of calls that actually have a voice path that is connected.
CallsAttempted	This counter represents the total number of calls that have been attempted on a device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the total number of successful calls that were made from a device.
CallsInProgress	This counter represents the number of calls that are currently in progress on a device.

Table B-10 Cisco H.323 (continued)

Counters	Counter Description
CallsRejectedDueToICTCallThrottling	This counter represents the total number of calls rejected due to Intercluster Trunk (ICT) call throttling since the start of the Cisco CallManager service. When the system reaches a threshold limit of 140 calls per 5 seconds, ICT will start throttling (rejecting) new calls. One cause for ICT call throttling occurs when calls across an ICT enter a route loop condition.
VideoCallsActive	This counter represents the number of video calls with video streaming connections that are currently active (in use) on all H.323 trunks that are registered with a Cisco Unified Communications Manager; in other words, the number of calls that actually have video-streaming connections on a Cisco Unified Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for all H.323 trunks that were registered with a Cisco Unified Communications Manager. This number increases when the call terminates.

Cisco Hunt Lists

The Cisco Hunt Lists object provides information about the hunt lists that are defined in Cisco Unified Communications Manager Administration. Table B-11 contains information about Cisco hunt list counters.

Table B-11 Cisco Hunt Lists

Counters	Counter Description
CallsAbandoned	This counter represents the number of abandoned calls that occurred through a hunt list. An abandoned call represents one in which a caller hangs up before the call is answered.
CallsActive	This counter represents the number of calls that are currently active (in use) that occurred through a hunt list. An active call represents one that gets distributed and answered, and to which a voice path connects.
CallsBusyAttempts	This counter represents the number of times that calls through a hunt list were attempted when all members of the line and/or route groups were busy.
CallsInProgress	This counter represents the number of calls that are currently in progress through a hunt list. A call in progress represents one that the call distributor is attempting to extend to a member of a line or route group and that has not yet been answered. Examples of a hunt list member include a line, a station device, a trunk device, or a port/channel of a trunk device.
CallsRingNoAnswer	This counter represents the total number of calls through a hunt list that rang but that called parties did not answer.

Table B-11 Cisco Hunt Lists (continued)

Counters	Counter Description
HuntListInService	This counter specifies whether the particular hunt list is currently in service. A value of 0 indicates that the hunt list is out of service; a value of 1 indicates that the hunt list is in service. Reasons that a hunt list could be out of service include the hunt list is not running on a primary Cisco Unified Communications Manager based on its Cisco Unified Communications Manager Group or the hunt list has been disabled in Cisco Unified Communications Manager Administration.
MembersAvailable	This counter represents the total number of available or idle members of line and route groups that belong to an in-service hunt list. An available member currently handles a call and will accept a new call. An idle member does not handle any call and will accept a new call. A hunt list member can comprise a route group, line group, or a combination. A member of a line group represents a directory number of a line on an IP phone or a voice-mail port. A member of a route group represents a station gateway, a trunk gateway, or port/channel of a trunk gateway.

Cisco HW Conference Bridge Device

The Cisco HW Conference Bridge Device object provides information about registered Cisco hardware conference bridge devices. Table B-12 contains information about Cisco hardware conference bridge device counters.

Table B-12 Cisco HW Conference Bridge Device

Counters	Counter Description
HWConferenceActive	This counter represents the number of conferences that are currently active (in use) on a HW conference bridge device. One resource represents one stream.
HWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a HW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a HW conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for this HW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a HW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of resources for a HW conference bridge device. This counter equals the sum of the counters ResourceAvailable and ResourceActive. One resource represents one stream.

Cisco IP Manager Assistant

The Cisco IP Manager Assistant (IPMA) Service object provides information about the Cisco Unified Communications Manager Assistant application. Table B-13 contains information on Cisco IPMA counters.

Table B-13 Cisco IP Manager Assistant Service

Counters	Counter Description
AssistantsActive	This counter represents the number of assistant consoles that are currently active. An active assistant console exists when an assistant is logged in from the assistant console desktop application.
LinesOpen	This counter represents the number of phone lines that the Cisco Unified Communications Manager Assistant application opened. An open phone line exists when the application assumes line control from CTI.
ManagersActive	This counter represents the current number of managers that the Cisco IPMA is servicing.
SessionsCurrent	This counter represents the total number of managers assistants that are currently using the Cisco Unified Communications Manager Assistant application. Each manager and each assistant constitute an active session; so, for one manager/assistant pair, this counter would reflect two sessions.

Cisco Lines

The Cisco Lines object represents the number of Cisco lines (directory numbers) that can dial and connect to a device. Lines represent all directory numbers that terminate on an endpoint. The directory number that is assigned to it identifies the line. The Cisco Lines object does not include directory numbers that include wildcards such as a pattern for a Digital or Analog Access gateway.

The Active counter represents the state of the line, either active or not active. A zero indicates that the line is not in use. When the number is greater than zero, this indicates that the line is active, and the number represents the number of calls that are currently in progress on that line. If more than one call is active, this indicates that the call is on hold either because of being placed on hold specifically (user hold) or because of a network hold operation (for example, a transfer is in progress, and it is on transfer hold). This applies to all directory numbers that are assigned to any device.

Cisco Locations

The Cisco Location object provides information about locations that are defined in Cisco Unified Communications Manager. Table B-14 contains information on Cisco location counters.

Table B-14 Cisco Locations

Counters	Counter Description
BandwidthAvailable	This counter represents the current bandwidth in a given location. A value of 0 indicates that no bandwidth is available.
BandwidthMaximum	This counter represents the maximum bandwidth that is available in a given location. A value of 0 indicates that infinite bandwidth is available.
CallsInProgress	This counter represents the number of calls that are currently in progress on a particular Cisco Unified Communications Manager.
OutOfResources	This counter represents the total number of times that a call on a particular Cisco Unified Communications Manager through the location failed due to lack of bandwidth.
RSVP AudioReservationErrorCounts	This counter represents the number of RSVP reservation errors in the audio stream.
RSVP MandatoryConnectionsInProgress	This counter represents the number of connections with mandatory RSVP that are in progress.
RSVP OptionalConnectionsInProgress	This counter represents the number of connections with optional RSVP that are in progress.
RSVP TotalCallsFailed	This counter represents the number of total calls that failed due to a RSVP reservation failure.
RSVP VideoCallsFailed	This counter represents the number of video calls that failed due to a RSVP reservation failure.
RSVP VideoReservationErrorCounts	This counter represents the number of RSVP reservation errors in the video stream
VideoBandwidthAvailable	This counter represents the bandwidth that is currently available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is available.
VideoBandwidthMaximum	This counter represents the maximum bandwidth that is available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is allocated for video.
VideoOutOfResources	This counter represents the total number of failed video-stream requests (most likely due to lack of bandwidth) in the location where the person who initiated the video conference resides.

Cisco Media Streaming Application

The Cisco IP Voice Media Streaming Application object provides information about the registered MTPs, MOH servers, conference bridge servers, and annunciators. Table B-15 contains information on Cisco IP Voice Media Streaming Application counters.

Note One object exists for each Cisco Unified Communications Manager in the Cisco Unified Communications Manager group that is associated with the device pool that the annunciator device is configured to use.

Table B-15 Cisco Media Streaming Application

Counter	Counter Description
ANNConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified Communications Manager connection was lost.
ANNConnectionState	For each Cisco Unified Communications Manager that is associated with an annunciator, this counter represents the current registration state to Cisco Unified Communications Manager; 0 indicates no registration to Cisco Unified Communications Manager; 1 indicates registration to the primary Cisco Unified Communications Manager; 2 indicates connection to the secondary Cisco Unified Communications Manager (connected to Cisco Unified Communications Manager but not registered until the primary Cisco Unified Communications Manager connection fails).
ANNConnectionsTotal	This counter represents the total number of annunciator instances that have been started since the Cisco IP Voice Media Streaming Application service started.
ANNInstancesActive	This counter represents the number of actively playing (currently in use) announcements.
ANNStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream. One internal stream provides the audio input and another output stream to the endpoint device.
ANNStreamsAvailable	This counter represents the remaining number of streams that are allocated for the annunciator device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for the Annunciator, Call Count) and is reduced by one for each active stream that started.
ANNStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the annunciator device since the Cisco IP Voice Media Streaming Application service started.
CFBConferencesActive	This counter represents the number of active (currently in use) conferences.
CFBConferencesTotal	This counter represents the total number of conferences that started since the Cisco IP Voice Media Streaming Application service started.
CFBConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified Communications Manager connection was lost.

Table B-15 Cisco Media Streaming Application (continued)

Counter	Counter Description
CFBConnectionState	For each Cisco Unified Communications Manager that is associated with a SW Conference Bridge, this counter represents the current registration state to Cisco Unified Communications Manager; 0 indicates no registration to Cisco Unified Communications Manager; 1 indicates registration to the primary Cisco Unified Communications Manager; 2 indicates connection to the secondary Cisco Unified Communications Manager (connected to Cisco Unified Communications Manager but not registered until the primary Cisco Unified Communications Manager connection fails).
CFBStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all conferences. Each stream direction counts as one stream. In a three-party conference, the number of active streams equals 6.
CFBStreamsAvailable	This counter represents the remaining number of streams that are allocated for the conference bridge that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for Conference Bridge, Call Count) and is reduced by one for each active stream started.
CFBStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the conference bridge since the Cisco IP Voice Media Streaming Application service started.
MOHAudioSourcesActive	This counter represents the number of active (currently in use) audio sources for this MOH server. Some of these audio sources may not be actively streaming audio data if no devices are listening. The exception exists for multicast audio sources, which will always be streaming audio. When an audio source is in use, even after the listener has disconnected, this counter will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified Communications Manager connection was lost.
MOHConnectionState	For each Cisco Unified Communications Manager that is associated with an MOH, this counter represents the current registration state to Cisco Unified Communications Manager; 0 indicates no registration to Cisco Unified Communications Manager; 1 indicates registration to the primary Cisco Unified Communications Manager; 2 indicates connection to the secondary Cisco Unified Communications Manager (connected to Cisco Unified Communications Manager but not registered until the primary Cisco Unified Communications Manager connection fails).

Table B-15 Cisco Media Streaming Application (continued)

Counter	Counter Description
MOHStreamsActive	This counter represents the total number of active (currently in use) simplex (one direction) streams for all connections. One output stream exists for each device that is listening to a unicast audio source, and one input stream exists for each active audio source, multiplied by the number of MOH codecs. When an audio source has been used once, it will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MOH device that are available for use. This counter starts as 408 plus the number of configured half-duplex unicast connections and is reduced by 1 for each active stream that started. The counter gets reduced by 2 for each multicast audio source, multiplied by the number of MOH codecs that are configured. The counter gets reduced by 1 for each unicast audio source, multiplied by the number of MOH codecs configured.
MOHStreamsTotal	This counter represents the total number of simplex (one direction) streams that have connected to the MOH server since the Cisco IP Voice Media Streaming Application service started.
MTPConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Streaming Application that a Cisco Unified Communications Manager connection was lost.
MTPConnectionState	For each Cisco Unified Communications Manager that is associated with an MTP, this counter represents the current registration state to Cisco Unified Communications Manager; 0 indicates no registration to Cisco Unified Communications Manager; 1 indicates registration to the primary Cisco Unified Communications Manager; 2 indicates connection to the secondary Cisco Unified Communications Manager (connected to Cisco Unified Communications Manager but not registered until the primary Cisco Unified Communications Manager connection fails).
MTPConnectionsTotal	This counter represents the total number of MTP instances that have been started since the Cisco IP Voice Media Streaming Application service started.
MTPInstancesActive	This counter represents the number of active (currently in use) instances of MTP.
MTPStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream.
MTPStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MTP device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for MTP, Call Count) and is reduced by one for each active stream started.
MTPStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the MTP device since the Cisco IP Voice Media Streaming Application service started.

Cisco Messaging Interface

The Cisco Messaging Interface object provides information about the Cisco Messaging Interface (CMI) service. Table B-16 contains information on Cisco Messaging Interface (CMI) counters.

Table B-16 Cisco Messaging Interface

Counters	Counter Description
HeartBeat	This counter represents the heartbeat of the CMI service. This incremental count indicates that the CMI service is up and running. If the count does not increase (increment), the CMI service is down.
SMDIMessageCountInbound	This counter represents the running count of inbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountInbound24Hour	This counter represents the rolling count of inbound SMDI messages in the last 24 hours.
SMDIMessageCountOutbound	This counter represents the running count of outbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountOutbound24Hour	This counter represents the rolling count of outbound SMDI messages in the last 24 hours.
StartTime	This counter represents the time in milliseconds when the CMI service started. The real-time clock in the computer, which simply acts as a reference point that indicates the current time and the time that has elapsed, in milliseconds, since the service started, provides the basis for this time. The reference point specifies midnight, January 1, 1970.

Cisco MGCP BRI Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP BRI devices. Table B-17 contains information on Cisco MGCP BRI device counters.

Table B-17 Cisco MGCP BRI Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP Basic Rate Interface (BRI) device
Channel 1 Status	This counter represents the status of the indicated B-Channel that is associated with the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates an active call on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-channel or for use as a Synch-Channel for BRI.

Table B-17 Cisco MGCP BRI Device (continued)

Counters	Counter Description
Channel 2 Status	This counter represents the status of the indicated B-Channel that is associated with the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates an active call on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-channel or for use as a Synch-Channel for BRI.
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corresponding digital access gateway. This value will get set to 1 (one) if the Data Link is up (in service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through this MGCP BRI device was attempted when no voice channels are available.

Cisco MGCP FXO Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP FXO devices. Table B-18 contains information on Cisco MGCP FXO device counters.

Table B-18 Cisco MGCP FXO Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were made from the port on an MGCP FXO device.
OutboundBusyAttempts	This counter represents the total number of times that a call through the port on this MGCP FXO device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXO port associated with this MGCP FXO device.

Cisco MGCP FXS Device

The Cisco MGCP Foreign Exchange Station (FXS) Device object provides information about registered Cisco MGCP FXS devices. One instance of this object gets created for each port on a Cisco Catalyst 6000 24 port FXS Analog Interface Module gateway. For example, a fully configured Catalyst 6000 Analog Interface Module would represent 24 separate instances of this object. Table B-19 contains information on Cisco MGCP FXS device counters.

Table B-19 Cisco MGCP FXS Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were made from this port on the MGCP FXS device.

Table B-19 Cisco MGCP FXS Device (continued)

Counters	Counter Description
OutboundBusyAttempts	This counter represents the total number of times that a call through this port on the MGCP FXS device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXS port that is associated with a MGCP FXS device.

Cisco MGCP Gateways

The Cisco MGCP Gateways object provides information about registered MGCP gateways. Table B-20 contains information on Cisco MGCP gateway counters.

Table B-20 Cisco MGCP Gateways

Counters	Counter Description
BRIChannelsActive	This counter represents the number of BRI voice channels that are currently active in a call in the gateway
BRISpansInService	This counter represents the number of BRI spans that are currently available for use in the gateway.
FXOPortsActive	This counter represents the number of FXO ports that are currently active in a call in the gateway.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the gateway.
FXSPortsActive	This counter represents the number of FXS ports that are currently active in a call in the gateway.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the gateway.
PRIChannelsActive	This counter represents the number of PRI voice channels that are currently active in a call in the gateway.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use in the gateway.
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are currently active in a call in the gateway.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use in the gateway.

Cisco MGCP PRI Device

The Cisco MGCP Primary Rate Interface (PRI) Device object provides information about registered Cisco MGCP PRI devices. Table B-21 contains information on Cisco MGCP PRI device counters.

Table B-21 Cisco MGCP PRI Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP PRI device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP PRI device.
Channel 1 Status through Channel 15 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI device. Possible values: 0 (Unknown) indicates that the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
Channel 16 Status	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI Device. Possible values: 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved, for an E1 PRI Interface, this channel is reserved for use as a D-Channel.
Channel 17 Status through Channel 31 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with the MGCP PRI Device. 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved.
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corresponding digital access gateway. This value will be set to 1 (one) if the Data Link is up (in service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through an MGCP PRI device was attempted when no voice channels were available.

Cisco MGCP T1 CAS Device

The Cisco MGCP T1 Channel Associated Signaling (CAS) Device object provides information about registered Cisco MGCP T1 CAS devices. Table B-22 contains information on Cisco MGCP TI CAS device counters.

Table B-22 Cisco MGCP T1 CAS Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP T1 CAS device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP T1 CAS device.

Table B-22 Cisco MGCP T1 CAS Device (continued)

Counters	Counter Description
Channel 1 Status through Channel 24 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with an MGCP T1 CAS device. Possible values: 0 (Unknown) indicates the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
OutboundBusyAttempts	This counter represents the total number of times that a call through the MGCP T1 CAS device was attempted when no voice channels were available.

Cisco Mobility Manager

The Cisco Mobility Manager object provides information on registered Cisco Unified Mobility Manager devices. Table B-23 contains information on Cisco Unified Mobility Manager device counters.

Table B-23 Cisco Mobility Manager

Counters	Counter Description
MobileCallsAnchored	This counter represents the total number of paths that are associated with single-mode/dual-mode phone call that is currently anchored on a Cisco Unified Communications Manager. Call anchoring occurs when a call enters an enterprise gateway and connects to a mobility application that then uses redirection to send the call back out an enterprise gateway. For example, this counter increments twice for a dual-mode phone-to-dual-mode phone call: once for the originating call and once for the terminating call. When the call terminates, this counter decrements accordingly.
MobilityHandinsAborted	This counter represents the total number of aborted handins.
MobileHandinsCompleted	This counter represents the total number of handins that were completed by dual-mode phones. A completed handin occurs when the call successfully connects in the enterprise network and the phone moves from WAN to WLAN.
MobilityHandinsFailed	This counter represents the total number of handins (calls on mobile devices that move from cellular to the wireless network) that failed.
MobilityHandoutsAborted	This counter represents the total number of aborted handouts.
MobileHandoutsCompleted	This counter represents the total number of handouts (calls on mobile devices that move from the enterprise WLAN network to the cellular network) that were completed. A completed handout occurs when the call successfully connects.
MobileHandoutsFailed	This counter represents the total number of handouts (calls on mobile devices that move from cellular to the wireless network) that failed.
MobilityFollowMeCallsAttempted	This counter represents the total number of follow-me calls that were attempted.
MobilityFollowMeCallsIgnoredDueToAnswerTooSoon	This counter represents the total number of follow-me calls that were ignored before the AnswerTooSoon timer went off.
MobilityIVRCallsAttempted	This counter represents the total number of attempted IVR calls.
MobilityIVRCallsFailed	This counter represents the total number of failed IVR calls.

Table B-23 Cisco Mobility Manager (continued)

Counters	Counter Description
MobilityIVRCallsSucceeded	This counter represents the total number of successful IVR calls.
MobilitySCCPDualModeRegistered	This counter represents the total number of dual-mode SCCP devices that are registered.
MobilitySIPDualModeRegistered	This counter represents the total number of dual-mode SIP devices that are registered.

Cisco Music On Hold (MOH) Device

The Cisco Music On Hold (MOH) Device object provides information about registered Cisco MOH devices. Table B-24 contains information on Cisco MOH device counters.

Table B-24 Cisco MOH Device

Counters	Counter Description
MOHHighestActiveResources	This counter represents the largest number of simultaneously active MOH connections for an MOH server. This number includes both multicast and unicast connections.
MOHMulticastResourceActive	This counter represents the number of currently active multicast connections to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHMulticastResourceAvailable	This counter represents the number of multicast MOH connections to multicast addresses that are served by an MOH server that are not active and are still available to be used now for the MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco Unified Communications Manager were already active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH connections that are allowed to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHTotalUnicastResources	This counter represents the total number of unicast MOH connections that are allowed by an MOH server. Each MOH unicast resource uses one stream.

Table B-24 Cisco MOH Device (continued)

Counters	Counter Description
MOHUnicastResourceActive	This counter represents the number of active unicast MOH connections to an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the number of unicast MOH connections that are not active and are still available to be used now for an MOH server. Each MOH unicast resource uses one stream.

Cisco MTP Device

The Cisco Media Termination Point (MTP) Device object provides information about registered Cisco MTP devices. Table B-25 contains information on Cisco MTP device counters.

Table B-25 Cisco MTP Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made to allocate an MTP resource from an MTP device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of MTP resources that are currently in use (active) for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceAvailable	This counter represents the total number of MTP resources that are not active and are still available to be used now for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceTotal	This counter represents the total number of MTP resources that an MTP device provides. This counter equals the sum of the counters ResourceAvailable and ResourceActive.

Cisco Phones

The Cisco Phones object provides information about the number of registered Cisco Unified IP Phones, including both hardware-based and other station devices.

The CallsAttempted counter represents the number of calls that have been attempted from this phone. This number increases each time that the phone goes off hook and on hook.

Cisco Presence Feature

The Cisco Presence object provides information about presence subscriptions, such as statistics that are related to the speed dial or call list Busy Lamp Field (BLF) subscriptions. Table B-26 contains information on Cisco Presence feature.

Table B-26 Cisco Presence

Counters	Counter Description
ActiveCallListAndTrunkSubscriptions	This counter represents the active presence subscriptions for the call list feature as well as presence subscriptions through SIP trunk.
ActiveSubscriptions	This counter represents all active incoming and outgoing presence subscriptions.
CallListAndTrunkSubscriptionsThrottled	This counter represents the cumulative number of rejected call list and trunk side presence subscriptions due to throttling for the call list feature.
IncomingLineSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the line side.
IncomingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the trunk side.
OutgoingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were sent on the trunk side.

Cisco QSIG Feature

The Cisco QSIG Feature object provides information regarding the operation of various QSIG features, such as call diversion and path replacement. Table B-27 contains information on the Cisco QSIG feature counters.

Table B-27 Cisco QSIG Feature

Counters	Counter Description
CallForwardByRerouteCompleted	This counter represents the number of successful calls that has been forwarded by rerouting. Call forward by rerouting enables the path for a forwarded call to be optimized (minimizes the number of B-Channels in use) from the originator perspective. This counter resets when the Cisco CallManager service parameter Call Forward by Reroute Enabled is enabled or disabled, or when the Cisco CallManager service restarts.
PathReplacementCompleted	This counter represents the number of successful path replacements that have occurred. Path replacement in a QSIG network optimizes the path between two edge PINX (PBXs) that are involved in a call. This counter resets when the Cisco CallManager service parameter Path Replacement Enabled is enabled or disabled, or when the Cisco CallManager service restarts.

Cisco Signaling Performance

The Cisco Signaling Performance object provides call-signaling data on transport communications on Cisco Unified Communications Manager. Table B-28 contains information on the Cisco Signaling Performance counter.

Table B-28 Cisco Signaling Performance

Counters	Counter Description
UDPPacketsThrottled	This counter represents the total number of incoming UDP packets that were throttled (dropped) because they exceeded the threshold for the number of incoming packets per second that is allowed from a single IP address. Configure the threshold via the SIP Station UDP Port Throttle Threshold and SIP Trunk UDP Port Throttle Threshold service parameters in Cisco Unified Communications Manager Administration. This counter increments for every throttled UDP packet that was received since the last restart of the Cisco CallManager Service.

Cisco SIP

The Cisco Session Initiation Protocol (SIP) object provides information about configured SIP devices. Table B-29 contains information on the Cisco SIP counters.

Table B-29 Cisco SIP

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on this SIP device.
CallsAttempted	This counter represents the number of calls that have been attempted on this SIP device, including the successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path was established) from a SIP device. This number increments when the call is terminated.
CallsInProgress	This counter represents the number of calls that are currently in progress on a SIP device, including all active calls. When all calls that are in progress are connected, the number of CallsInProgress equals the number of CallsActive.
VideoCallsActive	This counter represents the number of video calls with streaming video connections that are currently active (in use) on this SIP device.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for this SIP device. This number increments when the call is terminated.

Cisco SIP Normalization

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including initialization errors, runtime errors, and script status. Each device that has an associated script causes a new instance of these counters to be created. Table B-30 contains information on the Cisco SIP Normalization counters.

Table B-30 Cisco SIP Normalization

Display Name	Description
DeviceResetAutomatically	This counter indicates the number of times that Cisco Unified CM automatically resets the device (SIP trunk). The device reset is based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. When the device (SIP trunk) is reset due to script errors, the counter value increments. This count restarts when the device is reset manually.
DeviceResetManually	This counter indicates the number of times that the device (SIP trunk) is reset manually in Cisco Unified Communications Manager Administration or by other methods, such as AXL. When the device associated with a script is reset due to configuration changes, the counter value increments. The counter restarts in the following situations: • The SIP trunk is deleted. • The script on the trunk gets changed or deleted. • Cisco Unified Communications Manager restarts.
ErrorExecution	This counter represents the number of execution errors that occurred while the script executed. Execution errors can occur while a message handler executes. Execution errors can be caused by resource errors, an argument mismatch in a function call, and so on. When an execution error occurs, Cisco Unified CM performs the following actions: • Automatically restores the message to the original content before applying additional error handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in Cisco Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an execution error occurs. This counter provides a count from the most recent trunk reset that involved a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again.

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
ErrorInit	This counter represents the number of times a script error occurred after the script successfully loaded into memory, but failed to initialize in Cisco Unified CM. A script can fail to initialize due to resource errors, an argument mismatch in a function call, the expected table was not returned, and so on. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an initialization error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again. When the error occurs during initialization, Cisco Unified CM automatically disables the script.
ErrorInternal	This counter indicates the number of internal errors that occurred while the script executed. Internal errors are very rare. If the value in this counter is higher than zero, a defect exists in the system that is not related to the script content or execution. Collect SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter represents the number of times a script error occurred when the script loaded into memory in Cisco Unified Communications Manager. A script can fail to load due to memory issues or syntax errors. Check the SIPNormalizationScriptError alarm for details. Check the script syntax for errors, upload the corrected script as needed, and reset the trunk. This counter increments every time a load error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone will not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment even after you fix the script problem, examine the script again.
ErrorResource	This counter indicates whether the script encountered a resource error. Two kinds of resource errors exist: exceeding the value in the Memory Threshold field and exceeding the value in the Lua Instruction Threshold field. (Both fields display on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration.) If either condition occurs, Cisco Unified Communications Manager immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled. If a resource error occurs during execution, the configured system resource error recovery action is taken. (The setting of the System Resource Error Recovery Action field on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration defines this action.)

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
MemoryUsage	This counter specifies the amount of memory, in bytes, that the script consumes. This counter increases and decreases to match the amount of memory that the script uses. This count gets cleared when the script closes (because a closed script does not consume memory) and restarts when the script opens (gets enabled). A high number in this counter indicates a resource problem. Check the MemoryUsagePercentage counter and the SIPNormalizationResourceWarning alarm, which occur when the resource consumption exceeds an internally set threshold.
MemoryUsagePercentage	This counter specifies the percentage of the total amount of memory that the script consumes. The value in this counter is derived by dividing the value in the MemoryUsage counter by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying the result by 100 to arrive at a percentage. This counter increases and decreases in accordance with the MemoryUsage counter. This count gets cleared when the script closes (because closed scripts do not consume memory) and restarts when the script opens (gets enabled). When this counter reaches the internally controlled resource threshold, the SIPNormalizationResourceWarning alarm is issued.
MessageRollback	This counter indicates the number of times that the system automatically rolled back a message. The system rolls back the message by using the error handling that is specified in the Script Execution Error Recovery Action field in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. When an execution error occurs, Cisco Unified CM automatically restores the message to the original content before applying additional error handling actions. If error handling specifies Rollback only, no further action is taken beyond rolling back to the original message before the normalization attempt. For the other possible Script Execution Error Recovery Actions, message rollback always occurs first, followed by the specified action, such as disabling the script, resetting the script automatically, or resetting the trunk automatically.
msgAddContentBody	This counter represents the number of times that the script added a content body to the message. If you are using the msg:addContentBody API in the script, this counter increases each time that the msg:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeader	This counter represents the number of times that the script added a SIP header to the message. If you are using the msg:addHeader API in the script, this counter increases each time that the msg:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to a SIP header in the message. If you are using the msg:addHeaderUriParameter API in the script, this counter increases each time that the msg:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
msgAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to a SIP header in the message. If you are using the msg:addHeaderValueParameter API in the script, this counter increases each time that the msg:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgApplyNumberMask	This counter represents the number of times that the script applied a number mask to a SIP header in the message. If you are using the msg:applyNumberMask API in the script, this counter increases each time that the msg:applyNumberMask API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgBlock	This counter represents the number of times that the script blocked a message. If you are using the msg:block API in the script, this counter increases each time that the msg:block API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgConvertDiversionToHI	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgConvertHIToDiversion	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgModifyHeader	This counter represents the number of times that the script modified a SIP header in the message. If you are using the msg:modifyHeader API in the script, this counter increases each time that the msg:modifyHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveContentBody	This counter represents the number of times that the script removed a content body from the message. If you are using the msg:removeContentBody API in the script, this counter increases each time that the msg:removeContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeader	This counter represents the number of times that the script removed a SIP header from the message. If you are using the msg:removeHeader API in the script, this counter increases each time that the msg:removeHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeaderValue	This counter represents the number of times that the script removed a SIP header value from the message. If you are using the msg:removeHeaderValue API in the script, this counter increases each time that the msg:removeHeaderValue API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetRequestUri	This counter represents the number of times that the script modified the request URI in the message. If you are using the msg:setRequestUri API in the script, this counter increases each time that the msg:setRequestUri API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
msgSetResponseCode	This counter represents the number of times that the script modified the response code and/or response phrase in the message. If you are using the msg:setResponseCode API in the script, this counter increases each time that the msg:setResponseCode API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetSdp	This counter represents the number of times that the script set the SDP in the message. If you are using the msg:setSdp API in the script, this counter increases each time that the msg:setSdp API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddContentBody	This counter represents the number of times that the script added a content body to the PassThrough (pt) object. If you are using the pt:addContentBody API in the script, this counter increases each time that the pt:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeader	This counter represents the number of times that the script added a SIP header to the PassThrough (pt) object. If you are using the pt:addHeader API in the script, this counter increases each time that the pt:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to the PassThrough (pt) object. If you are using the pt:addHeaderUriParameter API in the script, this counter increases each time that the pt:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to the PassThrough (pt) object. If you are using the pt:addHeaderValueParameter API in the script, this counter increases each time that the pt:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddRequestUriParameter	This counter represents the number of times that the script added a request URI parameter to the PassThrough (pt) object. If you are using the pt:addRequestUriParameter API in the script, this counter increases each time that the pt:addRequestUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ScriptActive	This counter indicates whether the script is currently active (running on the trunk). The following values display for the counter: • 0—Indicates that the script is closed (disabled). • 1—Indicates that the script is open and operational. To open the script that should be running on this trunk, perform the following actions: 1. Check for any alarms that might indicate why the script is not open. 2. Correct any errors. 3. Upload a new script if necessary. 4. Reset the trunk.

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
ScriptClosed	This counter indicates the number of times that Cisco Unified Communications Manager has closed the script. When the script is closed, it is not enabled on this device. Cisco Unified CM closes the script under one of the following conditions: • The device was reset manually. • The device was reset automatically (due to an error). • The device was deleted. This count restarts when the SIP trunk is reset after a change to the script configuration and when Cisco Unified CM restarts.
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disabled the script. The values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration determine whether the script is disabled. The script also gets disabled as a result of script error conditions that are encountered during loading and initialization. This counter provides a count from the most recent manual device reset that involved a script configuration change (a device reset alone does not restart the count; the script must also have changed before the reset occurs). This counter increments every time Cisco Unified CM automatically disables a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Table B-30 Cisco SIP Normalization (continued)

Display Name	Description
ScriptOpened	This counter indicates the number of times that the Cisco Unified CM attempted to open the script. For the a script to open, it must load into memory in Cisco Unified CM, initialize, and be operational. A number greater than one in this counter means that Cisco Unified CM has made more than one attempt to open the script on this SIP trunk, either for an expected reason or due to an error during loading or initialization. The error can occur due to execution errors or resource errors or invalid syntax in the script. Expect this counter to be greater than one if any of these counters increment: DeviceResetManually, DeviceResetAutomatically, or ScriptResetAutomatically. The DeviceResetManually counter increments when an expected event, such as a maintenance window on the SIP trunk, causes the script to close. If the number in this counter is high for an unexpected reason, perform the following actions: • Check for alarms, such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the SIP trunk resets after a script configuration change and when Cisco Unified CM restarts.
ScriptResetAutomatically	This counter indicates the number of times that the system automatically reset the script. The script resets based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. This counter specifies a count of the number of automatic script resets after the last manual device reset; this counter increments every time the Cisco Unified CM automatically resets a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Cisco SIP Stack

The Cisco SIP Stack object provides information about Session Initiation Protocol (SIP) stack statistics that are generated or used by SIP devices such as SIP Proxy, SIP Redirect Server, SIP Registrar, and SIP User Agent. Table B-31 contains information on Cisco SIP Stack counters.

Table B-31 Cisco SIP Stack

Counters	Counter Description
AckIns	This counter represents the total number of ACK requests that the SIP device received.
AckOuts	This counter represents the total number of ACK requests that the SIP device sent.
ByeIns	This counter represents the total number of BYE requests that the SIP device received. This number includes retransmission.
ByeOuts	This counter represents the total number of BYE requests that the SIP device sent. This number includes retransmission.
CancelIns	This counter represents the total number of CANCEL requests that the SIP device received. This number includes retransmission.
CancelOuts	This counter represents the total number of CANCEL requests that the SIP device sent. This number includes retransmission.
CCBsAllocated	This counter represents the number of Call Control Blocks (CCB) that are currently in use by the SIP stack. Each active SIP dialog uses one CCB.
GlobalFailedClassIns	This counter represents the total number of 6xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that a SIP device, that is providing a client function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.
GlobalFailedClassOuts	This counter represents the total number of 6xx class SIP responses that the SIP device sent. This number includes retransmission. This class of responses indicates that a SIP device, that is providing a server function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.
InfoClassIns	This counter represents the total number of 1xx class SIP responses that the SIP device received. This includes retransmission. This class of responses provides information on the progress of a SIP request.
InfoClassOuts	This counter represents the total number of 1xx class SIP responses that the SIP device sent. This includes retransmission. This class of responses provides information on the progress of processing a SIP request.
InfoIns	This counter represents the total number of INFO requests that the SIP device has received. This number includes retransmission.
InfoOuts	This counter represents the total number of INFO requests that the SIP device has sent. This number includes retransmission.
InviteIns	This counter represents the total number of INVITE requests that the SIP device received. This number includes retransmission.

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
InviteOuts	This counter represents the total number of INVITE requests that the SIP device has sent. This number includes retransmission.
NotifyIns	This counter represents the total number of NOTIFY requests that the SIP device has received. This number includes retransmission.
NotifyOuts	This counter represents the total number of NOTIFY requests that the SIP device has sent. This number includes retransmission.
OptionsIns	This counter represents the total number of OPTIONS requests that the SIP device received. This number includes retransmission.
OptionsOuts	This counter represents the total number of OPTIONS requests that the SIP device has sent. This number includes retransmission.
PRAckIns	This counter represents the total number of PRACK requests that the SIP device has received. This number includes retransmission.
PRAckOuts	This counter represents the total number of PRACK requests that the SIP device has sent. This number includes retransmission.
PublishIns	This counter represents the total number of PUBLISH requests that the SIP device received. This number includes retransmissions.
PublishOuts	This counter represents the total number of PUBLISH requests that the SIP device has sent. This number includes retransmission
RedirClassIns	This counter represents the total number of 3xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
RedirClassOuts	This counter represents the total number of 3xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
ReferIns	This counter represents the total number of REFER requests that the SIP device has received. This number includes retransmission.
ReferOuts	This counter represents the total number of REFER requests that the SIP device has sent. This number includes retransmission.
RegisterIns	This counter represents the total number of REGISTER requests that the SIP device has received. This number includes retransmission.
RegisterOuts	This counter represents the total number of REGISTER requests that the SIP device has sent. This number includes retransmission.
RequestsFailedClassIns	This counter represents the total number of 4xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a client function.
RequestsFailedClassOuts	This counter represents the total number of 4xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a server function.
RetryByes	This counter represents the total number of BYE retries that the SIP device has sent. To determine the number of first BYE attempts, subtract the value of this counter from the value of the sipStatsByeOuts counter.

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
RetryCancels	This counter represents the total number of CANCEL retries that the SIP device has sent. To determine the number of first CANCEL attempts, subtract the value of this counter from the value of the sipStatsCancelOuts counter.
RetryInfo	This counter represents the total number of INFO retries that the SIP device has sent. To determine the number of first INFO attempts, subtract the value of this counter from the value of the sipStatsInfoOuts counter.
RetryInvites	This counter represents the total number of INVITE retries that the SIP device has sent. To determine the number of first INVITE attempts, subtract the value of this counter from the value of the sipStatsInviteOuts counter.
RetryNotify	This counter represents the total number of NOTIFY retries that the SIP device has sent. To determine the number of first NOTIFY attempts, subtract the value of this counter from the value of the sipStatsNotifyOuts counter.
RetryPRAck	This counter represents the total number of PRACK retries that the SIP device has sent. To determine the number of first PRACK attempts, subtract the value of this counter from the value of the sipStatsPRAckOuts counter.
RetryPublish	This counter represents the total number of PUBLISH retries that the SIP device has been sent. To determine the number of first PUBLISHs attempts, subtract the value of this counter from the value of the sipStatsPublishOuts counter.
RetryRefer	This counter represents the total number of REFER retries that the SIP device has sent. To determine the number of first REFER attempts, subtract the value of this counter from the value of the sipStatsReferOuts counter.
RetryRegisters	This counter represents the total number of REGISTER retries that the SIP device has sent. To determine the number of first REGISTER attempts, subtract the value of this counter from the value of the sipStatsRegisterOuts counter.
RetryRel1xx	This counter represents the total number of Reliable 1xx retries that the SIP device has sent.
RetryRequestsOut	This counter represents the total number of Request retries that the SIP device has sent.
RetryResponsesFinal	This counter represents the total number of Final Response retries that the SIP device has sent.
RetryResponsesNonFinal	This counter represents the total number of non-Final Response retries that the SIP device has sent.
RetrySubscribe	This counter represents the total number of SUBSCRIBE retries that the SIP device has sent. To determine the number of first SUBSCRIBE attempts, subtract the value of this counter from the value of the sipStatsSubscribeOuts counter.
RetryUpdate	This counter represents the total number of UPDATE retries that the SIP device has sent. To determine the number of first UPDATE attempts, subtract the value of this counter from the value of the sipStatsUpdateOuts counter.
SCBsAllocated	This counter represents the number of Subscription Control Blocks (SCB) that are currently in use by the SIP stack. Each subscription uses one SCB.
ServerFailedClassIns	This counter represents the total number of 5xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a client function.

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
ServerFailedClassOuts	This counter represents the total number of 5xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a server function.
SIPGenericCounter1	Do not use this counter unless directed to do so by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter2	Do not use this counter unless directed to do so by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter3	Do not use this counter unless directed to do so by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter4	Do not use this counter unless directed to do so by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
SIPHandlerSDLQueueSignalsPresent	This counter represents the number of SDL signals that are currently on the four SDL priority queues of the SIPHandler component. The SIPHandler component contains the SIP stack.
StatusCode1xxIns	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has received. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode1xxOuts	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has sent. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode2xxIns	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has received. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
StatusCode2xxOuts	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has sent. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted
StatusCode3xxins	This counter represents the total number of 3xx response messages, including retransmission, that the SIP device has received. This count includes the following 3xx responses: • 300 Multiple Choices • 301 Moved Permanently • 302 Moved Temporarily • 303 Incompatible Bandwidth Units • 305 Use Proxy • 380 Alternative Service
StatusCode302Outs	This counter represents the total number of 302 Moved Temporarily response messages, including retransmission, that the SIP device has sent.

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
StatusCode4xxIns	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has received. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
StatusCode4xxOuts	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has sent. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
StatusCode5xxIns	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has received. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode5xxOuts	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has sent. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode6xxIns	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has received. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
StatusCode6xxOuts	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has sent. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
SubscribeIns	This counter represents the total number of SUBSCRIBE requests that the SIP device has received. This number includes retransmission.
SubscribeOuts	This counter represents the total number of SUBSCRIBE requests that the SIP device has sent. This number includes retransmission.

Table B-31 Cisco SIP Stack (continued)

Counters	Counter Description
SuccessClassIns	This counter represents the total number of 2xx class SIP responses that the SIP device has received. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SuccessClassOuts	This counter represents the total number of 2xx class SIP responses that the SIP device has sent. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SummaryRequestsIn	This counter represents the total number of SIP request messages that have been received by the SIP device. This number includes retransmissions.
SummaryRequestsOut	This counter represents the total number of SIP request messages that the device sent. This number includes messages that originate on the device and messages that are being relayed by the device. When a particular message gets sent more than once, each transmission gets counted separately; for example, a message that is re-sent as a retransmission or as a result of forking.
SummaryResponsesIn	This counter represents the total number of SIP response messages that the SIP device received. This number includes retransmission.
SummaryResponsesOut	This counter represents the total number of SIP response messages that the SIP device sent (originated and relayed). This number includes retransmission.
UpdateIns	This counter represents the total number of UPDATE requests that the SIP device has received. This number includes retransmission.
UpdateOuts	This counter represents the total number of UPDATE requests that the SIP device has sent. This number includes retransmission.

Cisco SIP Station

The Cisco SIP Station object provides information about SIP line-side devices. Table B-32 contains information on the Cisco SIP Station counters.

Table B-32 Cisco SIP Station

Counters	Counter Description
ConfigMismatchesPersistent	This counter represents the number of times that a phone that is running SIP was persistently unable to register due to a configuration version mismatch between the TFTP server and Cisco Unified Communications Manager since the last restart of the Cisco Unified Communications Manager. This counter increments each time that Cisco Unified Communications Manager cannot resolve the mismatch and manual intervention is required (such as a configuration update or device reset).
ConfigMismatchesTemporary	This counter represents the number of times that a phone that is running SIP was temporarily unable to register due to a configuration version mismatch between the TFTP server and Cisco Unified Communications Manager since the last restart of the Cisco CallManager service. This counter increments each time Cisco Unified Communications Manager is able to resolve the mismatch automatically.

Table B-32 Cisco SIP Station (continued)

Counters	Counter Description
DBTimeouts	This counter represents the number of new registrations that failed because a timeout occurred while the system was attempting to retrieve the device configuration from the database.
NewRegAccepted	This counter represents the total number of new REGISTRATION requests that have been removed from the NewRegistration queue and processed since the last restart of the Cisco CallManager service.
NewRegQueueSize	This counter represents the number of REGISTRATION requests that are currently on the NewRegistration queue. The system places REGISTRATION requests that are received from devices that are not currently registered on this queue before they are processed.
NewRegRejected	This counter represents the total number of new REGISTRATION requests that were rejected with a 486 Busy Here response and not placed on the NewRegistration queue since the last restart of the Cisco CallManager service. The system rejects REGISTRATION requests if the NewRegistration queue exceeds a programmed size.
TokensAccepted	This counter represents the total number of token requests that have been granted since the last Cisco Communications Manager restart. Cisco Unified Communications Manager grants tokens as long as the number of outstanding tokens remains below the number that is specified in the Cisco CallManager service parameter Maximum Phone Fallback Queue Depth.
TokensOutstanding	This counter represents the number of devices that have been granted a token but have not yet registered. The system requires that devices that are reconnecting to a higher priority Cisco Unified Communications Manager server be granted a token before registering. Tokens protect Cisco Unified Communications Manager from being overloaded with registration requests when it comes back online after a failover situation.
TokensRejected	This counter represents the total number of token requests that have been rejected since the last Cisco Unified Communications Manager restart. Cisco Unified Communications Manager will reject token request if the number of outstanding tokens is greater than the number that is specified in the Cisco CallManager service parameter Maximum Phone Fallback Queue Depth.

Cisco SW Conf Bridge Device

The Cisco SW Conference Bridge Device object provides information about registered Cisco software conference bridge devices. Table B-33 contains information on the Cisco software conference bridge device counters.

Table B-33 Cisco SW Conf Bridge Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a SW conference device and failed because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for a SW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a SW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of conference resources that a SW conference device provides. One resource represents one stream.This counter equals the sum of the ResourceAvailable and ResourceActive counters.
SWConferenceActive	This counter represents the number of software-based conferences that are currently active (in use) on a SW conference device.
SWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a SW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.

Cisco TFTP Server

The Cisco Trivial File Transfer Protocol (TFTP) Server object provides information about the Cisco TFTP server. Table B-34 contains information on Cisco TFTP server counters.

Table B-34 Cisco TFTP Server

Counters	Counter Description
BuildAbortCount	This counter represents the number of times that the build process aborted when it received a Build all request. This counter increases when building of device/unit/softkey/dial rules gets aborted as a result of group level change notifications.
BuildCount	This counter represents the number of times since the TFTP service started that the TFTP server has built all the configuration files in response to a database change notification that affects all devices. This counter increases by one every time the TFTP server performs a new build of all the configuration files.
BuildDeviceCount	This counter represents the number of devices that were processed in the last build of all the configuration files. This counter also updates while processing device change notifications. The counter increases when a new device is added and decreases when an existing device is deleted.

Table B-34 Cisco TFTP Server (continued)

Counters	Counter Description
BuildDialruleCount	This counter represents the number of dial rules that were processed in the last build of the configuration files. This counter also updates while processing dial rule change notifications. The counter increases when a new dial rule is added and decreases when an existing dial rule is deleted.
BuildDuration	This counter represents the time in seconds that it took to build the last configuration files.
BuildSignCount	This counter represents the number of security-enabled phone devices for which the configuration file was digitally signed with the Cisco Unified Communications Manager server key in the last build of all the configuration files. This counter also updates while processing security-enabled phone device change notifications.
BuildSoftKeyCount	This counter represents the number of softkeys that were processed in the last build of the configuration files. This counter increments when a new softkey is added and decrements when an existing softkey is deleted.
BuildUnitCount	This counter represents the number of gateways that were processed in the last build of all the configuration files. This counter also updates while processing unit change notifications. The counter increases when a new gateway is added and decreases when an existing gateway is deleted.
ChangeNotifications	This counter represents the total number of all the Cisco Unified Communications Manager database change notifications that the TFTP server received. Each time that a device configuration is updated in Cisco Unified Communications Manager Administration, the TFTP server gets sent a database change notification to rebuild the XML file for the updated device.
DeviceChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for devices.
DialruleChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for dial rules.
EncryptCount	This counter represents the number of configuration files that were encrypted. This counter gets updated each time a configuration file is successfully encrypted
GKFoundCount	This counter represents the number of GK files that were found in the cache. This counter gets updated each time a GK file is found in the cache
GKNotFoundCount	This counter represents the number of GK files that were not found in the cache. This counter gets updated each time a request to get a GK file results in the cache not finding it
HeartBeat	This counter represents the heartbeat of the TFTP server. This incremental count indicates that the TFTP server is up and running. If the count does not increase, this means that the TFTP server is down.
HttpConnectRequests	This counter represents the number of clients that are currently requesting the HTTP GET file request.

Table B-34 Cisco TFTP Server (continued)

Counters	Counter Description
HttpRequests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the HTTP server handled. This counter represents the sum total of the following counters since the HTTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
HttpRequestsAborted	This counter represents the total number of HTTP requests that the HTTP server. canceled (aborted) unexpectedly. Requests could get aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.
HttpRequestsNotFound	This counter represents the total number of HTTP requests where the requested file was not found. When the HTTP server does not find the requested file, a message gets sent to the requesting device.
HttpRequestsOverflow	This counter represents the total number of HTTP requests that were rejected when the maximum number of allowable client connections was reached. The requests may have arrived while the TFTP server was building the configuration files or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
HttpRequestsProcessed	This counter represents the total number of HTTP requests that the HTTP server. successfully processed.
HttpServedFromDisk	This counters represents the number of requests that the HTTP server completed with the files that are on disk and not cached in memory.
LDFoundCount	This counter represents the number of LD files that were found in the cache. This counter gets updated each time a LD file is found in cache memory.
LDNotFoundCount	This counter represents the number of LD files that were not found in cache memory. This counter gets updated each time a request to get an LD file results in the cache not finding it.
MaxServingCount	This counter represents the maximum number of client connections that the TFTP can serve simultaneously. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets this value.
Requests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the TFTP server handles. This counter represents the sum total of the following counters since the TFTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
RequestsAborted	This counter represents the total number of TFTP requests that the TFTP server canceled (aborted) unexpectedly. Requests could be aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.
RequestsInProgress	This counter represents the number of file requests that the TFTP server currently is processing. This counter increases for each new file request and decreases for each file request that is completed. This counter indicates the current load of the TFTP server.

Table B-34 Cisco TFTP Server (continued)

Counters	Counter Description
RequestsNotFound	This counter represents the total number of TFTP requests for which the requested file was not found. When the TFTP server does not find the requested file, a message gets sent to the requesting device. If this counter increments in a cluster that is configured as secure, this event usually indicates an error condition. If, however, the cluster is configured as non-secure, it is normal for the CTL file to be absent (not found), which results in a message being sent to the requesting device and a corresponding increment in this counter. For non-secure clusters, then, this normal occurrence does not represent an error condition.
RequestsOverflow	This counter represents the total number of TFTP requests that were rejected because the maximum number of allowable client connections was exceeded, because requests arrived while the TFTP server was building the configuration files, or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
RequestsProcessed	This counter represents the total number of TFTP requests that the TFTP server successfully processed.
SegmentsAcknowledged	This counter represents the total number of data segments that the client devices acknowledged. Files get sent to the requesting device in data segments of 512 bytes, and for each 512-byte segment, the device sends the TFTP server an acknowledgment message. Each additional data segment gets sent upon receipt of the acknowledgment for the previous data segment until the complete file successfully gets transmitted to the requesting device.
SegmentsFromDisk	This counter represents the number of data segments that the TFTP server reads from the files on disk, while serving files.
SegmentSent	This counter represents the total number of data segments that the TFTP server sent. Files get sent to the requesting device in data segments of 512 bytes.
SEPFoundCount	This counter represents the number of SEP files that were successfully found in the cache. This counter gets updated each time that a SEP file is found in the cache.
SEPNotFoundCount	This counter represents the number of SEP files that were not found in the cache. This counter gets updated each time that a request to get a SEP file produces a not found in cache memory result.
SIPFoundCount	This counter represents the number of SIP files that were successfully found in the cache. This counter gets updated each time that a SIP file is found in the cache
SIPNotFoundCount	This counter represents the number of SIP files that were not found in the cache. This counter gets updated each time that a request to get a SIP file produces a not found in cache memory result.
SoftkeyChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for softkeys.
UnitChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete gateway-related configuration files.

Cisco Transcode Device

The Cisco Transcode Device object provides information about registered Cisco transcoding devices. Table B-35 contains information on Cisco transcoder device counters.

Table B-35 Cisco Transcode Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a transcoder resource from a transcoder device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of transcoder resources that are currently in use (active) for a transcoder device. Each transcoder resource uses two streams.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a transcoder device. Each transcoder resource uses two streams.
ResourceTotal	This counter represents the total number of transcoder resources that a transcoder device provided. This counter equals the sum of the counters ResourceActive and ResourceAvailable.

Cisco Video Conference Bridge

The Cisco Video Conference Bridge object provides information about registered Cisco video conference bridge devices. Table B-36 contains information on Cisco video conference bridge device counters.

Table B-36 Cisco Video Conference Bridge

Counters	Counter Description
ConferencesActive	This counter represents the total number of video conferences that are currently active (in use) on a video conference bridge device. The system specifies a conference as active when the first call connects to the bridge.
ConferencesAvailable	This counter represents the number of video conferences that are not active and are still available on a video conference device.
ConferencesCompleted	This counter represents the total number of video conferences that have been allocated and released on a video conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
ConferencesTotal	This counter represents the total number of video conferences that are configured for a video conference device.
OutOfConferences	This counter represents the total number of times that an attempt was made to initiate a video conference from a video conference device and failed because the device already had the maximum number of active conferences that is allowed (as specified by the TotalConferences counter).

Table B-36 Cisco Video Conference Bridge (continued)

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a video conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the total number of resources that are currently active (in use) on a video conference bridge device. One resource gets used per participant.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available on a device to handle additional participants for a video conference bridge device.
ResourceTotal	This counter represents the total number of resources that are configured on a video conference bridge device. One resource gets used per participant.

Cisco Web Dialer

The Cisco Web Dialer object provides information about the Cisco Web Dialer application and the Redirector servlet. Table B-37 contains information on the Cisco Web Dialer counters.

Table B-37 Cisco Web Dialer

Counters	Counter Description
CallsCompleted	This counter represents the number of Make Call and End Call requests that the Cisco Web Dialer application successfully completed.
CallsFailed	This counter represents the number of Make Call and End Call requests that were unsuccessful.
RedirectorSessionsHandled	This counter represents the total number of HTTP sessions that the Redirector servlet handled since the last service startup.
RedirectorSessionsInProgress	This counter represents the number of HTTP sessions that are currently being serviced by the Redirector servlet.
RequestsCompleted	This counter represents the number of Make Call and End Call requests that the Web Dialer servlet has successfully completed.
RequestsFailed	This counter represents the number of Make Call and End Call requests that failed.
SessionsHandled	This counter represents the total number of CTI sessions that the Cisco Web Dialer servlet handled since the last service startup.
SessionsInProgress	This counter represents the number of CTI sessions that the Cisco Web Dialer servlet is currently servicing.

Cisco WSM Connector

The WSM object provides information on WSMConnectors that are configured on Cisco Unified Communications Manager. Each WSMConnector represents a physical Motorola WSM device. Table B-38 contains information on the Cisco WSM Connector counters.

Table B-38 Cisco WSM Connector

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on the WSMConnector device.
CallsAttempted	This counter represents the number of calls that have been attempted on the WSMConnector device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that are connected (a voice path was established) through the WSMConnector device. The counter increments when the call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progress on the WSMConnector device. This includes all active calls. When the number of CallsInProgress equals the number of CallsActive, this indicates that all calls are connected.
DMMSRegistered	This counter represents the number of DMMS subscribers that are registered to the WSM.

IME Client

The IME Client object provides information about the Cisco IME client on the Cisco Unified Communications Manager server. Table B-39 contains information on the Cisco IME client counters.

Table B-39 Cisco IME Client

Counters	Counter Description
CallsAccepted	This counter indicates the number of Cisco IME calls that the Cisco Unified Communications Manager received successfully and that the called party answered, resulting in an IP call.
CallsAttempted	This counter indicates the number of calls that the Cisco Unified Communications Manager received through Cisco IME. This number includes accepted calls, failed calls, and busy, no-answer calls. The counter increments each time that Cisco Unified Communications Manager receives a call through Cisco IME.
CallsReceived	This counter indicates the number of calls that Cisco Unified Communications Manager receives through Cisco IME. This number includes accepted calls, failed calls, and busy, no-answer calls. The counter increments on call initiation.
CallsSetup	This counter indicates the number of Cisco IME calls that Cisco Unified Communications Manager placed successfully and that the remote party answered, resulting in an IP call.
DomainsUnique	This counter indicates the number of unique domain names of peer enterprises that the Cisco IME client discovered. The counter serves as an indicator of overall system usage.

Table B-39 Cisco IME Client (continued)

Counters	Counter Description
FallbackCallsFailed	This counter indicates the total number of failed fallback attempts.
FallbackCallsSuccessful	This counter indicates the total number of Cisco IME calls that have fallen back to the PSTN mid-call due to a quality problem. The counter includes calls initiated and calls received by this Cisco Unified Communications Manager.
IMESetupsFailed	This counter indicates the total number of call attempts for which a Cisco IME route was available but that were set up through the PSTN due to a failure to connect to the target over the IP network.
RoutesLearned	This counter indicates the total number of distinct phone numbers that the Cisco IME has learned and that are present as routes in the Cisco Unified Communications Manager routing tables. If this number grows too large, the server may exceed the per-cluster limit, and you may need to add additional servers to your cluster.
RoutesPublished	This counter indicates the total number of DIDs that were published successfully into the IME distributed cache across all Cisco IME client instances. The counter provides a dynamic measurement that gives you an indication of your own provisioned usage and a sense of how successful the system has been in storing the DIDs in the network.
RoutesRejected	This counter indicates the number of learned routes that were rejected because the the administrator blacklisted the number or domain. This counter provides an indication of the number of cases where a VoIP call cannot happen in the future because of the blocked validation.
VCRUploadRequests	This counter indicates the number of voice call record (VCR) upload requests that the Cisco Unified Communications Manager has sent to the Cisco IME server to be stored in the IME distributed cache.

IME Client Instance

The IME Client Instance object provides information about the Cisco IME client instance on the Cisco Unified Communications Manager server. Table B-40 contains information on the Cisco IME client instance counters.

Table B-40 IME Client

Counters	Counter Description
IMEServiceStatus	This counter indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Cisco Unified Communications Manager). The following values may display for the counter: • 0—Indicates an unknown state (which may mean that the Cisco IME service is not active). If the value specifies 0, an alert gets generated once per hour while the connection remains in the unknown state. • 1—Indicates a healthy state; that is, the Cisco IME service is active, and the Cisco Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured. • 2—Indicates an unhealthy state; that is, the Cisco IME service is active, but the Cisco Unified Communications Manager has not successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.

Where to Find More Information

Related Topics

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX C

Cisco Unity Connection Performance Objects and Counters

This appendix contains the following sections:

- CUC Data Store, page C-2
- CUC Data Store: Databases, page C-2
- CUC Digital Notifications, page C-3
- CUC Directory Services, page C-3
- CUC Message Store, page C-3
- CUC Message Store: Databases, page C-5
- CUC Personal Call Transfer Rules, page C-5
- CUC Phone System, page C-5
- CUC Phone System: Ports, page C-8
- CUC Replication, page C-8
- CUC Replicator: Remote Connection Locations, page C-8
- CUC Sessions: Calendar Access, page C-9
- CUC Sessions: E-mail Access, page C-9
- CUC Sessions: IMAP Server, page C-10
- CUC Sessions: RSS, page C-11
- CUC Sessions: SMTP Server, page C-11
- CUC Sessions: SpeechView Processor, page C-12
- CUC Sessions: TRaP, page C-12
- CUC Sessions: TTS, page C-13
- CUC Sessions: Unified Client, page C-13
- CUC Sessions: Voice, page C-13
- CUC Sessions: VUI, page C-15
- CUC Sessions: Web, page C-15
- CUC Sessions: Web E-mail Access, page C-16
- Where to Find More Information, page C-16

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for Cisco Unity Connection, access the performance monitoring counters in the Cisco Unified Real-Time Monitoring Tool (Unified CM Real Time Monitoring Tool).

CUC Data Store

The CUC Data Store object provides information about registered database usage by Cisco Unity Connection. Table C-1 contains information about CUC Data Store counters.

Table C-1 CUC Data Store

Counters	Counter Descriptions
Allocated Memory [kb]	Amount of database server virtual-address space [in kilobytes].
Database Connections	Total number of connections to the database server.
Disk Free (kb)	Amount of free disk space (in kilobytes).
Disk Reads	Total number of disk read operations for all data chunks (rows) in the last 30 seconds.
Disk Reads/second	Number of read operations from the disk per second.
Disk Writes	Number of write operations to the disk in the last 30 seconds.
Disk Writes/second	Number of write operations to the disk per second.
Shared Memory [kb]	Amount of database server shared memory used [in kilobytes].

CUC Data Store: Databases

The CUC Data: Databases object provides information about the databases that Cisco Unity Connection uses.

Table C-2 CUC Data Store: Databases

Counters	Counter Descriptions
Disk Free/chunk [kb]	The amount of free space available [in kilobytes] in the selected data chunk.
Disk Reads/chunk	Number of read operations for the selected data chunk.
Disk Writes/chunk	Number of write operations for the selected data chunk.

CUC Digital Notifications

The CUC Digital Notifications object provides information about the total number of SMS and SMTP notifications. Table C-3 contains information about CUC Digital Notification counters.

Table C-3 CUC Digital Notifications

Counters	Counter Descriptions
SMS Notifications Failed	The total number of SMS notifications failing to connect.
SMS Notifications Total	The total number of SMS notifications sent to subscribers by Cisco Unity Connection.
SMTP Notifications Total	The total number of SMTP notifications that Cisco Unity Connection sent to subscribers.

CUC Directory Services

The CUC Directory Services object provides information about the performance of the directory services that Cisco Unity Connection uses.

The Directory Search Duration Average [s] counter represents the average time [in seconds] to complete a directory search request for the Cisco Unity Connection server.

CUC Message Store

The CUC Message Store object provides information about the performance of the Cisco Unity Connection message store. Table C-4 contains information about CUC Message Store counters.

Table C-4 CUC Message Store

Counters	Counter Descriptions
Bad Mail Total	Total number of messages sent to the Bad Mail folder since the last restart of the MTA server.
Delivery Receipts Total	Total number of delivery receipts since the last restart of the MTA server.
Incoming Recalls	Number of incoming requests to recall local copies of messages initiated by remote senders on other network locations.
Intersite Messages Delivered Per Minute	Number of intersite messages delivered in the last minute.
Intersite Messages Delivered Total	Total number of intersite messages delivered since the last restart of the MTA server.
Intersite Messages Received Per Minute	Number of intersite messages received in the last minute.
Intersite Messages Received Total	Total number of intersite messages received since the last restart of the MTA server.
Intersite Messages Total	Total number of intersite messages that have been delivered and received since the last restart of the MTA server.
Local Recalls	Number of message recalls initiated by local senders on this server.
Message Size Average [kb]	The average size of the MTA at each sample in kilobytes.

Table C-4 CUC Message Store (continued)

Counters	Counter Descriptions
Messages Delivered Total	Total number of messages delivered since the last restart of the MTA server.
Messages Received Total	Total number of messages received since the last restart of the MTA server.
Non-delivery Receipts Total	Total number of non-delivery receipts since the last restart of the MTA server.
Number of Items Recalled	Total number of message recalls. This number includes each individual copy of a message that was sent to multiple recipients, so this number could be much larger than the Total Recalls, Local and Remote performance counter.
Queued Messages Current	The number of messages currently queued in the MTA.
Read Receipts Total	Total number of read receipts since the last restart of the MTA server.
Retries Total	Total number of retries since the last restart of the MTA server.
Total dispatch message folder items delivered	Total number of dispatch messages that have been delivered to individual user mailboxes since the MTA started. This number includes a count of each individual copy of a message sent to multiple recipients.
Total dispatch messages accepted	Total number of dispatch messages that have been accepted since the last restart of the MTA server
Total dispatch messages delivered	Total number of dispatch messages that have been delivered since the MTA started. This number includes each message just once, regardless of the number of recipients.
Total dispatch message items rejected	Total number of individual copies of dispatch messages that have been declined since the last restart of the MTA server.
Total dispatch messages removed due to acceptance	Total number of dispatch messages that have been removed from user mailboxes due to the message being accepted by another user since the last restart of the MTA server
Total recalls, local and remote	Total number of message recalls initiated by local and remote senders. This number should be equal to the total of Incoming Recalls and Local Recalls performance counters.
VPIM Message Decode Duration Average [s]	The average time [in seconds] to decode voice messages in MIME format to the original format.
VPIM Message Encode Duration Average [s]	The average time [in seconds] to encode voice messages to MIME format.
VPIM Messages Delivered Per Minute	The number of VPIM messages that the Cisco Unity Connection Messages Store delivered within a minute.
VPIM Messages Delivered Total	The total number of VPIM messages that the Cisco Unity Connection Messages Store delivered.
VPIM Messages Received Per Minute	The number of VPIM messages that the Cisco Unity Connection Messages Store received per minute.
VPIM Messages Received Total	The total number of VPIM messages that the Cisco Unity Connection Messages Store received.
VPIM Messages Total	The total number of VPIM messages that the Cisco Unity Connection Message Store processed.

CUC Message Store: Databases

The CUC Message Store: Databases object provides information about the message store database that Cisco Unity Connection uses.

The Messages Delivered Per Message Store counter represents the total number of messages that were delivered per message store since the last restart of the MTA server.

CUC Personal Call Transfer Rules

The CUC Personal Call Transfer Rules object provides information about the numbers and usage of the personal call transfer rules (PCTR). Table C-5 contains information about CUC Personal Call Transfer Rules counters.

Table C-5 CUC Personal Call Transfer Rules

Counters	Counter Descriptions
Applicable Rule Found	Personal call transfer rule (PCTR) call resulted in rule processing, and an applicable transfer rule is found.
Destinations Tried	Number of destinations tried while transfer rules were applied.
PCTR Calls	Calls that are subject to personal call transfer rule (PCTR) processing: user assigned COS is enabled for PCTR, user is a Cisco Unified Communications Manager user, user has not disabled PCTR.
Rules Evaluated	Number of rules that are evaluated during rule processing in a personal call transfer rule (PCTR) call.
Subscriber Reached	Number of times that a subscriber was reached while transfer rules were applied.
Transfer Failed	Number of times that Cisco Unity Connection fails to transfer a call to a destination while personal call transfer rules were applied. Transfer failures include all conditions except when the called destination is connected, busy, or RNA or times out. A caller hanging up during a transfer gets considered a transfer failure.
Voicemail Reached	Number of times that voice mail was reached while transfer rules were applied.

CUC Phone System

The CUC Phone System object provides information about the performance of the phone system integration. Table C-6 contains information about CUC Phone System counters.

Table C-6 CUC Phone System

Counters	Counter Descriptions
Call Count Current	The current number of incoming and outgoing calls to the Cisco Unity Connection server.
Call Count Total	The total number of incoming and outgoing calls to the Cisco Unity Connection server.

Table C-6 CUC Phone System (continued)

Counters	Counter Descriptions
Call Duration Average [s]	The average duration [in seconds] of incoming and outgoing calls from the Cisco Unity Connection server.
Call Duration Total [s]	The total duration [in seconds] of incoming and outgoing calls from the Cisco Unity Connection server.
Calls Unanswered Total	The total number of unanswered calls on the Cisco Unity Connection server.
Incoming Calls CFB Current	The current number of incoming calls that were received as Call Forward Busy.
Incoming Calls CFB Total	The total number of incoming calls that were received as Call Forward Busy.
Incoming Calls CFNA Current	The current number of incoming calls that were received as Call Forward No Answer.
Incoming Calls CFNA Total	The total number of incoming calls that were received as Call Forward No Answer.
Incoming Calls Current	The current number of incoming calls.
Incoming Calls Direct Current	The current number of incoming calls that were received as direct calls.
Incoming Calls Direct Total	The total number of incoming calls that were received as direct calls.
Incoming Calls Duration Average [s]	The average duration [in seconds] of all incoming calls to the Cisco Unity Connection server.
Incoming Calls Duration Total [s]	The total duration [in seconds] of all incoming calls to the Cisco Unity Connection server.
Incoming Calls No Info Total	The total number of incoming calls without integration information.
Incoming Calls Total	The total number of incoming calls.
Message Notification Duration Average [s]	The average time [in seconds] to complete all message notifications from the Cisco Unity Connection server.
Message Notification Duration Total [s]	The total time [in seconds] to complete all message notifications from the Cisco Unity Connection server.
Message Notifications Failed	The total number of message notifications that failed to connect to a destination number.
Message Notifications Total	The total number of message notifications that Cisco Unity Connection sent to subscribers.
MWI Request Duration Average [ms]	The average duration [in milliseconds] of all MWI requests from the Cisco Unity Connection server.
MWI Request Duration Total [ms]	The total duration [in milliseconds] of all MWI requests from the Cisco Unity Connection server.
MWI Requests Failed Total	The total number of MWI requests that failed to connect to a destination number or complete MWI operation.
MWI Requests Total	The total number of MWI requests that Cisco Unity Connection sent.
Outgoing Calls Duration Average [s]	The average duration [in seconds] of all outgoing calls from the Cisco Unity Connection server.
Outgoing Calls Duration Total [s]	The total duration [in seconds] of all outgoing calls from the Cisco Unity Connection server.

Table C-6 CUC Phone System (continued)

Counters	Counter Descriptions
Outgoing Calls Release Transfers Completed	The number of completed release transfers from the Cisco Unity Connection server.
Outgoing Calls Release Transfers Failed	The number of release transfers from the Cisco Unity Connection server that failed to connect to a destination number.
Outgoing Calls Release Transfers Total	The total number of release transfers that were attempted from the Cisco Unity Connection server.
Outgoing Calls Supervised Transfers Completed	The number of completed supervised transfers from the Cisco Unity Connection server.
Outgoing Calls Supervised Transfers Dropped	The number of supervised transfers from the Cisco Unity Connection server that were dropped while in progress.
Outgoing Calls Supervised Transfers Failed	The number of supervised transfers from the Cisco Unity Connection server that failed to connect to a destination number.
Outgoing Calls Supervised Transfers Total	The total number of supervised transfers from the Cisco Unity Connection server.
Outgoing Calls Transfers Total	The total number of release and supervised transfers that Cisco Unity Connection attempted.
Pager Notifications Duration Average [s]	The average time [in seconds] to complete all pager notifications from the Cisco Unity Connection server.
Pager Notifications Duration Total [s]	The total time [in seconds] to complete all pager notifications from the Cisco Unity Connection server.
Pager Notifications Failed	The total number of pager notifications that failed to connect to a destination number.
Pager Notifications Total	The total number of pager notifications that Cisco Unity Connection sent to subscribers.
Port Idle Duration [s]	The total time [in seconds] that any port remains idle between incoming calls to the Cisco Unity Connection server.
Port Idle Duration Average [s]	The average time [in seconds] that any port remains idle between incoming calls to the Cisco Unity Connection server.
Ports Idle Current	The current number of integration ports that are not in use by the Cisco Unity Connection server.
Ports In Use Current	The current number of integration ports that are in use by the Cisco Unity Connection server.
Ports Locked	The current count of the ports that no longer respond or are otherwise unusable by Cisco Unity Connection.

CUC Phone System: Ports

The CUC Phone System: Ports object provides information about the voice messaging ports on Cisco Unity Connection. Table C-7 contains information about CUC Phone System: Ports counters.

Table C-7 CUC Phone System: Ports

Counters	Counter Descriptions
Port Calls	The total number of calls that were received on this port since the Cisco Unity Connection server was last restarted. This includes all types of calls: Incoming calls, MWI dialouts, Notification dialouts, TRAP dialouts, and VPIM dialouts.
Port Idle Percent	The distribution percentage of idle ports on the Cisco Unity Connection server.
Port Usage Duration Average [s]	The average time [in seconds] that a port has been actively processing calls.
Port Usage Duration Total [s]	The total time [in seconds] that a port has been actively processing calls.
Port Usage Percent	The distribution percentage of calls into ports on the Cisco Unity Connection server.

CUC Replication

The CUC Replication object provides information about the replication for Cisco Unity Connection redundancy. Table C-8 contains information about CUC Replication counters.

Table C-8 CUC Replication

Counters	Counter Descriptions
File Replication Latency [s]	How long file exists before replication starts.
File Replication Latency Max [s]	Maximum file replication latency since the service started.
File Transfer Rate [kbytes/s]	Transfer rate for each replicated file.
Files Replicated Total	Number of files replicated since the service started.
Transfer Rate [bytes/s]	Number of bytes transferred each second.

CUC Replicator: Remote Connection Locations

The CUC Replicator: Remote Connection Locations object provides information about replication with remote Connection locations. Table C-9 contains information about CUC Replicator: Remote Connection Locations counters.

Table C-9 CUC Replicator: Remote Connection Locations

Counters	Counter Descriptions
Dependencies Requests Received	The number of replication dependencies requested received from the Connection location.
Dependencies Requests Sent	The number of replication dependencies requests sent to the Connection location.

Table C-9 CUC Replicator: Remote Connection Locations (continued)

Counters	Counter Descriptions
Message Receive Failures	The number of replication messages from this Connection location that were not received because of failures.
Message Send Failures	The number of replication messages to the Connection location that were not sent because of failures.
Messages Received	The number of replication messages received from the Connection location.
Messages Sent	The number of replication messages sent to the Connection location.
NDR Messages Received	The number of replication NDR messages received from the Connection location.
USN Requests Received	The number of USN request received from the Connection location. This usually indicates that a USN timeout occurred on the remote node.

CUC Sessions: Calendar Access

The CUC Sessions: Calendar Access object provides information about the Cisco Unity Connection calendar integration. Table C-10 contains information about CUC Sessions: Calendar Access counters.

Table C-10 CUC Sessions: Calendar Access

Counters	Counter Descriptions
Connections To Exchange Failure - Total	Total number of Exchange connection failures.
Connections To MP Failure - Total	Total number of MeetingPlace connection failures.
Exchange Requests - Total	Total number of Exchange calendar requests.
Exchange Response Time [ms] - Current	Current Exchange Response Time in milliseconds.
Meeting Join Request - Total	Total number of requests to join the meeting.
MP Request - Total	Total number of MeetingPlace calendar requests.
MP Response Time [ms] - Current	Current MeetingPlace Response Time in milliseconds.

CUC Sessions: E-mail Access

The CUC Sessions: E-mail Access object provides information about e-mail voice sessions. Table C-11 contains information about CUC Sessions: E-mail Access counters.

Table C-11 CUC Sessions: E-Mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart of Cisco Unity Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measured on a per-call basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured on a per-call basis.

Table C-11 CUC Sessions: E-Mail Access (continued)

Counters	Counter Descriptions
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Unity Connection.

CUC Sessions: IMAP Server

The CUC Sessions: IMAP Server object provides information about the IMAP server. Table C-12 contains information about CUC Sessions: IMAP Server counters.

Table C-12 CUC Sessions: IMAP Server

Counters	Counter Descriptions
Commands per minute	The number of IMAP commands per minute.
Connection Length Average [s]	The average duration [in seconds] of the connections to the IMAP server in the previous minute.
Current IDLE Sessions	The number of idle sessions on the IMAP server.
Errors Total	The total number of IMAP errors that the IMAP server returned since the last restart of the IMAP server.
EXAMINE Requests Total	The total number of EXAMINE requests to the IMAP server since the last restart of the IMAP server.
Failed Login Requests Total	The total number of failed LOGIN requests to the IMAP server since the last restart of the IMAP server.
FETCH Requests Total	The total number of FETCH requests to the IMAP server since the last restart of the IMAP server.
Login Requests Total	The total number of LOGIN requests to the IMAP server since the last restart of the IMAP server.
Logout Requests Total	The total number of LOGOUT requests to the IMAP server since the last restart of the IMAP server.
Messages Read Total	The total number of IMAP FETCH commands that have returned the body of the a message since the IMAP was last restarted.
Messages Read/hour	The number of IMAP FETCH commands in the previous hour that returned the body of a message.
Messages/fetch Average	Average number of messages that the IMAP FETCH command returned.
NOOP Requests Total	The total number of NOOP requests to the IMAP server since the last restart of the IMAP server.
Response Time [ms]	The response time [in milliseconds] for IMAP commands.
SEARCH Requests Total	The total number of SEARCH requests to the IMAP server since the last restart of the IMAP server.
Socket Connections Current	The number of active socket connections to the IMAP server.
Socket Connections Total	The total number of socket connections that have been made to the IMAP server since it was last restarted.

Table C-12 CUC Sessions: IMAP Server (continued)

Counters	Counter Descriptions
STARTTLS Requests Total	The total number of STARTTLS requests to the IMAP server since the last restart of the IMAP server. This counter also increments when clients connect to the IMAP SSL port directly.
STATUS Requests Total	The total number of STATUS requests to the IMAP server since the last restart of the IMAP server.
TLS Connections Current	The number of active Transport Layer Security connections to the IMAP server.
TLS Errors Total	The total number of failed TLS connections to the IMAP server since the last restart of the IMAP server.
Unsolicited Notify Response Time Average [ms]	Average Unsolicited Notify Response Time [in milliseconds] for the IMAP server.
Unsolicited Notify Responses Total	Total number of Unsolicited Notify Responses that the IMAP server made since it was last restarted.

CUC Sessions: RSS

The CUC Sessions: RSS object provides information about RSS sessions. Table C-13 contains information about CUC Sessions: RSS counters.

Table C-13 CUC Sessions: RSS

Counters	Counter Descriptions
RSS Messages Offered Total	The total number of RSS messages that were offered for streaming.
RSS Messages Streamed Total	The total number of RSS messages that the Cisco Unity Connection server streamed.
RSS Sessions Current	The current number of RSS sessions.
RSS Sessions Total	The total number of RSS sessions.

CUC Sessions: SMTP Server

The CUC Sessions: SMTP Server object provides information about SMTP server sessions. Table C-14 contains information about CUC Sessions: SMTP Server counters.

Table C-14 CUC Sessions: SMTP Server

Counters	Counter Descriptions
Total Delivered Messages	The number of SMTP messages that were delivered since the start of the system.
Total Messages	The number of SMTP messages delivered or received since the start of the system.
Total Received Messages	The number of SMTP messages that were received since the start of the system.

CUC Sessions: SpeechView Processor

The CUC Sessions: SpeechView Processor object provides information about <blah>. Table C-15 contains information about CUC Sessions: TRaP counters.

Table C-15 CUC Sessions: SpeechView Processor

Counters	Counter Descriptions
Average wait time	The average time it takes to receive successful transcriptions from the external service
Total failures	The total number of failed transcriptions since the last restart of the SpeechView Processor service.
Total timeouts	The total number transcriptions that timed out since the last restart of the SpeechView Processor service.
Transcribed messages	The total number successful transcriptions since the last restart of the SpeechView Processor service.

CUC Sessions: TRaP

The CUC Sessions: TRaP object provides information about telephone record and playback (TRaP) sessions. Table C-16 contains information about CUC Sessions: TRaP counters.

Table C-16 CUC Sessions: TRaP

Counters	Counter Descriptions
Reverse TRaP Session Duration Average [s]	The average duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Session Duration Total [s]	The total duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Sessions Current	The current number of active reverse TRaP sessions.
Reverse TRaP Sessions Total	The total number of reverse TRaP sessions since the last start of Cisco Unity Connection.
TRaP Session Duration Average [s]	The average duration [in seconds] of all TRaP sessions.
TRaP Session Duration Total [s]	The total duration [in seconds] of all TRaP sessions.
TRaP Sessions Current	The current number of active TRaP sessions.
TRaP Sessions Total	The total number of TRaP sessions since the last start of Cisco Unity Connection.

CUC Sessions: TTS

The CUC Sessions: TTS object provides information about text-to-speech (TTS) sessions. Table C-17 contains information about CUC Sessions: TTS counters.

Table C-17 CUC Sessions: TTS

Counters	Counter Descriptions
Session Duration Average [s]	The average duration [in seconds] of all TTS sessions.
Session Duration Total [s]	The total duration [in seconds] of all TTS sessions.
Sessions Current	The current number of active TTS voice sessions.
Sessions Total	The total number of TTS voice sessions since the last start of Cisco Unity Connection.

CUC Sessions: Unified Client

The CUC Sessions: Unified Client object provides information about the Unified Client for Cisco Unity Connection.

The Connections Total counter represents the total number of Unified Client IMAP requests.

CUC Sessions: Voice

The CUC Sessions: Voice object provides information about voice sessions. Table C-18 contains information on CUC Sessions: Voice counters.

Table C-18 CUC Sessions: Voice

Counters	Counter Descriptions
Delay - Directory Search [ms]	The delay [in milliseconds] that a caller experienced when the caller attempted to search through the directory. This counter measures the time between the entered search criteria and the return results.
Delay - Opening Greeting [ms]	The delay [in milliseconds] that a caller experienced before any audio was received. This counter measures the time between the system receiving a call and the time audio begins streaming to the caller.
Delay - Subscriber Delete Message [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experienced when the subscriber attempted to delete a message. This counter measures the time between the last delete message prompt and the confirmation of the deletion.
Delay - Subscriber Logon [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experienced due to authentication.
Delay - Subscriber Message Count [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experienced during message counting in the subscriber message box.
Delay - Subscriber Message Header [ms]	The delay [in milliseconds] that a caller experienced while Cisco Unity Connection is gathering message header information.
Failsafes Total	The total number of times that the failsafe conversation has been played.

Table C-18 CUC Sessions: Voice (continued)

Counters	Counter Descriptions
G.711a Sessions Current	The current number of active G.711 (a-law) voice sessions.
G.711a Sessions Total	The total number of active G.711 (a-law) voice sessions since the last restart of Cisco Unity Connection.
G.711u Sessions Current	The current number of active G.711 (u-law) voice sessions.
G.711u Sessions Total	The total number of active G.711 (u-law) voice sessions since the last restart of Cisco Unity Connection.
G.722 Sessions Current	The current number of active G.722 voice sessions.
G.722 Sessions Total	The total number of active G.722 voice sessions since the last restart of Cisco Unity Connection.
G.729 Sessions Current	The current number of active G.729 voice sessions.
G.729 Sessions Total	The total number of active G.729 voice sessions since the last restart of Cisco Unity Connection.
iLBC Sessions Current	The current number of active iLBC voice sessions.
iLBC Sessions Total	The total number of active iLBC voice sessions since the last restart of Cisco Unity Connection.
Meeting search delay delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experienced due to looking up meetings.
Messages Deleted	The total number of voice messages that were deleted through the TUI from the time Cisco Unity Connection was last restarted.
Messages Forwarded	The total number of voice messages that were forwarded through the TUI from the time Cisco Unity Connection was last restarted.
Messages Read	The total number of voice messages that were read through the TUI from the time Cisco Unity Connection was last restarted.
Messages Replied	The total number of voice messages that received replies through the TUI from the time Cisco Unity Connection was last restarted.
Messages Sent	The total number of voice messages that were sent through the TUI from the time Cisco Unity Connection was last restarted.
MRCP Define Grammar Delay [ms]	The delay [in milliseconds] between an MRCP define-grammar request and its response.
MRCP Define Grammar Delay Average [ms]	The average delay [in milliseconds] between an MRCP define-grammar request and its response.
MRCP Define Grammar Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP define-grammar request and its response.
MRCP Delay [ms]	The delay [in milliseconds] between an MRCP request and its response.
MRCP Delay Average [ms]	The average delay [in milliseconds] between an MRCP request and its response.
MRCP Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP request and its response.
Sessions Current	The current number of all active voice sessions for any codec.

Table C-18 CUC Sessions: Voice (continued)

Counters	Counter Descriptions
Sessions Total	The total number of voice sessions for any codec - G.711 mu-law and G.729 - since the last restart of Cisco Unity Connection.
Subscriber Lookup Delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experienced due to finding and loading a subscriber by DTMF ID.

CUC Sessions: VUI

The CUC Sessions: VUI object provides information about the voice user interface (VUI). Table C-19 contains information on CUC Sessions: VUI counters.

Table C-19 CUC Sessions: VUI

Counter	Counter Descriptions
Delay - Subscriber Message Access [ms]	The delay [in milliseconds] that a user when experienced when the user attempted to access a message. This counter measures the time between the voice command of intending to listen to a message and the actual playback of the message.
Matches Total	The total number of matches in the VUI conversation.
Messages Read	The total number of messages that were read through the VUI from the time that Cisco Unity Connection was last restarted.
No-matches Total	The total number of no-matches in the VUI conversation.
Session Duration Average/call [s]	The average duration [in seconds] of a VUI session as measured on a per-call basis.
Session Duration Total [s]	The duration [in seconds] of all VUI sessions.
Sessions Current	The current number of active VUI sessions for any codec.
Sessions Total	The total number of VUI and voice sessions for any codec.

CUC Sessions: Web

The CUC Sessions: Web object provides information about the Cisco Personal Communications Assistant (Cisco PCA) and Cisco Unity Connection Administration sessions. Table C-20 contains information on CUC Sessions: Web counters.

Table C-20 CUC Sessions: Web

Counters	Counter Descriptions
CPCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to a user Inbox or Assistant.
CPCA Failed Authentications Total	The number of failed authentications.
CPCA Pages Served Total	The total number of CPCA pages that the Cisco Unity Connection server served.
CPCA Requests In Queue Current	The number of requests in CPCA queue waiting to be processed.
CPCA Server Busy Pages Total	The total number of server busy pages that the Cisco Unity Connection server returned.

Table C-20 CUC Sessions: Web (continued)

Counters	Counter Descriptions
CPCA Sessions Current	The current number of CPCA sessions.
CPCA Sessions Total	The total number of CPCA sessions.
CUCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to the System Administrator window.
CUCA Response Time Max [ms]	The maximum time [in milliseconds] for the Tomcat server to respond to any given request.

CUC Sessions: Web E-mail Access

The CUC Sessions: Web E-mail Access object provides information about web e-mail access sessions (IMAP). Table C-21 contains information about CUC Sessions: Web E-mail Access counters.

Table C-21 CUC Sessions: Web E-mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart of Cisco Unity Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measured on a per-call basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured on a per-call basis.
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Unity Connection.

Where to Find More Information

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX D

Performance Objects and Counters for Cisco Intercompany Media Engine

This chapter provides information on Cisco Intercompany Media Engine-related objects and counters. The chapter covers the following objects and counters:

- IME Configuration Manager, page D-1
- IME Server, page D-2
- IME Server System Performance, page D-3

IME Configuration Manager

The IME Configuration Manager object provides information about the IME distributed cache certificate. Table D-1 contains information on the Cisco IME configuration counters.

Table D-1 IME Configuration Manager

Counters	Counter Description
DaysUntilCertExpiry	This counter indicates the number of days that remain until the IME distributed cache certificate expires. You must replace the certificate before it expires. When the value of this counter falls below 14, an alert gets generated once every day until the value exceeds 14.

IME Server

The IME Server object provides information about the Cisco IME server. Table D-2 contains information on the Cisco IME Server counters.

Table D-2 IME Server

Counters	Counter Description
BlockedValidationOrigTLSLimit	This counter indicates the total number of blocked validations that occurred because the TLSValidationThreshold was reached.
BlockedValidationTermTLSLimit	This counter indicates the total number of blocked validations that occurred because the TLSValidationThreshold was reached.
ClientsRegistered	This counter indicates the number of Cisco IME clients that are currently connected to the Cisco IME server.
IMEDistributedCacheHealth	The counter indicates the health of the IME distributed cache. The following values may display: • 0 (red)—Warns that the IME distributed cache is not functioning properly; for example, the Cisco IME cannot resolve issues after the network has been partitioned In this case, validation attempts might fail. For example, the Cisco IME service is not connected to the network and is unable to reach the bootstrap servers. An alert gets generated once every hour until the value changes from red status. • 1 (yellow)—Indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. (Check the Cisco IME alarms to determine network issues.) • 2 (green)—Indicates that the Cisco IME is functioning normally and is considered healthy.
IMEDistributedCacheNodeCount	The counter is an integer that indicates an approximation of the total number of nodes in the IME distributed cache. Since each physical Cisco IME server hosts multiple nodes, this counter does not directly indicate the number of physical Cisco IME servers that participate in the IME distributed cache. This counter can provide an indication of the health of the IME distributed cache; for example, a problem may exist with the IME distributed cache if an expected value displays on one day (for example, 300), but then on the next day, the value drops dramatically (for example, to 10 or 2).
IMEDistributedCacheQuota	Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Cisco Unified CMs attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
IMEDistributedCacheQuotaUsed	Indicates the total number of unique DID numbers that have been configured, to be published via enrolled patterns for Intercompany Media Services, by Cisco Unified CMs currently attached to this IME server.
IMEDistributedCacheReads	This counter indicates the total number of reads that the Cisco IME server has attempted into the IME distributed cache. This number serves as an indicator of whether the Cisco IME server is functional; that is, whether the server is interacting with other nodes.

Table D-2 IME Server (continued)

Counters	Counter Description
IMEDistributedCacheStoredData	This counter indicates the amount of IME distributed cache storage, measured in bytes, that this Cisco IME server provides.
IMEDistributedCacheStores	This counter indicates the total number of stores (published numbers) that the Cisco IME server has attempted into the IME distributed cache. This number serves as an indicator of whether the Cisco IME server is functional.
InternetBandwidthRecv	This counter measures the amount of downlink Internet bandwidth, in Kbits/s, that the Cisco IME server is consuming.
InternetBandwidthSend	This counter measures the amount of uplink Internet bandwidth that the Cisco IME server in Kbits/s is consuming.
TerminatingVCRs	This counter indicates the total Cisco IME voice call records (VCRs) that are stored on the Cisco IME server after receiving calls. You can use these records for validating learned routes.
ValidationAttempts	This counter indicates the total number of attempts that the Cisco IME server has made at performing a validation because the dialed number was found in the Cisco IME network. This counter provides an overall indication of system usage.
ValidationsAwaitingConfirmation	This counter indicates the total number of destination phone numbers that have been validated, but that are awaiting further calls to improve the security of the system. If you use a higher level of security for learning new routes, the Cisco IME server requires multiple successful validations for a route before that route is available for calls over IP. This counter tracks the number of successful validations that have not resulted in available IP routes.
ValidationsPending	This counter, which is an integer, indicates the number of scheduled validation attempts to retrieve a learned route. This value indicates the backlog of work for the Cisco IME service on the Cisco IME server. An alert gets generated when the value rises either above the high watermark or falls below the low watermark. After the high watermark is reached, an alert gets sent immediately and then once an hour until the value falls below the high watermark. When the high watermark is reached, the Cisco IME service cannot clear the backlog of work prior to the expiration of data; this situation causes records to drop, and validation may not occur. To reduce the workload, add more Cisco IME servers that can share the workload.
ValidationsBlocked	This counter indicates the number of times that the Cisco IME service rejected a validation attempt because the calling party was not trusted; that is, the party was on a blacklist or not on a whitelist. This value provides an indication of the number of cases where a VoIP calls cannot happen in the future because of the blocked validation.

IME Server System Performance

The Cisco IME System Performance object provides information about performance on the Cisco IME server. Table D-3 contains information on the Cisco IME server system performance counters.

Table D-3 IME Server System Performance

Counters	Counter Description
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the queue on the Cisco IME server. High-priority signals include timeout events, internal KeepAlive messages, internal process creation, and so on. A large number of high-priority events causes degraded performance of the Cisco IME service and results in slower or failed validations. Use this counter in conjunction with the QueueSignalsProcessed 1-High counter to determine the processing delay on the Cisco IME server.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the queue on the Cisco IME server. Normal-priority signals include call validations, IME distributed cache operations such as stores and reads, and so on. A large number of normal-priority events causes degraded performance of the Cisco IME service and may result in slower or failed validations or disruption to IME distributed cache connectivity. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the processing delay on the Cisco IME server. Since high-priority signal must complete before normal priority signals begin to process, check the high-priority counters to accurately understand why a delay occurs.
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the queue on the Cisco IME server. Low-priority signals include IME distributed cache signaling and other events. A large number of signals in this queue may disrupt IME distributed cache connectivity or other events.
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest-priority signals in the queue on the Cisco IME server. A large number of signals in this queue may disrupt IME distributed cache connectivity and other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay for this queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay for this queue. High-priority signals are processed before normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 3-Low counter to determine the processing delay for this queue.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 4-Lowest counter to determine the processing delay for this queue.
QueueSignalsProcessed Total	This counter provides a total of all queue signals that the Cisco IME service processes for each one-second period for all queue levels: high, normal, low, and lowest.

Where to Find More Information

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX E

System Alert Descriptions and Default Configurations

The following list comprises the system alerts, their definitions, and default settings.

- AuthenticationFailed, page E-2
- CiscoDRFFailure, page E-2
- CoreDumpFileFound, page E-3
- CpuPegging, page E-3
- CriticalServiceDown, page E-4
- HardwareFailure, page E-5
- LogFileSearchStringFound, page E-5
- LogPartitionHighWaterMarkExceeded, page E-6
- LogPartitionLowWaterMarkExceeded, page E-6
- LowActivePartitionAvailableDiskSpace, page E-7
- LowAvailableVirtualMemory, page E-8
- LowInactivePartitionAvailableDiskSpace, page E-8
- LowSwapPartitionAvailableDiskSpace, page E-9
- ServerDown, page E-9
- SparePartitionHighWaterMarkExceeded, page E-10
- SparePartitionLowWaterMarkExceeded, page E-11
- SyslogSeverityMatchFound, page E-11
- SyslogStringMatchFound, page E-12
- SystemVersionMismatched, page E-13
- TotalProcessesAndThreadsExceededThreshold, page E-13

AuthenticationFailed

Authentication validates the user ID and password that are submitted during log in. An alarm gets raised when an invalid user ID and/or the password gets used.

Default Configuration

Table E-1 Default Configuration for the AuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Number of AuthenticationFailed events exceeds: 1 time in the last 1 minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoDRFFailure

This alert occurs when the DRF backup or restore process encounters errors.

Default Configuration

Table E-2 Default Configuration for the CiscoDRFFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoDRFFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-2 Default Configuration for the CiscoDRFFailure RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

CoreDumpFileFound

This alert occurs when the CoreDumpFileFound event gets generated. This indicates that a core dump file exists in the system.

Default Configuration

Table E-3 Default Configuration for the CoreDumpFileFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CoreDumpFileFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Not Selected
Enable Email	Selected
Trigger Alert Action	Default

CpuPegging

CPU usage gets monitored based on configured thresholds. If the usage goes above the configured threshold, this alert gets generated.

Default Configuration

Table E-4 Default Configuration for the CpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: 99%
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CriticalServiceDown

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

Default Configuration

Table E-5 Default Configuration for the CriticalServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Service status is DOWN
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

HardwareFailure

This alert occurs when a hardware failure event (disk drive failure, power supply failure, and others) has occurred.

Default Configuration

Table E-6 Default Configuration for the HardwareFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: HardwareFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogFileSearchStringFound

This alert occurs when the LogFileSearchStringFound event gets generated. This indicates that the search string was found in the log file.

Default Configuration

Table E-7 Default Configuration for the LogFileSearchStringFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: LogFileSearchStringFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-7 Default Configuration for the LogFileSearchStringFound RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionHighWaterMarkExceeded

This alert occurs when the percentage of used disk space in the log partition exceeds the configured high water mark. When this alert gets generated, LPM deletes files in the log partition (down to low water mark) to avoid running out of disk space.

Note LPM may delete files that you want to keep. You should act immediately when you receive the LogPartitionLowWaterMarkExceeded alert.

Default Configuration

Table E-8 Default Configuration for the LogPartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionLowWaterMarkExceeded

This alert occurs when the LogPartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark.

Note Be aware that this alert is an early warning. The administrator should start freeing up disk space. Using RTMT/TLC, you can collect trace/log files and delete them from the server. The administrator should adjust the number of trace files that are kept to avoid hitting the low water mark again.

Default Configuration

Table E-9 Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowActivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space on the active partition is lower than the configured value.

Default Configuration

Table E-10 Default Configuration for the LowActivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Active Partition available diskspace below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowAvailableVirtualMemory

RTMT monitors virtual memory usage. When memory runs low, a LowAvailableVirtualMemory alert gets generated.

Default Configuration

Table E-11 Default Configuration for the LowAvailableVirtualMemory RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Available virtual memory below (30%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowInactivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space of the inactive partition equals less than the configured value.

Default Configuration

Table E-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive Partition available disk space below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily

Table E-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LowSwapPartitionAvailableDiskSpace

This alert indicates that the available disk space on the swap partition is low.

Note The swap partition is part of virtual memory, so low available swap partition disk space means low virtual memory as well.

Default Configuration

Table E-13 Default Configuration for the LowSwapPartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Swap Partition available disk space below (10%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ServerDown

This alert occurs when a remote node cannot be reached.

Note *Unified CM clusters only:* The ServerDown alert gets generated when the currently "active" AMC (primary AMC or the backup AMC, if the primary is not available) cannot reach another server in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

Default Configuration

Table E-14 Default Configuration for the ServerDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ServerDown occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionHighWaterMarkExceeded

This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table E-15 Default Configuration for the SparePartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionLowWaterMarkExceeded

This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition has exceeded the low water mark threshold.

Default Configuration

Table E-16 Default Configuration for the SparePartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SyslogSeverityMatchFound

This alert occurs when the SyslogSeverityMatchFound event gets generated. This indicates that a syslog message with the matching severity level exists.

Default Configuration

Table E-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogSeverityMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert (continued)

Value	Default Configuration
Syslog Severity Parameters	Critical
Enable Email	Selected
Trigger Alert Action	Default

SyslogStringMatchFound

This alert occurs when the SyslogStringMatchFound event gets generated. The alert indicates that a syslog message with the matching search string exists.

Default Configuration

Table E-18 Default Configuration for the SyslogStringMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogStringMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Syslog Alert Parameters	(Text box for search string)
Enable Email	Selected
Trigger Alert Action	Default

SystemVersionMismatched

This alert occurs when a mismatch in system version exists.

Default Configuration

Table E-19 Default Configuration for the SystemVersionMismatched RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SystemVersionMismatched occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TotalProcessesAndThreadsExceededThreshold

This alert occurs when the TotalProcessesAndThreadsExceededThreshold event gets generated. The alert indicates that the current total number of processes and threads exceeds the maximum number of tasks that are configured for the Cisco RIS Data Collector Service Parameter. This situation could indicate that a process is leaking or that a process has thread leaking.

Default Configuration

Table E-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TotalProcessesAndThreadsExceededThreshold event generated
Duration	Trigger alert immediately

Table E-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

APPENDIX F

CallManager Alert Descriptions and Default Configurations

The following list comprises the CallManager alerts, their definitions, and default settings.

- BeginThrottlingCallListBLFSubscriptions, page F-2
- CallProcessingNodeCpuPegging, page F-3
- CDRAgentSendFileFailed, page F-3
- CDRFileDeliveryFailed, page F-4
- CDRHighWaterMarkExceeded, page F-5
- CDRMaximumDiskSpaceExceeded, page F-5
- CodeYellow, page F-6
- DBChangeNotifyFailure, page F-7
- DBReplicationFailure, page F-7
- DDRBlockPrevention, page F-8
- DDRDown, page F-9
- ExcessiveVoiceQualityReports, page F-9
- IMEDistributedCacheInactive, page F-10
- IMEOverQuota, page F-10
- IMEQualityAlert, page F-11
- InsufficientFallbackIdentifiers, page F-12
- IMEServiceStatus, page F-13
- InvalidCredentials, page F-14
- IMEQualityAlert, page F-11
- LowTFTPServerHeartbeatRate, page F-15
- MaliciousCallTrace, page F-16
- MediaListExhausted, page F-16
- MgcpDChannelOutOfService, page F-17
- NumberOfRegisteredDevicesExceeded, page F-17
- NumberOfRegisteredGatewaysDecreased, page F-18

- NumberOfRegisteredGatewaysIncreased, page F-19
- NumberOfRegisteredMediaDevicesDecreased, page F-19
- NumberOfRegisteredMediaDevicesIncreased, page F-20
- NumberOfRegisteredPhonesDropped, page F-20
- RouteListExhausted, page F-21
- SDLLinkOutOfService, page F-21
- TCPSetupToIMEFailed, page F-22
- TLSConnectionToIMEFailed, page F-23

BeginThrottlingCallListBLFSubscriptions

This alert occurs when the BeginThrottlingCallListBLFSubscriptions event gets generated. This indicates that the Cisco Unified Communications Manager initiated a throttling of the CallList BLF Subscriptions to prevent a system overload.

Default Configuration

Table F-1 Default Configuration for the BeginThrottlingCallListBLFSubscriptions RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: BeginThrottlingCallListBLFSubscriptions event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CallProcessingNodeCpuPegging

This alert occurs when the percentage of CPU load on a call processing server exceeds the configured percentage for the configured time.

Note If the administrator takes no action, high CPU pegging can lead to a crash, especially in CallManager service. CoreDumpFound and CriticalServiceDown alerts might also be issued.

The CallProcessingNodeCpuPegging alert gives you time work proactively to avoid a Cisco Unified Communications Manager crash.

Default Configuration

Table F-2 Default Configuration for the CallProcessingNodeCpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Processor load over (90%)
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRAgentSendFileFailed

This alert gets raised when the CDR Agent cannot send CDR files from a Cisco Unified Communications Manager node to a CDR repository node within the Cisco Unified Communications Manager cluster.

Default Configuration

Table F-3 Default Configuration for the CDRAgentSendFileFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-3 Default Configuration for the CDRAgentSendFileFailed RTMT Alert (continued)

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRAgentSendFileFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRFileDeliveryFailed

This alert gets raised when FTP delivery of CDR files to the outside billing server fails.

Default Configuration

Table F-4 Default Configuration for the CDRFileDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRFileDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRHighWaterMarkExceeded

This alert gets raised when the high water mark for CDR files gets exceeded. It also indicates that some successfully delivered CDR files got deleted.

Default Configuration

Table F-5 Default Configuration for the CDRHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRHighWaterMarkExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRMaximumDiskSpaceExceeded

This alarm gets raised when the CDR files disk usage exceeds the maximum disk allocation. It also indicates that some undelivered files got deleted.

Default Configuration

Table F-6 Default Configuration for the CDRMaximumDiskSpaceExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRMaximumDiskSpaceExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table F-6 Default Configuration for the CDRMaximumDiskSpaceExceeded RTMT Alert

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

CodeYellow

The AverageExpectedDelay counter represents the current average expected delay to handle any incoming message. If the value exceeds the value that is specified in Code Yellow Entry Latency service parameter, the CodeYellow alarm gets generated. You can configure the CodeYellow alert to download trace files for troubleshooting purposes.

Default Configuration

Table F-7 Default Configuration for the CodeYellow RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco CallManager CodeYellowEntry event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace Download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

DBChangeNotifyFailure

This alert occurs when the Cisco Database Notification Service experiences problems and might stop. This condition indicates change notification requests that are queued in the database got stuck and changes made to the system will not take effect. Ensure that the Cisco Database Layer Monitor is running on the node where the alert exists. If it is, restart the service. If that does not return this alert to safe range, collect the output of **show tech notify** and **show tech dbstateinfo** and contact TAC for information about how to proceed.

Default Configuration

Table F-8 Default Configuration for the DBChangeNotifyFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: DBChangeNotify queue delay over 2 minutes
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DBReplicationFailure

This alarm indicates a failure in IDS replication and requires database administrator intervention.

Note Be aware that DBReplicationFailure is based on the replication status perfmon counter (instead of DBReplicationFailure alarm as was previously the case). This alert gets triggered whenever the corresponding replication status perfmon counter specifies a value of **3** (Bad Replication) or **4** (Replication Setup Not Successful).

Default Configuration

Table F-9 Default Configuration for the DBReplicationFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-9 Default Configuration for the DBReplicationFailure RTMT Alert (continued)

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: DBReplicationFailure occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DDRBlockPrevention

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 31 occurs, which invokes a proactive procedure to avoid denial of service. This procedure does not impact call processing; you can ignore replication alarms during this process.

The procedure takes up to 60 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure that the procedure is complete. Do not perform a system reboot during this process.

Default Configuration

Table F-10 Default Configuration for the DDRBlockPrevention RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 31 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DDRDown

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 32 occurs. An auto recover procedure runs in the background and no action is needed.

The procedure takes about 15 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure the procedure is complete.

Default Configuration

Table F-11 Default Configuration for the DDRDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 32 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ExcessiveVoiceQualityReports

This alert gets generated when the number of QRT problems that are reported during the configured time interval exceed the configured value. The default threshold specifies 0 within 60 minutes.

Default Configuration

Table F-12 Default Configuration for the ExcessiveVoiceQualityReports RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of quality reports exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately

Table F-12 Default Configuration for the ExcessiveVoiceQualityReports RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

This alarm gets generated when a Cisco Unified Communications Manager attempts to connect to the Cisco IME server, but the IME distributed cache is not currently active.

Ensure that the certificate for the Cisco IME server is provisioned and that the IME distributed cache has been activated via the CLI.

Default Configuration

Table F-13 Default Configuration for the IMEDistributedCacheInactive Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEOverQuota

This alert indicates that the Cisco Unified Communications Manager servers that use this Cisco IME service have exceed the quota for published direct inward dialing numbers (DIDs) to the IME distributed cache. The alert includes the name of the Cisco IME server as well as the current and target quota values.

Ensure that you have correctly provisioned the DID prefixes on all of the Cisco Unified Communications Manager servers that use this Cisco IME service.

If you have provisioned the prefixes correctly, you have exceeded the capacity of your Cisco IME service, and you need to configure another service and divide the DID prefixes across the Cisco IME client instances (Cisco Unified Communications Managers) on different Cisco IME services.

Default Configuration

Table F-14 Default Configuration for the IMEOverQuota Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP over quota
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEQualityAlert

This alert gets generated when Cisco Unified Communications Manager determines that a substantial number of Cisco IME calls fail back to PSTN or fail to be set up due to IP network quality problems. Two types of events trigger this alert:

- A large number of the currently active Cisco IME calls have all requested fallback or have fallen back to the PSTN.
- A large number of the recent call attempts have gone to the PSTN and not been made over IP.

When you receive this alert, check your IP connectivity. If no problems exist with the IP connectivity, you may need to review the CDRs, CMRs, and logs from the firewalls to determine why calls have fallen back to the PSTN or have not been made over IP.

Default Configuration

Table F-15 Default Configuration for the IMEQualityAlert Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME link quality problem
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Table F-15 Default Configuration for the IMEQualityAlert Alert (continued)

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

This alert gets generated when too many Cisco IME calls that are currently in progress use the same fallback DID and no more DTMF digit sequences exist to allocate to a new Cisco IME call that Cisco Unified Communications Manager is processing. The new call continues, but the call cannot fallback to the PSTN if voice-quality deteriorates.

If this alert gets generated, note the fallback profile that associates with this call. Check that profile in Cisco Unified Communications Manager Administration, and examine the current setting for the "Fallback Number of Correlation DTMF Digits" field. Increase the value of that field by one, and check whether the new value eliminates these alerts. In general, this parameter should be large enough so that the number of simultaneous Cisco IME calls that are made to enrolled numbers that associate with that profile is always substantially less than 10 raised to the power of this number. For example, if you always have fewer than 10,000 simultaneous Cisco IME calls for the patterns that associate with this fallback profile, setting this value to 5 (10 to the power of 5 equals 100,000) should keep Cisco Unified Communications Manager from generating this alert.

However, increasing this value results in a small increase in the amount of time it takes to perform the fallback. As such, you should set the "Fallback Number of Correlation DTMF Digits" field to a value just large enough to prevent this alert from getting generated.

Instead of increasing the value of the DTMF digits field, you can add another fallback profile with a different fallback DID and associate that fallback profile with a smaller number of enrolled patterns. If you use this method, you can use a smaller number of digits.

Default Configuration

Table F-16 Default Configuration for the InsufficientFallbackIdentifiers Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cannot allocate fallback identifier
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within one minute
Schedule	24 hours daily

Table F-16 Default Configuration for the InsufficientFallbackIdentifiers Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

IMEServiceStatus

This alert indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Cisco Unified Communications Manager). The alert indicates the following states:

- 0—Unknown. Likely indicates that the Cisco IME service has not been activated.
- 1—Healthy. Indicates that the Cisco Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.
- 2—Unhealthy. Indicates that the Cisco IME has been activated but has not successfully completed handshake procedures with the Cisco IME server. Note that this counter reflects the handshake status of both the primary and the secondary IME servers.

Default Configuration

Table F-17 Default Configuration for the IMEServiceStatus Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP Connection Problem
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert every 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server because the username and/or password configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the configured username and password match the username and password that are configured in Cisco Unified Communications Manager.

Default Configuration

Table F-18 Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Credential Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowCallManagerHeartbeatRate

This alert occurs when the CallManager heartbeat rate equals less than the configured value.

Default Configuration

Table F-19 Default Configuration for the LowCallManagerHeartbeatRate RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CallManager Server heartbeat rate below 24 beats per minute.

Table F-19 Default Configuration for the LowCallManagerHeartbeatRate RTMT Alert (continued)

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowTFTPServerHeartbeatRate

This alert occurs when TFTP server heartbeat rate equals less than the configured value.

Default Configuration

Table F-20 Default Configuration for the LowTFTPServerHeartbeatRate RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TFTP server heartbeat rate below 24 beats per minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MaliciousCallTrace

This indicates that a malicious call exists in Cisco Unified Communications Manager. The malicious call identification (MCID) feature gets invoked.

Default Configuration

Table F-21 Default Configuration for the MaliciousCallTrace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Malicious call trace generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MediaListExhausted

This alert occurs when the number of MediaListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available media resources that are defined in the media list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table F-22 Default Configuration for the MediaListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of MediaListExhausted events exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately

Table F-22 Default Configuration for the MediaListExhausted RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MgcpDChannelOutOfService

This alert gets triggered when the BRI D-Channel remains out of service.

Default Configuration

Table F-23 Default Configuration for the MgcpDChannelOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: MGCP DChannel is out-of-service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredDevicesExceeded

This alert occurs when the NumberOfRegisteredDevicesExceeded event gets generated.

Default Configuration

Table F-24 Default Configuration for the NumberOfRegisteredDevicesExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-24 Default Configuration for the NumberOfRegisteredDevicesExceeded RTMT Alert

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: NumberOfRegisteredDevicesExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysDecreased

This alert occurs when the number of registered gateways in a cluster decreases between consecutive polls.

Default Configuration

Table F-25 Default Configuration for the NumberOfRegisteredGatewaysDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of registered gateway decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysIncreased

This alert occurs when the number of registered gateways in the cluster increased between consecutive polls.

Default Configuration

Table F-26 Default Configuration for the NumberOfRegisteredGatewaysIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered gateways increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesDecreased

This alert occurs when the number of registered media devices in a cluster decreases between consecutive polls.

Default Configuration

Table F-27 Default Configuration for the NumberOfRegisteredMediaDevicesDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesIncreased

This alert occurs when the number of registered media devices in a cluster increases between consecutive polls.

Default Configuration

Table F-28 Default Configuration for the NumberOfRegisteredMediaDevicesIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredPhonesDropped

This alert occurs when the number of registered phones in a cluster drops more than the configured percentage between consecutive polls.

Default Configuration

Table F-29 Default Configuration for the NumberOfRegisteredPhonesDropped RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered phones in the cluster drops (10%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RouteListExhausted

This alert occurs when the number of RouteListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available channels that are defined in the route list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table F-30 Default Configuration for the RouteListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of RouteListExhausted exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SDLLinkOutOfService

This alert occurs when the SDLLinkOutOfService event gets generated. This event indicates that the local Cisco Unified Communications Manager cannot communicate with the remote Cisco Unified Communications Manager This event usually indicates network errors or a non-running remote Cisco Unified Communications Manager.

Default Configuration

Table F-31 Default Configuration for the SDLLinkOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOutOfService event generated

Table F-31 Default Configuration for the SDLLinkOutOfService RTMT Alert (continued)

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TCPSetupToIMEFailed

This alert occurs when Cisco Unified Communications Manager cannot establish a TCP connection to a Cisco IME server. This alert typically occurs when the IP address and port of the Cisco IME server are misconfigured in Cisco Unified Communications Manager Administration or when an Intranet connectivity problem exists and prevents the connection from being set up.

Ensure that the IP address and port of the Cisco IME server in the alert are valid. If the problem persists, test the connectivity between the Cisco Unified Communications Manager servers and the Cisco IME server.

Default Configuration

Table F-32 Default Configuration for the TCPSetupToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Connection Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TLSConnectionToIMEFailed

This alert occurs when a TLS connection to the Cisco IME service could not be established because the certificate presented by the Cisco IME service has expired or is not in the Cisco Unified Communications Manager CTL.

Ensure that the Cisco IME service certificate has been configured into the Cisco Unified Communications Manager.

Default Configuration

Table F-33 Default Configuration for the TLSConnectionToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLS Failure to Cisco IME service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Additional Information

See the Related Topics, page 9-10.

APPENDIX G

Cisco Unity Connection Alert Descriptions and Default Configurations

The following list comprises the Cisco Unity Connection alerts, their definitions, and default settings.

- NoConnectionToPeer, page G-1
- AutoFailoverSucceeded, page G-2
- AutoFailoverFailed, page G-3
- AutoFailbackSucceeded, page G-4
- AutoFailbackFailed, page G-4
- SbrFailed (Split Brain Resolution Failed), page G-5
- DiskConsumptionCloseToCapacityThreshold, page G-6
- DiskConsumptionExceedsCapacityThreshold, page G-6
- LicenseExpirationWarning, page G-7
- LicenseExpired, page G-8

Note The first six alerts apply to Cisco Unity Connection cluster configurations only. Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster configuration.

NoConnectionToPeer

(Cisco Unity Connection cluster configuration only) This alert is generated when the servers of a Cisco Unity Connection cluster cannot communicate with each other (for example, when the network connection is lost).

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-1 Default Configuration for the NoConnectionToPeer RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: NoConnectionToPeer event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverSucceeded

(Cisco Unity Connection cluster configuration only) This alert is generated in the following conditions:

- When the server with the Secondary status automatically changes its status to Primary (for example, when a critical failure occurs on the server with the Primary status) and assumes responsibility for handling the voice messaging functions and database for the cluster. This alert signals that the following events occurred:
  - The server that originally had the Primary status experienced a serious failure.
  - The server that originally had the Secondary status now has the Primary status and is handling all calls successfully.
- When the server that stopped functioning (described above) is brought back online and the server status automatically changes so that both servers resume sharing responsibility for handling the voice messaging functions and replication.

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-2 Default Configuration for the AutoFailoverSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational

Table G-2 Default Configuration for the AutoFailoverSucceeded RTMT Alert (continued)

Value	Default Configuration
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverSucceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverFailed

(Cisco Unity Connection cluster configuration only) This alert is generated in the following conditions:

- When the server with the Secondary status attempts to automatically change its status to Primary (for example, when a critical failure occurs on the server with the Primary status), but the automatic server status change fails so that the server with the Secondary status keeps the Secondary status.
- When a server that has stopped functioning (for example, a critical failure occurred) is not brought back online. Only one server in the cluster is functioning.

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-3 Default Configuration for the AutoFailoverFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table G-3 Default Configuration for the AutoFailoverFailed RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

AutoFailbackSucceeded

(Cisco Unity Connection cluster configuration only) This alert is generated when the problem that caused the server with the Primary status to stop functioning (causing the server with the Secondary status to change its status to Primary) is resolved and both servers are again online. Then, the servers automatically change status so that the server that had stopped functioning has the Primary status and the other server has the Secondary status.

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-4 Default Configuration for the AutoFailbackSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackSucceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailbackFailed

(Cisco Unity Connection cluster configuration only) This alert occurs when the Publisher server is not online and the server with the Primary status fails to automatically change status.

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-5 Default Configuration for the AutoFailbackFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SbrFailed (Split Brain Resolution Failed)

When a Cisco Unity Connection cluster is configured, if two servers cannot communicate with each other, they will both have the Primary status at the same time (a "split brain" condition), handle voice messaging functions, save messages to their own message stores, but not perform any replication. Users can retrieve their messages, but only one server knows that these messages have been retrieved.

When both servers are able to communicate with each other, they resolve this split brain condition by determining the correct contents and state of each user mailbox:

- Whether new messages that have been received.
- Whether MWIs for new messages have already been sent.
- Which messages have been listened to.
- Which messages have been deleted.

If the resolution of the split brain condition fails, this alert occurs.

Note Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster and this alert.

Default Configuration

Table G-6 Default Configuration for the SbrFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational

Table G-6 Default Configuration for the SbrFailed RTMT Alert (continued)

Value	Default Configuration
Threshold	Trigger alert when following condition met: SbrFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionCloseToCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server reaches ten percent below the percentage limit that the **System Settings > Advanced > Disk Capacity** window in Cisco Unity Connection Administration specifies. For example, with a capacity threshold limit of 95 percent, the alert gets triggered when usage reaches at least 85 percent.

Default Configuration

Table G-7 Default Configuration for the DiskConsumptionCloseToCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionCloseToCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionExceedsCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server meets or exceeds the percentage limit that the **System Settings > Advanced > Disk Capacity** window in Cisco Unity Connection Administration specifies.

Default Configuration

Table G-8 Default Configuration for the DiskConsumptionExceedsCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionExceedsCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpirationWarning

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. Before the license expiration date is reached, the system sends a message, and this alert occurs. The log indicates how many days remain until the license expires.

Default Configuration

Table G-9 Default Configuration for the LicenseExpirationWarning RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpirationWarning event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpired

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. When the license expiration date is reached, the license becomes invalid, and this alert occurs.

Default Configuration

Table G-10 Default Configuration for the LicenseExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Additional Information

For additional information, see the "Related Topics" section on page 9-10.

APPENDIX H

Cisco Intercompany Media Engine Alert Descriptions and Default Configurations

The following list comprises the Cisco Intercompany Media Engine alerts, their definitions, and default settings:

- BannedFromNetwork, page H-1
- IMEDistributedCacheCertificateExpiring, page H-2
- IMEDistributedCacheFailure, page H-3
- IMESdlLinkOutOfService, page H-3
- InvalidCertificate, page H-4
- InvalidCredentials, page H-5
- MessageOfTheDay, page H-5
- SWUpdateRequired, page H-6
- TicketPasswordChanged, page H-7
- ValidationsPendingExceeded, page H-7

BannedFromNetwork

This alert indicates that network administrators have banned this Cisco IME server from the network (IME distributed cache ring), making this Cisco IME service fully or partly inoperative. Network administrators rarely ban servers but do so if they detect that the server is being used to launch malicious attacks into the network. If you receive this alert in error, contact TAC immediately.

Default Configuration

Table H-1 Default Configuration for the BannedFromNetwork Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers

Table H-1 Default Configuration for the BannedFromNetwork Alert (continued)

Value	Default Configuration
Threshold	Trigger alert when following condition met: Cisco IME service banned from network
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheCertificateExpiring

This alert indicates the number of days that remain until the certificate that is used for the IME distributed cache expires. You must replace the certificate prior to expiration.

Default Configuration

Table H-2 Default Configuration for the IMEDistributedCacheCertificateExpiring Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME distributed cache certificate about to expire. 14 days.
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheFailure

This alert indicates the health of the IME distributed cache. A value of zero (red) means that the IME distributed cache is suffering from a significant problem such as one of the following conditions:

- The Cisco IME cannot resolve issues after the network was partitioned. In this case, validation attempts may fail.
- The Cisco IME service is not connected to the network at all and is unable to reach the bootstrap servers.

A value of one (yellow) indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. Check for any alarms that may indicate why this counter is 1. A value of two indicates that IME distributed cache is functioning normally and the system is considered healthy.

Default Configuration

Table H-3 Default Configuration for the IMEDistributedCacheFailure Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IME distributed cache failure in states 1: network experience minor issues 0: network in trouble
Duration	Trigger alert immediately
Frequency	Trigger 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMESdlLinkOutOfService

This alert indicates that the Cisco IME service has lost communication with Cisco IME Config Manager services, such as Cisco AMC service or Cisco CallManager service.

This alert usually indicates that one of these services has gone down (either intentionally, for maintenance; or unintentionally, due to a service failure or connectivity failure).

Default Configuration

Table H-4 Default Configuration for the IMESdlLinkOutOfService Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOOS event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCertificate

This alert indicates that the administrator enabled the IME distributed cache on the Cisco IME server but omitted the configuration of a valid certificate or configured an incorrect certificate.

Default Configuration

Table H-5 Default Configuration for the InvalidCertificate Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid certificate configured
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server, because the username and password that are configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the username and password that are configured match those configured in Cisco Unified Communications Manager.

Default Configuration

Table H-6 Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid or mismatched credentials.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MessageOfTheDay

The Cisco IME service generates this alert when the administrators of the Cisco IME network have a message for you.

Default Configuration

Table H-7 Default Configuration for the MessageOfTheDay Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers

Table H-7 Default Configuration for the MessageOfTheDay Alert (continued)

Value	Default Configuration
Threshold	Trigger alert when following condition met: Message from network administrators
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SWUpdateRequired

The Cisco IME server generates this alert when a new version of the Cisco IME server software is required. This alert repeats until you perform the upgrade. To obtain more information about the software update, go to the Cisco website. You should install critical updates within days of receiving this alert.

These upgrades address security vulnerabilities or key functional outages. In some cases, if you do not apply a critical upgrade immediately, the Cisco IME server may become unable to connect to the network.

Default Configuration

Table H-8 Default Configuration for the SWUpdateRequired Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Software update required
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TicketPasswordChanged

The Cisco IME server generates this alert when the administrator changes the password that is used to generate the validation tickets.

Verify that an authorized administrator changed the password. Unauthorized changes may indicate compromise to the administrative interfaces on the Cisco IME service. If you determine that unauthorized changes have been made, change the administrative passwords on the Cisco IME server immediately to prevent further unauthorized access. To change the administrative password, type **set password admin** in the Cisco IME server CLI.

Default Configuration

Table H-9 Default Configuration for the TicketPasswordChanged Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Ticket password changed
Duration	Trigger alert immediately
Frequency	Trigger on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ValidationsPendingExceeded

This alert indicates the number of pending validations on the Cisco IME server. This number provides an indicator of the backlog of work on the Cisco IME server.

Default Configuration

Table H-10 Default Configuration for the ValidationsPendingExceeded Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Table H-10 Default Configuration for the ValidationsPendingExceeded Alert (continued)

Value	Default Configuration
Threshold	Trigger alert when following condition met: Cisco IME pending validations exceeded 100
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

INDEX

A

absolute range 11-20
alert central, accessing 10-1
alert notification
  configuring parameters for counter (table) 6-6
  e-mail for counter 6-5
  message 6-5
  schedule 6-5
  thresholds 6-5
alert notification, configuring 10-6
alerts
  accessing alert central 10-1
  action configuration (table) 9-8
  configuring actions 10-6
  configuring e-mail for 10-6
  configuring with Default alert action 10-7
  customization (table) 9-6
  emailing notification 3-5
  logs, described 9-9
  notification for a counter 3-5
  preconfigured 9-2
  scheduling notification 3-5
  setting properties 10-3
  suspending 10-5
  thresholds 3-5
audit logs 11-19
  browse 11-19
  download 11-19
  schedule download 11-19

B

browse audit logs 11-19

C

call control discovery
  reports
    learned patterns 5-25
category
  adding 6-2
  deleting 6-3
  renaming 6-2
category tabs
  described 3-3
  sample rates 3-3
Cisco Analog Access
  perfmon object and counters B-2
Cisco Annunciator Device
  perfmon object and counters B-3
Cisco CallManager
  perfmon object and counters B-4
Cisco CallManager System Performance
  perfmon object and counters B-12
Cisco CTIManager
  perfmon object and counters B-14
Cisco Dual-Mode Mobility perfmon object and counters B-15
Cisco Extension Mobility
  perfmon object and counters B-16
Cisco Gatekeeper
  perfmon object and counters B-17
Cisco H.323

perfmon object and counters B-17
Cisco Hunt Lists
perfmon object and counters B-18
Cisco HW Conference Bridge Device
perfmon object and counters B-19
Cisco IP Manager Assistant
perfmon object and counters B-20
Cisco Lines
perfmon object and counters B-20
Cisco Locations
perfmon object and counters B-21
Cisco Media Streaming Application
perfmon object and counters B-22
Cisco Messaging Interface
perfmon object and counters B-25
Cisco MGCP BRI Device
perfmon object and counters B-25
Cisco MGCP FXO Device
perfmon object and counters B-26
Cisco MGCP FXS Device
perfmon object and counters B-26
Cisco MGCP Gateways
perfmon object and counters B-27
Cisco MGCP Gateways B-28
Cisco MGCP PRI Device
perfmon object and counters B-28
Cisco MGCP T1CAS Device
perfmon object and counters B-28
Cisco MOH Device
perfmon object and counters B-29, B-30
Cisco MTP Device
perfmon object and counters B-31
Cisco Phones
perfmon object and counters B-31
Cisco Presence Feature
perfmon object and counters B-32
Cisco QSIG Feature
perfmon object and counters B-32
Cisco Signaling Performance
perfmon object and counters B-33
Cisco SIP
perfmon object and counters B-32, B-33
Cisco SIP Normalization
perfmon object and counters B-34
Cisco SIP Stack
perfmon object and counters B-41
Cisco SW Conf Bridge Device
perfmon object and counters B-51
Cisco TFTP Server
perfmon object and counters B-51
Cisco Tomcat Connector
perfmon object and counters A-2
Cisco Transcode Device
perfmon object and counters B-55
Cisco Unity Connection
using Port Monitor 8-1
Cisco Video Conference Bridge
perfmon object and counters B-55
Cisco WebDialer
perfmon object and counters B-56
Cisco WSM Connector
perfmon object and counters B-57
configuration profile
adding 2-7
deleting 2-8
restoring 2-7
using default 2-7
conventions 1-xix
counters
adding 6-3
alert notification 3-5
alert notification parameters (table) 6-6
configuring alert notification for 6-5
data sample, configuring 6-9
data sample parameters (table) 6-9
properties 3-4
viewing data 6-10
zooming 3-3, 3-4

CTI
Cisco CTIManager
perfmon object and counters B-14
finding CTI devices 5-17
monitoring CTI applications 5-21
monitoring CTI devices 5-22
monitoring CTI lines 5-23
viewing CTIManager information 5-21
CUC Data Store, perfmon object and counters C-2
CUC Data Store: Databases, perfmon object and counters C-2
CUC Digital Notifications, perfmon object and counters C-3
CUC Directory Services, perfmon object and counters C-3
CUC Message Store, perfmon object and counters C-3
CUC Message Store: Databases, perfmon object and counters C-5
CUC Personal Call Transfer Rules, perfmon object and counters C-5
CUC Phone System, perfmon object and counters C-5
CUC Phone System: Ports, perfmon object and counters C-8
CUC Replication, perfmon object and counters C-8
CUC Replicator: Remote Connection Locations, perfmon object and counters C-8
CUC Sessions: Calendar Access, perfmon object and counters C-9
CUC Sessions: E-mail Access, perfmon object and counters C-9
CUC Sessions: IMAP Server, perfmon object and counters C-10
CUC Sessions: RSS, perfmon object and counters C-11
CUC Sessions: SMTP Server, perfmon object and counters C-11
CUC Sessions: SpeechView Processor, perfmon object and counters C-12
CUC Sessions: TRaP, perfmon object and counters C-12
CUC Sessions: TTS, perfmon object and counters C-13
CUC Sessions: Unified Client, perfmon object and counters C-13
CUC Sessions: Voice, perfmon object and counters C-13
CUC Sessions: VUI, perfmon object and counters C-15
CUC Sessions: Web, perfmon object and counters C-15
CUC Sessions: Web E-mail Access, perfmon object and counters C-16

D

Database Change Notification Client
perfmon object and counters A-5
Database Change Notification Server
perfmon object and counters A-6
Database Change Notification Subscription
perfmon object and counters A-7
Database Local DSN
perfmon object and counters A-7
data sample
configuring parameters (table) 6-9
DB User Host Information Counters
perfmon object and counters A-7
document
audience 1-xvi
conventions 1-xix
organization 1-xvi
purpose 1-xv
documentation
related 1-xviii
download audit logs 11-19

E

e-mail configuration
alerts 10-6
Enterprise Replication DBSpace Monitors
perfmon object and counters A-7
Enterprise Replication Perfmon Counters
perfmon object and counters A-8

I

IME Configuration Manager

perfmon object and counters D-1
IME Server
perfmon object and counters D-2
IME Server System Performance
perfmon object and counters D-3
installation logs
collecting 11-7
IP
perfmon object and counters A-8
IP6
perfmon object and counters A-9

L

learned pattern reports 5-25
Log Partition Monitoring
configuring 13-1
logs
alerts 9-9

M

Memory
perfmon object and counters A-10
monitoring
CTI applications 5-21
CTI devices 5-17, 5-22
CTI lines 5-23
gateways 5-17
H.323 devices 5-17
hunt list 5-17
media resources 5-17
phones 5-17
SIP trunk 5-17
voice-mail devices 5-17

N

Network Interface
perfmon object and counters A-12
Number of Replicates
perfmon object and counters A-13

O

object and counters
Database Change Notification Client A-5
organization 1-xvi

P

Partition
perfmon object and counters A-13
perfmon
counters
adding 6-3
category tabs, described 3-3
properties 3-4
sample rates 3-3
object and counters
Cisco Analog Access B-2
Cisco Annunciator Device B-3
Cisco CallManager B-4
Cisco CallManager System Performance B-12
Cisco Call Restriction B-3
Cisco CTIManager B-14
Cisco Dual-Mode Mobility B-15
Cisco Extension Mobility B-16
Cisco Gatekeeper B-17
Cisco H.323 B-17
Cisco Hunt Lists B-18
Cisco HW Conference Bridge Device B-19
Cisco IP Manager Assistant B-20
Cisco Lines B-20
Cisco Locations B-21

Cisco Media Streaming Application B-22
Cisco Messaging Interface B-25
Cisco MGCP FXO Device B-26
Cisco MGCP FXS Device B-26
Cisco MGCP Gateways B-27
Cisco MGCP PRI Device B-28
Cisco MGCP T1CAS Device B-28
Cisco MobilityManager B-29
Cisco MOH Device B-30
Cisco MTP Device B-31
Cisco Phones B-31
Cisco Presence Feature B-32
Cisco QSIG Feature B-32
Cisco Signaling Performance B-33
Cisco SIP B-32, B-33
Cisco SIP Stack B-41
Cisco SIP Station B-49
Cisco SW Conf Bridge Device B-51
Cisco TFTP Server B-51
Cisco Tomcat Connector A-2
Cisco Transcode Device B-55
Cisco Video Conference Bridge B-55
Cisco WebDialer B-56
Cisco WSM Connector B-57
CUC Data Store C-2
CUC Data Store: Databases C-2
CUC Digital Notifications C-3
CUC Directory Services C-3
CUC Message Store C-3
CUC Message Store: Databases C-5
CUC Personal Call Transfer Rules C-5
CUC Phone System C-5
CUC Phone System: Ports C-8
CUC Replication C-8
CUC Replicator: Remote Connection Locations C-8
CUC Sessions: E-mail Access C-9
CUC Sessions: IMAP Server C-10
CUC Sessions: RSS C-11
CUC Sessions: SMTP Server C-11
CUC Sessions: TRaP C-12
CUC Sessions: TTS C-13
CUC Sessions: Unified Client C-13
CUC Sessions: Voice C-13
CUC Sessions: VUI C-15
CUC Sessions: Web C-15
CUC Sessions: Web E-mail Access C-16
Database Change Notification Server A-6
Database Change Notification Subscription A-7
Database Local DSN A-7
DB User Host Information A-7
Enterprise Replication A-8
Enterprise Replication DBSpace Monitors A-7
IME Configuration Manager D-1
IME Server D-2
IME Server System Performance D-3
IP A-8
IP6 A-9
Memory A-10
Network Interface A-12
Partition A-13
Process A-14
Processor A-16
System A-16
TCP A-17
Thread A-18
Tomcat JVM A-3
Tomcat Web Application A-4
Perfmon data logging 7-4
perfmon data logging
troubleshooting 3-5
understanding 3-5
perfmon logs
understanding 3-5
performance counter
adding a counter instance 6-5
removing 6-4
performance counters

displaying in chart format 6-3
displaying in table format 6-3
performance monitoring
category tabs,described 3-3
configuring alert notification for counters 6-5
counters
adding 6-3
properties 3-4
Number of Replicates A-13
object and counters
Cisco Analog Access B-2
Cisco Annunciator Device B-3
Cisco CallManager B-4
Cisco CallManager System Performance B-12
Cisco CTIManager B-14
Cisco Dual-Mode Mobility B-15
Cisco Extension Mobility B-16
Cisco Gatekeeper B-17
Cisco H.323 B-17
Cisco Hunt Lists B-18
Cisco HW Conference Bridge Device B-19
Cisco IP Manager Assistant B-20
Cisco Lines B-20
Cisco Locations B-21
Cisco Media Streaming Application B-22
Cisco Messaging Interface B-25
Cisco MGCP BRI Device B-25
Cisco MGCP FXO Device B-26
Cisco MGCP FXS Device B-26
Cisco MGCP Gateways B-27
Cisco MGCP PRI Device B-28
Cisco MGCP T1CAS Device B-28
Cisco Mobility Manager B-29
Cisco MOH Device B-30
Cisco MTP Device B-31
Cisco Phones B-31
Cisco Presence Feature B-32
Cisco QSIG Feature B-32
Cisco Signaling Performance B-33
Cisco SIP B-32, B-33
Cisco SIP Normalization B-34
Cisco SIP Stack B-41
Cisco SIP Station B-49
Cisco SW Conf Bridge Device B-51
Cisco TFTP Server B-51
Cisco Tomcat Connector A-2
Cisco Transcode Device B-55
Cisco Video Conference Bridge B-55
Cisco WebDialer B-56
Cisco WSM Connector B-57
CUC Data Store C-2
CUC Data Store: Databases C-2
CUC Digital Notifications C-3
CUC Directory Services C-3
CUC Message Store C-3
CUC Message Store: Databases C-5
CUC Personal Call Transfer Rules C-5
CUC Phone System C-5
CUC Phone System: Ports C-8
CUC Replication C-8
CUC Replicator: Remote Connection Locations C-8
CUC Sessions: Calendar Access C-9
CUC Sessions: E-mail Access C-9
CUC Sessions: IMAP Server C-10
CUC Sessions: RSS C-11
CUC Sessions: SMTP Server C-11
CUC Sessions: SpeechView Processor C-12
CUC Sessions: TRaP C-12
CUC Sessions: TTS C-13
CUC Sessions: Unified Client C-13
CUC Sessions: Voice C-13
CUC Sessions: VUI C-15
CUC Sessions: Web C-15
CUC Sessions: Web E-mail Access C-16
Database Change Notification Server A-6
Database Change Notification Subscription A-7
Database Local DSN A-7

DB User Host Information A-7
Enterprise Replication A-8
Enterprise Replication DBSpace Monitors A-7
IME Configuration Manager D-1
IME Server D-2
IME Server System Performance D-3
IP A-8
IP6 A-9
Memory A-10
Network Interface A-12
Number of Replicates A-13
Partition A-13
Process A-14
Processor A-16
System A-16
Thread A-18
Tomcat JVM A-3
Tomcat Web Application A-4
sample rates 3-3
viewing counter data 6-10
performance queries 6-3
plug-ins
accessing 13-1
downloading 13-1
polling intervals
sample rate 3-3
polling rate 5-20
Port Monitor
using 8-1
Process
perfmon object and counters A-14
Processor
perfmon object and counters A-16

R

Real-Time Monitoring Tool
alert notification
configuring for a counter 6-5
alerts
accessing alert central 10-1
action configuration (table) 9-8
configuring alert actions 10-6
configuring e-mail for 10-6
configuring with Default alert action 10-7
customization (table) 9-6
logs, described 9-9
notification for a counter 3-5
preconfigured 9-2
setting properties 10-3
suspending 10-5
category
adding 6-2
deleting 6-3
renaming 6-2
category tabs,described 3-3
collecting a crash dump 11-16
collecting traces 11-3
collecting traces using the query wizard 11-8
collecting traces using the schedule collection option 11-12
configuration profile
adding 2-7
deleting 2-8
restoring 2-7
using default 2-7
counters
alert notification 3-5
data sample 6-9
displaying property description 6-8
viewing data 6-10
zooming 3-3, 3-4
data samples 6-9
deleting scheduled collections 11-15
finding
CTI applications 5-21
CTI devices 5-22
CTI lines 5-23

devices 5-17
highlighting a chart 3-4
logging and report generation
call log 5-7
device log 5-16
server log 4-4
service log 5-13
polling interval 3-3
polling rate, configuring 5-20
related topics for trace collection 11-33
sample rate 3-3
session trace 5-8
SysLog Viewer 12-1
updating trace configuration settings 11-32
using the real time trace option 11-28
using the real time trace option, monitor user event 11-29
using the real time trace option, view real time data 11-28
viewing
CTIManager information 5-21
device properties 5-19
phone information 5-19
viewing trace collection status 11-15
viewing trace files using the local browse option 11-22
viewing trace files using the remote browse option 11-23
zooming a counter 3-3
related documentation 1-xviii
relative range 11-21
reports
learned patterns 5-25

S

sample rate 3-3
schedule download of audit logs 11-19
server authentication certificates
importing using the trace collection option 11-2
SysLog Viewer 12-1
System
perfmon object and counters A-16

T

TCP A-17
perfmon object and counters A-17
Thread
perfmon object and counters A-18
Tomcat JVM
perfmon object and counters A-3
Tomcat Web Application
perfmon object and counters A-4
Trace
collection
collecting crash dump option 11-16
collecting files option 11-3
configuration, described 11-1
deleting scheduled collections 11-15
list of topics 11-1
related topics 11-33
schedule collection option 11-12
using the local browse option 11-22
using the query wizard option 11-8
using the real time trace option 11-28
using the real time trace option, monitor user event 11-29
using the real time trace option, view real time data 11-28
using the remote browse option 11-23
viewing status 11-15
trace and log central
collecting installation and upgrade logs 11-7
troubleshooting
Perfmon data logging
configuring 7-4
parameters 7-5
viewing log files 7-3

U

upgrade logs
collecting 11-7

Z

zooming a counter 3-3, 3-4