Cisco Unified Serviceability Administration Guide, Release11.5(1)SU1

First Published: August 22, 2016

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

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.

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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://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. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xi

Purpose xi

Audience xii

Related Documentation xii

Conventions xii

Obtain Documentation, Support, and Security Guidelines xiv

Cisco Product Security Overview xiv

Documentation Organization xiv

CHAPTER 1

Seviceability Administrative Overview 1

Overview 1

Reporting Tools 2

Remote Serviceability Tools 3

Customized Login Message 3

CHAPTER 2

Getting Started 5

Access 5

Access Cisco Unified IM and Presence Serviceability 6

Install Server Certificate 7

HTTPS 7

Install Internet Explorer 7 Certificate 8

Serviceability Interface 9

CHAPTER 3

Alarms 13

Overview 13

Alarm Configuration 14

Alarm Definitions 15

Alarm Information 16
Set Up Alarms 16
Alarm Service Setup 17
Syslog Agent Enterprise Parameters 17
Set Up Alarm Service 17
Set Up Alarm Services That Use Cisco Tomcat 19
Service Groups 19
Alarm Configuration Settings 20
Alarm Definitions and User-Defined Description Additions 24
View Alarm Definitions and Add User-Defined Descriptions 24
System Alarm Catalog Descriptions 25
CallManager Alarm Catalog Descriptions 26
IM and Presence Alarm Catalog Descriptions 27

CHAPTER 4 Trace 29

Trace 29
Trace Configuration 30
Trace Settings 30
Trace Collection 31
Called Party Tracing 31
Set Up Trace Configuration 31
Configure Trace 32
Set Up Trace Parameters 32
Service Groups in Trace Configuration 34
Debug Trace Level Settings 40
Trace Field Descriptions 41
Database Layer Monitor Trace Fields 41
Cisco RIS Data Collector Trace Fields 42
Cisco CallManager SDI Trace Fields 43
Cisco CallManager SDL Trace Fields 44
Cisco CTIManager SDL Trace Fields 46
Cisco Extended Functions Trace Fields 47
Cisco Extension Mobility Trace Fields 48
Cisco IP Manager Assistant Trace Fields 49
Cisco IP Voice Media Streaming App Trace Fields 49

Cisco TFTP Trace Fields 50
Cisco Web Dialer Web Service Trace Fields 50
IM and Presence SIP Proxy Service Trace Filter Settings 51
IM and Presence Trace Field Descriptions 52
Cisco Access Log Trace Fields 52
Cisco Authentication Trace Fields 52
Cisco Calendar Trace Fields 52
Cisco CTI Gateway Trace Fields 53
Cisco Database Layer Monitor Trace Fields 53
Cisco Enum Trace Fields 53
Cisco Method/Event Trace Fields 53
Cisco Number Expansion Trace Fields 54
Cisco Parser Trace Fields 54
Cisco Privacy Trace Fields 54
Cisco Proxy Trace Fields 54
Cisco RIS Data Collector Trace Fields 55
Cisco Registry Trace Fields 55
Cisco Routing Trace Fields 56
Cisco Server Trace Fields 56
Cisco SIP Message and State Machine Trace Fields 56
Cisco SIP TCP Trace Fields 56
Cisco SIP TLS Trace Fields 57
Cisco Web Service Trace Fields 57
Trace Output Settings 57
Trace Setting Troubleshooting 58
Troubleshoot Trace Settings Window 58
Troubleshoot Trace Settings 58

CHAPTER 5 Services 61
Feature Services 61
Database and Administration Services 62
Locations Bandwidth Manager 62
Cisco AXL Web Service 62
Cisco UXL Web Service 63
Cisco Bulk Provisioning Service 63

Cisco TAPS Service 63
Platform Administrative Web Service 63
Performance and monitoring services 64
Cisco Serviceability Reporter 64
Cisco CallManager SNMP Service 64
CM Services 64
Cisco CallManager 64
Cisco TFTP 65
Cisco Unified Mobile Voice Access Service 65
Cisco IP Voice Media Streaming App 66
Cisco CTIManager 66
Cisco Extension Mobility 66
Cisco Dialed Number Analyzer 66
Cisco Dialed Number Analyzer Server 66
Cisco DHCP Monitor Service 67
Cisco Intercluster Lookup Service 67
Cisco UserSync Service 67
Cisco UserLookup Web Service 67
IM and Presence Services 67
Cisco SIP Proxy 67
Cisco Presence Engine 67
Cisco XCP Text Conference Manager 68
Cisco XCP Web Connection Manager 68
Cisco XCP Connection Manager 68
Cisco XCP SIP Federation Connection Manager 68
Cisco XCP XMPP Federation Connection Manager 68
Cisco XCP Message Archiver 68
Cisco XCP Directory Service 68
Cisco XCP Authentication Service 69
CTI Services 69
Cisco IP Manager Assistant 69
Cisco WebDialer Web Service 69
Self-Provisioning IVR 69
CDR Services 70
CAR Web Service 70

Cisco SOAP - CDROnDemand Service 70
Security Services 70
Cisco CTL Provider 70
Cisco Certificate Authority Proxy Function (CAPF) 71
Directory Services 71
Cisco DirSync 71
Location Based Tracking Services 71
Cisco Wireless Controller Synchronization Service 72
Voice Quality Reporter Services 72
Cisco Extended Functions 72
Network Services 72
Performance and Monitoring Services 72
Backup and Restore Services 73
System Services 74
Platform Services 74
Security Services 76
Database Services 77
SOAP Services 77
CM Services 78
IM and Presence Service Services 78
CDR Services 80
Admin Services 81
Services setup 82
Control Center 82
Set Up Services 82
Service Activation 83
Cluster Service Activation Recommendations for Cisco Unified Communications Manager 83
Cluster Service Activation Recommendations for IM and Presence Service 87
Activate Feature Services 90
Start, Stop, and Restart Services in Control Center or CLI 91
Start, Stop, and Restart Services in Control Center 91
Start, Stop, and Restart Services Using Command Line Interface 92

CHAPTER 6 Tools and Reports 93
Serviceability Reports Archive 93

Serviceability Reporter Service Parameters 94
Device Statistics Report 94
Server Statistics Report 97
Service Statistics Report 100
Call Activities Report 103
Alert Summary Report 107
Performance Protection Report 109
Set Up Serviceability Reports Archive Overview 110
Set Up Serviceability Reports Archive 111
Access to Serviceability Reports Archive 112
Activate Serviceability Reports Archive 112
Access Serviceability Reports Archive 112
CDR Repository Manager 113
Set Up General Parameters 114
General Parameter Settings 115
Set Up Application Billing Servers 116
Application Billing Server Parameter Settings 117
Delete Application Billing Servers 118
Locations 118
Locations Topology 119
View Locations Topology 119
View Assertion Details 120
Locations Discrepancy 120
View Locations Discrepancy 120
Effective Path 121
View Effective Path 122
Disconnected Groups 122
View Disconnected Groups 122

CHAPTER 7 Audit Logs 125
Audit Logs 125
Audit Logging (Standard) 125
Audit Logging (Detailed) 129
Audit Log Types 129
System Audit Logs 129

Application Audit Logs 130
Database Audit Logs 130
Audit Log Configuration Task Flow 130
Set up Audit Logging 131
Configure Remote Audit Log Transfer Protocol 131
Configure Email Server for Alert Notifications 132
Enable Email Alerts 132
Configure Remote Audit Logging for Platform Logs 133
Configure Logstash Server Information 133
Configure the FileBeat Client 133
Audit Log Configuration Settings 134

CHAPTER 8 Simple Network Management Protocol 139
Simple Network Management Protocol Support 139
SNMP Basics 140
SNMP Management Information Base 141
Set Up SNMP 155
Troubleshooting SNMP 155
SNMP Configuration Requirements 156
SNMP Version 1 Support 156
SNMP Version 2c Support 157
SNMP Version 3 Support 157
SNMP Services 157
SNMP Community Strings and Users 158
SNMP Traps and Informs 158
SNMP Trace Configuration 161
SNMP V1 and V2c Setup 161
Find Community String 161
Set Up Community String 162
Community String Configuration Settings 163
Delete Community String 164
Find SNMP V1 and V2c Notification Destination 165
Set Up SNMP V1 and V2c Notification Destination 166
Notification Destination Settings for SNMP V1 and V2c 167
Delete SNMP V1 and V2c Notification Destination 168

SNMP V3 Setup 168
Find SNMP V3 User 169
Set Up SNMP V3 User 169
SNMP V3 User Configuration Settings 170
Delete SNMP V3 User 172
Find SNMP V3 Notification Destination 172
Set Up SNMP V3 Notification Destination 173
Notification Destination Settings for SNMP V3 174
Delete SNMP V3 Notification Destination 175
MIB2 System Group 176
Set Up MIB2 System Group 176
MIB2 System Group Settings 177
SNMP Trap Settings 177
Set Up SNMP Traps 177
Generate SNMP Traps 178
CISCO-SYSLOG-MIB Trap Parameters 181
CISCO-CCM-MIB Trap Parameters 182
CISCO-UNITY-MIB Trap Parameters 183

CHAPTER 9 **Call Home** 185
Call Home 185
Smart Call Home 185
Anonymous Call Home 186
Smart Call Home Interaction 189
Prerequisites for Call Home 190
Access Call Home 190
Call Home Settings 190
Call Home Configuration 191
Limitations 194
References for Call Home 194

Preface

- Purpose, page xi
- Audience, page xii
- Related Documentation, page xii
- Conventions, page xii
- Obtain Documentation, Support, and Security Guidelines, page xiv
- Cisco Product Security Overview, page xiv
- Documentation Organization, page xiv

Purpose

The *Cisco Unified Serviceability Administration Guide* provides descriptions and procedures for configuring alarms, traces, SNMP, and through Cisco Unified Serviceability for the following:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unity Connection

Tip For Cisco Unity Connection, you must perform serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability; for example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

Cisco Unified Serviceability supports the functionality that is described in the *Cisco Unified Serviceability Administration Guide*; for tasks that are specific to Cisco Unity Connection Serviceability, refer to the *Cisco Unity Connection Serviceability Administration Guide*.

Audience

The *Cisco Unified Serviceability Administration Guide* assists administrators that configure, troubleshoot, and support Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, or Cisco Unity Connection. This guide requires knowledge of telephony and IP networking technology.

Related Documentation

Use this guide with the documentation for your configuration.

Product	Documentation
Cisco Unified Communications Manager	*Cisco Unified Real-Time Monitoring Tool Administration Guide*, *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*, and *Cisco Unified Communications Manager Call Detail Records Administration Guide*
Cisco Unified Communications Manager IM and Presence Service	*Cisco Unified Real-Time Monitoring Tool Administration Guide*
Cisco Unity Connection	*Cisco Unity Connection Serviceability Administration Guide*, and *Cisco Unified Real-Time Monitoring Tool Administration Guide*

These documents provide the following information:

- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide* - This document describes how to configure and use Cisco Unified Communications Manager CDR Analysis and Reporting, a tool that is used to create user, system, device, and billing reports.
- *Cisco Unified Communications Manager Call Detail Records Administration Guide* - This document includes call detail record (CDR) definitions.
- *Cisco Unified Real-Time Monitoring Tool Administration Guide* - This document describes how to use Unified RTMT, a tool that allows you to monitor many aspects of the system, such as critical services, alerts, and performance counters.
- *Cisco Unity Connection Serviceability Administration Guide* - This document provides descriptions and procedures for using alarms, traces, clusters, and reports through Cisco Unity Connection Serviceability.

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.
^	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.

Obtain Documentation, 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`.

Documentation Organization

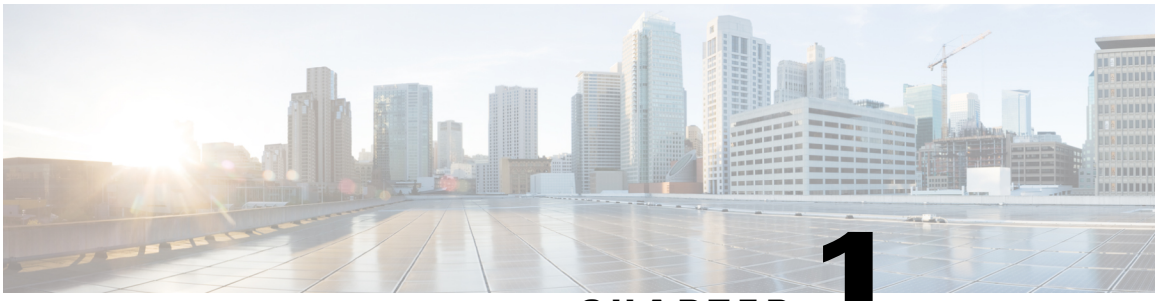
Provides information about Cisco Unified Serviceability for Unified Communications Manager and IM and Presence Serviceability configuration procedures.

- Cisco Unified Serviceability — Overview of Serviceability, including browser support.
- Getting Started — Description of how to access and use the Serviceability GUI.
- Alarms — Overview of Serviceability GUI alarms and alarm definitions, procedures for configuring alarms, and procedures for searching and editing alarm definitions.
- Trace — Overview of trace parameter configuration, and an overview of trace collection in the Cisco Unified Real-Time Monitoring Tool. Provides procedures for configuring trace parameters for network and feature services and for configuring the troubleshooting trace settings for services.
- Tools and Reports — Description of each network and feature service that displays; provides procedures and recommendations for activating, deactivating, starting, and stopping feature and network services.

Provides an overview on the reports that are generated by the Cisco Serviceability Reporter service; provides procedures for viewing reports that are generated by the Cisco Serviceability Reporter service.

  - Unified Communications Manager only: Provides information on using the CDR Management Configuration window to set the amount of disk space to allocate call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure billing application server destinations for CDRs.

- Simple Network Management Protocol — Overview of support of Simple Network Management Protocol (SNMP) versions 1, 2c, and 3, and configuration procedures.
- Call Home — Overview of the Call Home service and describes how to configure the Call Home feature.



CHAPTER 1

Seviceability Administrative Overview

- Overview, page 1
- Reporting Tools, page 2
- Remote Serviceability Tools, page 3
- Customized Login Message, page 3

Overview

Cisco Unified Serviceability is a web-based troubleshooting tool that provides the following functionality:

- Saves alarms and events for troubleshooting and provides alarm message definitions.
- Saves trace information to log files for troubleshooting.
- Monitors real-time behavior of components through the Cisco Unified Real-Time Monitoring Tool (Unified RTMT).
- Provides audit capability by logging configuration changes to the system by a user or as a result of the user action. This functionality supports the Information Assurance feature of Cisco Unified Communications Manager and Cisco Unity Connection.
- Provides feature services that you can activate, deactivate, and view through the **Service Activation** window.
- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Cisco Unified Communications Manager, IM and Presence Service and Cisco Unity Connection to work as a managed device for Simple Network Management Protocol (SNMP) remote management and troubleshooting.
- Monitors the disk usage of the log partition on a node (or all nodes in the cluster).
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.
- Cisco Unified Communications Manager only: Generates Cisco Unified Communications Manager reports for Quality of Service, traffic, and billing information through Cisco Unified Communications Manager CDR Analysis and Reporting.

Note IM and Presence Service uses a different Serviceability interface than the others and therefore is referred to separately when required.

Tip Cisco RIS Data Collector provides Process and Thread statistic counters in the Cisco Unified Real-Time Monitoring Tool. To configure the maximum number of processes and threads that are allowed, so Cisco RIS Data Collector can provide these associated counters, access the Maximum Number of Threads and Process service parameter for the Cisco RIS Data Collector service in the administration interface for your configuration.

Cisco Unified Communications Manager: For information on configuring service parameters, refer to the *System Configuration Guide for Cisco Unified Communications Manager*.

Cisco Unity Connection: For information on configuring service parameters, refer to the *System Administration Guide for Cisco Unity Connection*.

Tip Cisco Unity Connection only: For Cisco Unity Connection, you must perform serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability; for example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

Cisco Unified Serviceability supports the functionality that is described in the Cisco Unified Serviceability Administration Guide; for tasks that are specific to Cisco Unity Connection Serviceability, refer to the *Cisco Unity Connection Serviceability Administration Guide*.

Reporting Tools

Cisco Unified Serviceability provides the following reporting tools:

- Cisco Unified Communications Manager only:
  - Cisco Unified Communications Manager only:Cisco Unified Communications Manager CDR Analysis and Reporting - Generates Cisco Unified Communications Manager reports for Quality of Service, traffic, and billing information through Cisco Unified Communications Manager CDR Analysis and Reporting. For more information, see *CDR Analysis and Reporting Administration Guide*.
  - Cisco Unified Communications Manager only: Cisco Unified Communications Manager Dialed Number Analyzer - Allows you to test and diagnose a deployed Cisco Unified Communications Manager dial plan configuration, analyze the test results, and use the results to improve the dial plan. For more information on how to access and use Dialed Number Analyzer, see *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.
  - Cisco Unified Communications Manageronly: Cisco Unified Reporting Web Application - Allows you to inspect or troubleshoot data for a standalone server or a cluster. This application, which is separate from Cisco Unified Serviceability, combines data by category from all accessible Cisco Unified Communications Manager servers in a cluster into one output view. Some reports run health checks to identify conditions that could affect server or cluster operations. If you are an

authorized user, you access Cisco Unified Reporting in the main navigation menu in Cisco Unified Communications Manager Administration or with the**File** > **Cisco Unified Reporting** link on the Unified RTMT menu. For more information, see *Cisco Unified Reporting Administration Guide*.

Serviceability Reports Archive - Archives reports that the Cisco Serviceability Reporter service generates.

- Cisco Unified Real-Time Monitoring Tool (Unified RTMT) - Monitors real-time behavior of components through Unified RTMT; creates daily reports that you can access through the Serviceability Reports Archive. For more information, see *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
- You can access Cisco Unified IM and Presence Reporting in the main navigation menu in Cisco Unified Communications IM and Presence Service.

Remote Serviceability Tools

Note The content in this section does not apply to Cisco Unity Connection.

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

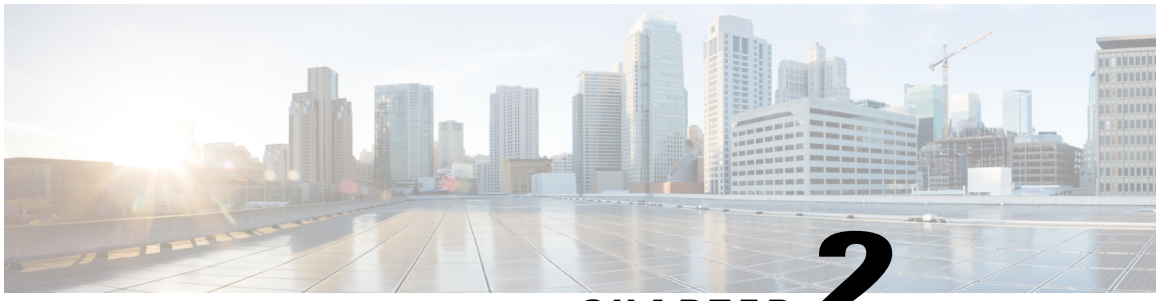
Unified Communications Manager supports the following capabilities for remote serviceability:

- Simple Network Management Protocol (SNMP) - Provides remote management for managed devices such as Unified Communications Manager.
- Show Command Line Interface - Displays Unified Communications Manager system data.

Customized Login Message

You can upload a text file that contains a customized login message that appears on the initial Serviceability window.

For more information and the procedure for uploading your customized login message, refer to the *Administration Guide for Cisco Unified Communications Manager* .



CHAPTER 2

Getting Started

- Access, page 5
- Install Server Certificate, page 7
- Serviceability Interface, page 9

Access

You can access the Serviceability application several ways:

- By entering `https://<server name or IP address>:8443/ccmservice/` in a browser window and then entering a valid username and password.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in the Cisco Unified Communications Manager Administration console.
- By choosing **Application** > **Serviceability Webpage** in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT) menu and then entering a valid username and password.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco Unity Connection.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco IM and Presence Administration..

Tip After you log in to Cisco Unified Serviceability, you can access all administrative applications that display in the Navigation menu, except for Cisco Unified OS Administration and Disaster Recovery System, without logging in again. The web pages that you can access within Cisco Unified Serviceability depend on your assigned roles and privileges. Cisco Unified OS Administration and Disaster Recovery System require a separate authentication procedure.

The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application.

Tip Cisco Unified Communications Manager only: Any user who has the "Standard CCM Admin Users" role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *Administration Guide for Cisco Unified Communications Manager* .

Tip Cisco Unity Connection only: Any user who has the System Administrator role or Technician role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

If you get a security alert that the site is not trusted, this indicates that the server certificate has not yet downloaded.

To access Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 In a supported browser, browse to the server where the Cisco Unified Serviceability service runs.

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

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

Note If the system prompts you about certificates, see topics related to installing the server certificate.

Step 2 Enter a valid username and password; click **Login**.
To clear the username and password, click **Reset**.

When you log in to Cisco Unified Serviceability, the last successful system login attempt and the last unsuccessful system login attempt for each user along with the user id, date, time and IP address is displayed in the main Cisco Unified Serviceability window.

Related Topics

Install Server Certificate, on page 7

Access Cisco Unified IM and Presence Serviceability

After you sign into Cisco Unified IM and Presence Serviceability, you can access all applications that display in the Navigation list box without having to sign in to each application. Select the application you require from the list box, and select **Go**.

Before You Begin

If you have already signed in to one of the applications that display in the Navigation list box (not Cisco Unified IM and Presence OS Administration or IM and Presence Disaster Recovery System), you can access Cisco Unified IM and Presence Serviceability without signing in. From the Navigation list box, select Cisco Unified IM and Presence Serviceability; then, select **Go**.

Procedure

Step 1 Enter `https://<server name or IP address>`, where the server name or IP address equals the server where the Cisco Unified IM and Presence Serviceability service runs.

Step 2 Sign in to Unified Communications Manager IM and Presence Administration.

Step 3 If the system prompts you about certificates, you must enable HTTPS to secure communications between the browser client and the web server.

Step 4 Enter the application user and application user password that you specified during installation when the system prompts you for a username and password.

Step 5 After Unified Communications Manager IM and Presence Administration displays, select **Navigation** > **Cisco Unified IM and Presence Serviceability** from the menu in the upper right corner of the main window.

When you log in to Cisco Unified IM and Presence Serviceability, the last successful system login attempt and the last unsuccessful system login attempt for each user along with the user id, date, time and IP address is displayed in the main Cisco Unified IM and Presence Serviceability window.

Install Server Certificate

Note For additional information about using HTTPS with Cisco Unified Communications Manager, refer to Cisco Unified Communications Manager Security Guide.

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

Note Ensure that the browser certificate and the server certificate are an exact match.

Note Because of the way Internet Explorer 7 handles certificates, this browser displays an error status after you import the server certificate. This status persists if you reenter the URL or refresh or relaunch the browser and does not indicate an error. Refer to the Install Internet Explorer 7 Certificate, on page 8 for more information.

HTTPS

When you first attempt to access Cisco Unified Serviceability, a Security Alert dialog box, which indicates that the server is not trusted because the server certificate does not exist in the Trusted folder, displays. When the dialog box displays, perform one of the following tasks:

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

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

Install Internet Explorer 7 Certificate

Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager or Cisco Unity Connection server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration or Cisco Unity Connection website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Java Runtime Environment (JRE) must be present to provide Java-related browser support for IE.

Be sure to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1 Browse to application on the Tomcat server by entering the hostname (server name) or IP address in the browser.
The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**
The administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.
The Certification Path tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

Step 5 Select the General tab in the Certificate window and click **Install Certificate**.
The Certificate Import wizard launches.

Step 6 To start the wizard, click **Next**.
The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.
A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.
The Import wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools** > **Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.
After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname or IP address or refresh or relaunch the browser.

Serviceability Interface

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

- Cisco Unified Communications Manager only: To access Dialed Number Analyzer to test and diagnose a deployed Unified Communications Manager dial plan configuration, analyze the test results and use the results to tune the dial plan, activate the Cisco Dialed Number Analyzer service by choosing **Tools** > **Service Activation** and choosing **Tools** > **Dialed Number Analyzer**.
- You must activate the Cisco Dialed Number Analyzer Server service needs along with the Cisco Dialed Number Analyzer service by choosing **Tools** > **Service Activation** and choosing **Tools** > **Dialed Number Analyzer Server**. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

  For more information on how to use the Dialed Number Analyzer, refer to the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.
- Unified Communications Manager only: To access Cisco Unified Communications Manager CDR Analysis and Reporting from **Tools** > **CDR Analysis and Reporting**, perform the required procedures, as described in the *CDR Analysis and Reporting Administration Guide*.

Note You cannot access the Cisco Unified Communications Manager CDR Analysis and Reporting tool unless you are a member of the Cisco CAR Administrators user group. Refer to the "Configuring the CDR Analysis and Reporting Tool" chapter in the *CDR Analysis and Reporting Administration Guide* for information on how to become a member of the Cisco CAR Administrators user group.

- To display documentation for a single window, choose **Help** > **This Page** in Cisco Unified Serviceability.
- To display a list of documents that are available with this release (or to access the online help index), choose **Help** > **Contents** in Cisco Unified Serviceability.
- To verify the version of Cisco Unified Serviceability that runs on the server, choose **Help** > **About** or click the **About** link in the upper right corner of the window.
- To go directly to the home page in Cisco Unified Serviceability from a configuration window, choose **Cisco Unified Serviceability** from the Navigation drop-down list box in the upper right corner of the window.

Note In some scenarios, you cannot access the Cisco Unified Serviceability from Cisco Unified OS Administration. A "Loading, please wait" message displays indefinitely. If the redirect fails, log out from Cisco Unified OS Administration, select Cisco Unified Serviceability from the Navigation drop-down list box, and log in to Cisco Unified Serviceability.

- To go directly to the home page in Cisco Unified IM and Presence Serviceability from a configuration window, select **Cisco Unified IM and Presence Serviceability** from the Navigation drop-down list box in the upper right corner of the window.
- To access other application GUIs, choose the application from the Navigation drop-down list box in the upper right corner of the window; then, click **Go**.
- To log out of Cisco Unified Serviceability, click the **Logout** link in the upper right corner of the Cisco Unified Serviceability window.
- In each Cisco Unified Serviceability configuration window, configuration icons display that correspond to the configuration buttons at the bottom of the window; for example, you can either click the Save icon or the Save button to complete the task.

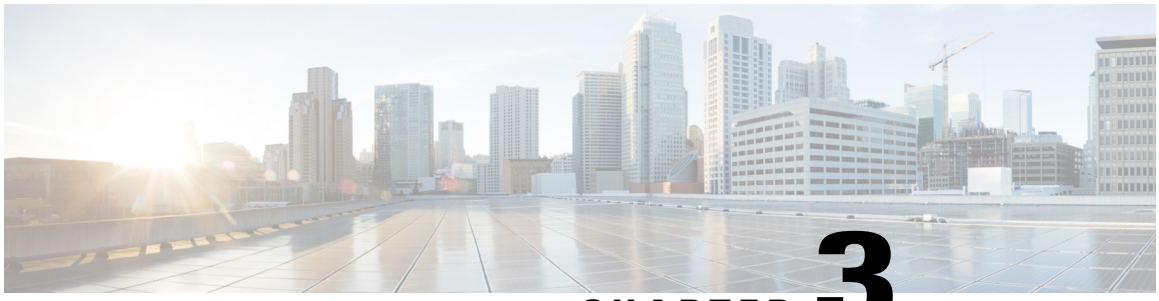
Tip Cisco Unified Serviceability does not support the buttons in your browser. Do not use the browser buttons, for example, the Back button, when you perform configuration tasks.

Tip When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before indicating that the session has timed out and redirecting you to the login window. After you log in again, you may have to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Cisco Unified Serviceability Icons

Table 1: Cisco Unified Serviceability Icons

Icon	Purpose
	Adds a new configuration
	Cancels the operation
	Clears the configuration that you specify
	Deletes the configuration that you select
	Shows the online help for the configuration
	Refreshes the window to display the latest configuration
	Restarts the service that you select
	Saves the information that you entered
	Sets the default for the configuration
	Starts the service that you select
	Stops the service that you select



CHAPTER 3

Alarms

- Overview, page 13
- Alarm Configuration, page 14
- Alarm Definitions, page 15
- Alarm Information, page 16
- Set Up Alarms, page 16
- Alarm Service Setup, page 17
- Alarm Definitions and User-Defined Description Additions, page 24

Overview

Cisco Unified Serviceability and Cisco Unified IM and Presence Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting and also applies to clusters.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from Debug to Emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDL trace log file (for Cisco CallManager and CTIManager services only), or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure and that are specified in the routing list in the alarm definition (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or write the alarm information to its final destination (such as a log file).

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

Note Cisco Unity Connection SNMP does not support traps.

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

You use the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool (Unifed RTMT) to collect alarms that get sent to an SDL trace log file (for Cisco CallManager and CTIManager services only). You use the SysLog Viewer in Unifed RTMT to view alarm information that gets sent to the local syslog.

Alarm Configuration

You can configure alarms for services, such as Cisco Database Layer Monitor, in Cisco Unified Serviceability. Then, you configure the location or locations, such as Syslog Viewer (local syslog), where you want the system to send the alarm information. With this option, you can do the following:

- Configure alarms for services on a particular server or on all servers (Unified Communications Manager clusters only)
- Configure different remote syslog servers for the configured services or servers
- Configure different alarm event level settings for different destinations

Cisco Syslog Agent enterprise parameters in Cisco Unified Communications Manager Administration allow you to forward all alarms that meet or exceed the configured threshold to a remote syslog server with these two settings: remote syslog server name and syslog severity. To access these Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Cisco Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

The alarms include system (OS/hardware platform), application (services), and security alarms.

Note If you configure both the Cisco Syslog Agent alarm enterprise parameters and application (service) alarms in Cisco Unified Serviceability, the system can send the same alarm to the remote syslog twice.

If local syslog is enabled for an application alarm, the system sends the alarm to the enterprise remote syslog server only when the alarm exceeds both the local syslog threshold and the enterprise threshold.

If remote syslog is also enabled in Cisco Unified Serviceability, the system forwards the alarm to the remote syslog server by using the application threshold that is configured in Cisco Unified Serviceability, which may result in the alarm being sent to the remote syslog server twice.

The event level/severity settings provide a filtering mechanism for the alarms and messages that the system collects. This setting helps to prevent the Syslog and trace files from becoming overloaded. The system forwards only alarms and messages that exceed the configured threshold.

For more information about the severity levels attached to alarms and events, see the Alarm Definitions, on page 15.

Alarm Definitions

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

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

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

- Unified Communications Manager only: SDL - The system sends the alarm information to the SDL trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- SDI - The system sends the alarm information to the SDI trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Sys Log - The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an event level in the Alarm Configuration window, and enter a server name or IP address for the remote syslog server.
- Event Log - The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT), if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Data Collector - The system sends the alarm information to the real-time information system (RIS data collector) for alert purposes only. You cannot configure this option in the Alarm Configuration window.
- SNMP Traps - System generates an SNMP trap. You cannot configure this option in the Alarm Configuration window.

Tip If the SNMP Traps location displays in the routing list, the system forwards the alarm information to the CCM MIB SNMP agent, which generates traps according to the definition in CISCO-CCM-MIB.

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

For each alarm definition, you can include an additional explanation or recommendation. All administrators have access to the added information. You directly enter information into the User Defined Text pane that

displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified Serviceability adds the information to the database.

Alarm Information

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

Set Up Alarms

Perform the following steps to configure alarms.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, Cisco Unity Connection Administrationor Cisco Unified IM and Presence Administration, configure the Cisco Syslog Agent enterprise parameters to send system, application (services), and security alarms/messages to a remote syslog server that you specify. Skip this step to configure application (services) alarms/messages in Cisco Unified Serviceability.

Step 2 In Cisco Unified Serviceability, configure the servers, services, destinations, and event levels for the applications (services) alarm information that you want to collect.

Step 3 (Optional) Add a definition to an alarm.

- All services can go to the SDI log (but must be configured in Trace also).
- All services can go to the SysLog Viewer.
- Cisco Unified Communications Manager only: Only the Cisco CallManager and Cisco CTIManager services use the SDL log.
- To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name. If you do not configure the remote server name, Cisco Unified Serviceability does not send the Syslog messages to the remote syslog server.

  Tip Do not configure a Cisco Unified Communications Manager server as a remote Syslog server.

Step 4 If you chose an SDL trace file as the alarm destination, collect traces and view the information with the Trace and Log Central option in Unified RTMT.

Step 5 If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in Unified RTMT.

Step 6 See the corresponding alarm definition for the description and recommended action.

Alarm Service Setup

Syslog Agent Enterprise Parameters

You can configure the Cisco Syslog Agent enterprise parameters to send system, application, and security alarms/messages that exceed the configured threshold to a remote syslog server that you specify. To access the Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Cisco Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

Next, configure the remote syslog server names (Remote Syslog Server Name 1, Remote Syslog Server Name 2, Remote Syslog Server Name 3, Remote Syslog Server Name 4, and Remote Syslog Server Name 5) and syslog severity. Ensure that you specify valid IP addresses while configuring the server names. The syslog severity is applicable to all the remote syslog servers that you configure. Then click **Save**. For the valid values to enter, click the **?** button. If no server name is specified, Cisco Unified Serviceability does not send the Syslog messages.

Caution While configuring remote syslog servers in Cisco Unified Communications Manager, do not add duplicate entries for remote syslog server names. If you add duplicate entries, the Cisco Syslog Agent will ignore the duplicate entries while sending messages to the remote syslog servers.

Note Do not configure a Cisco Unified Communications Manager as a remote syslog server. The Cisco Unified Communications Manager node does not accept Syslog messages from another server.

Set Up Alarm Service

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

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

Cisco Unity Connection also uses alarms, which are available in Cisco Unity Connection Serviceability. You cannot configure alarms in Cisco Unity Connection Serviceability. For details, see the *Cisco Unity Connection Serviceability Administration Guide*.

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

Procedure

Step 1 Choose **Alarm** > **Configuration**.
The Alarm Configuration window displays.

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

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

Tip For a list of services that correspond to the service groups, see Service groups.

Step 4 From the Service drop-down list, choose the service for which you want to configure the alarm; then, click **Go**.
Only services that support the service group and your configuration display.

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

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

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

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

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

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

What to Do Next

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

To access the alarm definitions for the Cisco Extension Mobility Application service, Cisco Unified Communications Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window described in Alarm definitions.

Set Up Alarm Services That Use Cisco Tomcat

The following services use Cisco Tomcat for alarm generation:

- Cisco Extension Mobility Application
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

The system login alarm AuthenticationFailed also uses Cisco Tomcat. To generate alarms for these services, perform the following procedure.

Procedure

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

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

Step 3 From the Services Group drop-down list, choose **Platform Services**; then, click **Go**.

Step 4 From the Services drop-down list, choose **Cisco Tomcat**; then, click **Go**.

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

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

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

Service Groups

The following table lists the services that correspond to the options in the Service Group drop-down list in the Alarm Configuration window.

Note Not all listed service groups and services apply to all system configurations.

Table 2: Service Groups in Alarm Configuration

Service Group	Services
CM Services	Cisco CTIManager, Cisco CallManager, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer Server, Cisco Extended Functions, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, and Cisco TFTP
CTI Services	Cisco IP Manager Assistant and Cisco WebDialer Web Service
CDR Services	Cisco CAR Scheduler, Cisco CDR Agent, and Cisco CDR Repository Manager

Service Group	Services
Database and Admin Services	Cisco Bulk Provisioning Service, Cisco Database Layer Monitor, and Cisco License Manager
Performance and Monitoring Services	Cisco AMC Service and Cisco RIS Data Collector
Directory Services	Cisco DirSync
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master
System Services	Cisco Trace Collection Service
Platform Services	Cisco Tomcat

Alarm Configuration Settings

The following table describes all alarm configuration settings, even though the service may not support the settings.

Table 3: Alarm Configuration Settings

Name	Description
Server	From the drop-down list, choose the server (node) for which you want to configure the alarm; then, click **Go**.
Service Group	Cisco Unity Connection supports only the following service groups: Database and Admin Services, Performance and Monitoring Services, Backup and Restore Services, System Services, and Platform Services. From the drop-down list, choose the category of services, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.
Service	From the Service drop-down list, choose the service for which you want to configure the alarm; then, click **Go**. Only services that support the service group and your configuration display. **Tip** The drop-down list displays both active and inactive services.

Name	Description
Cisco Unified Communications Manager and Cisco Cisco Unified Communications Manager IM and Presence Service only: Apply to All Nodes	To apply the alarm settings for the service to all nodes in a cluster, check the check box.
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
Enable Alarm for Remote Syslogs	The Syslog file serves as the alarm destination. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified Serviceability does not send the Syslog messages. The configured AMC primary and failover collectors use the remote syslog settings. The remote syslog settings used by the collectors are those configured on the respective individual nodes. If the remote syslog is only configured on AMC primary collector without configuring remote syslog on AMC failover collector and failover occurs in AMC primary collector, then no remote syslogs will be generated. You must configure exactly the same settings on all nodes, to send the remote syslog alarms to the same remote syslog server. When failover occurs in AMC controller or when the collector configuration changes to a different node, the remote syslog settings on a backup or newly configured node is used. To prevent too many alarms flooding the system, you can check the **Exclude End Point Alarms** check box. This ensures that the endpoint phone-related events get logged into a separate file. **Exclude End Point Alarms** check box is displayed only for the CallManager services, and is not checked by default. You need to check the **Apply to All Nodes** also, when you check this check box. The configuration options for endpoint alarms are listed in Alarm configuration settings. **Tip** Do not specify a Cisco Cisco Unified Communications Manager or a Cisco Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.

Name	Description
Remote Syslog Servers	In each of the Server Name 1, Server Name 2, Server Name 3, Server Name 4, and Server Name 5 fields, enter the name or IP address of the remote syslog server that you want to use to accept syslog messages. For example, if you want to send the alarms to Cisco Unified Operations Manager, specify the Cisco Unified Operations Manager as the server name. **Tip** Do not specify a Cisco Cisco Unified Communications Manager or a Cisco Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.
Enable Alarm for SDI Trace	The SDI trace library serves as the alarm destination. To log alarms, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see Set up trace parameters.
Cisco Unified Communications Manager and Cisco Unified Communications Manager BE only: Enable Alarm for SDL Trace	The SDL trace library serves as the alarm destination. This destination applies only to the Cisco CallManager service and the CTIManager service. Configure this alarm destination by using Trace SDL configuration. To log alarms in the SDL trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the Set up trace parameters.

Name	Description
Alarm Event Level	From the drop-down list, choose one of the following options: **Emergency** This level designates system as unusable. **Alert** This level indicates that immediate action is needed. **Critical** The system detects a critical condition. **Error** This level signifies that error condition exists. **Warning** This level indicates that a warning condition is detected. **Notice** This level designates a normal but significant condition. **Informational** This level designates information messages only. **Debug** This level designates detailed event information that Cisco Technical Assistance Center engineers use for debugging.

The following tables describe the default alarm configuration settings.

	Local Syslogs	Remote Syslogs	SDI Trace	SDL Trace
Enable Alarm	Checked	Unchecked	Checked	Checked
Alarm Event Level	Error	Disabled	Error	Error

Exclude End Point Alarms	Local Syslog	Alternate Syslog	Remote Syslog	Syslog Severity and Strangulate Alert	Syslog Traps
Checked	No	Yes	No	No	No
Unchecked	No	Yes	Yes	Yes	Yes

Alarm Definitions and User-Defined Description Additions

This section provides procedural information to search, view, and create user information for alarm definitions that display in the Serviceability interface.

View Alarm Definitions and Add User-Defined Descriptions

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

Tip Cisco Unified Communications Manager and Cisco Unity Connection only: You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability. You cannot add user-defined descriptions to alarm definitions in Cisco Unity Connection Serviceability.

Cisco Unity Connection also uses certain alarm definitions in Cisco Unified Serviceability, and they must be viewed in Cisco Unified Serviceability. Be aware that alarms that are associated with the catalogs in System catalogs are available for viewing.

Before You Begin

Review the description of alarm definition catalogs.

Procedure

Step 1 Select **Alarm** > **Definitions**.

Step 2 Perform one of the following actions:

- Select an alarm as follows:
  - Select an alarm catalog from the **Find alarms where** drop-down list, for example, a System Alarm catalog or IM and Presence alarm catalog.
  - Select the specific catalog name from the **Equals** drop-down list.
- Enter the alarm name in the **Enter Alarm Name** field.

Step 3 Select **Find**.

Step 4 Perform one of the following actions if multiple pages of alarm definitions exist:

- To select another page, select the appropriate navigation button at the bottom of the **Alarm Message Definitions** window.
- To change the number of alarms that display in the window, select a different value from the **Rows per Page** drop-down list.

Step 5 Select the alarm definition for which you want alarm details.

Step 6 Enter text in the **User Defined Text** field if you want to add information to the alarm, and then select **Save**.

Tip If you add text in the **User Defined Text** field, you can select **Clear All** at any time to delete the information that you entered.

Step 7 Select **Save**.

Step 8 Select **Back to Find/List Alarms** from the Related Links drop-down list if you want to return to the **Alarm Message Definitions** window.

Step 9 Select **Go**.

System Alarm Catalog Descriptions

The following table contains the System Alarm Catalog alarm descriptions. The System Alarm Catalog supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 4: System Catalogs

Name	Description
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishment of security associations between servers in a cluster.
DBAlarmCatalog	All Cisco database alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Java Applications alarm definitions. **Tip** Cisco License Manager, which supports Cisco Unified Communications Manager, uses this catalog. **Tip** You cannot configure JavaApplications alarms by using the alarm configuration GUI. For Cisco Unified Communications Manager and Cisco Unity Connection, you generally configure these alarms to go to the Event Logs; for Cisco Unified Communications Manager, you can configure these alarms to generate SNMP traps to integrate with CiscoWorks LAN Management Solution. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
EMAlarmCatalog	Alarms for Extension Mobility
LoginAlarmCatalog	All login-related alarm definitions
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters.

Name	Description
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services.
TFTPAlarmCatalog	All Cisco TFTP alarm definitions
TVSAlarmCatalog	Alarms for Trust Verification Service
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP traps from the command line interface (CLI). For information on the CLI, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*. **Tip** Cisco Unity Connection SNMP does not support traps in either Unified Communications Manager and Cisco Unity Connection systems.
CertMonitorAlarmCatalog	All certificate expiration definitions.
CTLproviderAlarmCatalog	Alarms for Certificate Trust List (CTL) Provider service
CDPAlarmCatalog	Alarms for Cisco Discovery Protocol (CDP) service
IMSAlarmCatalog	All user authentication and credential definitions.

CallManager Alarm Catalog Descriptions

The information in this section does not apply to Cisco Unity Connection.

The following table contains the CallManager Alarm Catalog descriptions.

Table 5: CallManager Alarm Catalog

Name	Description
CallManager	All Cisco CallManager service alarm definitions
CDRRepAlarmCatalog	All CDRRep alarm definitions
CARAlarmCatalog	All CDR analysis and reporting alarm definitions
CEFAlarmCatalog	All Cisco Extended Functions alarm definitions
CMIAlarmCatalog	All Cisco messaging interface alarm definitions
CtiManagerAlarmCatalog	All Cisco computer telephony integration (CTI) manager alarm definitions
IpVmsAlarmCatalog	All IP voice media streaming applications alarm definitions

Name	Description
TCDSRVAlarmCatalog	All Cisco telephony call dispatcher service alarm definitions
Phone	Alarms for phone-related tasks, such as downloads
CAPFAlarmCatalog	Alarms for Certificate Authority Proxy Function (CAPF) service
SAMLSSOAlarmCatalog	Alarms for SAML Single Sign On feature.

IM and Presence Alarm Catalog Descriptions

The following table contains the IM and Presence Service Alarm Catalog description.

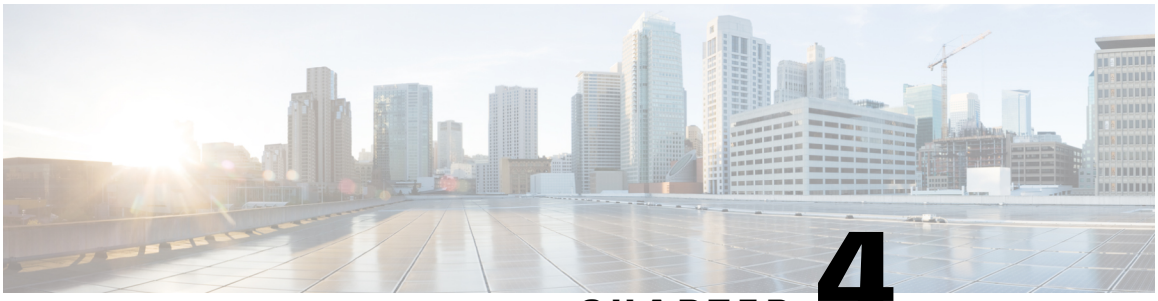
Table 6: IM and Presence Service Alarm Catalog

Name	Description
CiscoUPSConfigAgent	All Config Agent alarms that notify the IM and Presence Service SIP Proxy of configuration changes in the IM and Presence Service IDS database.
CiscoUPInterclusterSyncAgent	All Intercluster Sync Agent alarms that synchronize end user information between IM and Presence Service clusters for intercluster routing.
CiscoUPSPresenceEngine	All Presence Engine alarms that collect information regarding the availability status and communications capabilities of a user.
CiscoUPSSIPProxy	All SIP Proxy alarms that are related to routing, requestor identification, and transport interconnection.
CiscoUPSSOAP	All simple object access protocol (SOAP) alarms that provide a secure SOAP interface to and from external clients using HTTPS.
CiscoUPSSyncAgent	All Sync Agent alarms that keep the IM and Presence Service data synchronized with Cisco Unified Communications Manager data.
CiscoUPXCP	All XCP alarms that collect information on the status of XCP components and services on IM and Presence Service.
CiscoUPServerRecoveryManager	All server recovery manager alarms that relate to the failover and fallback process between nodes in a presence redundancy group.

Name	Description
CiscoUPReplWatcher	All ReplWatcher alarms that monitor IDS Replication State.
CiscoUPXCPConfigManager	All Cisco XCP Config Manager alarm definitions that relate to XCP components.

Alarm information, which includes an explanation and recommended action, also includes the application name, server name, and other information, to help you perform troubleshooting, even for problems that are not on your local IM and Presence Service node.

For more information about the alarms that are specific to the IM and Presence Service, see *System Error Messages for IM and Presence on Cisco Unified Communications Manager*.



CHAPTER 4

Trace

- Trace, page 29
- Configure Trace, page 32

Trace

Cisco Unified Serviceability provides trace tools to assist you in troubleshooting issues with your voice application. Cisco Unified Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace (for Cisco CallManager and Cisco CTIManager services, applicable to Cisco Unified Communications Manager only), and Log4J trace (for Java applications).

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

Cisco Unified Communications Manager only: If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateway.

Cisco Unified Communications Manager only: In the Alarm Configuration window, you can direct alarms to various locations, including SDL trace log files. If you want to do so, you can configure trace for alerts in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Cisco Unified IM and Presence Serviceability provides trace tools to assist you in troubleshooting issues with your instant messaging and presence application. Cisco Unified IM and Presence Serviceability supports:

- SDI trace
- Log4J trace (for Java applications)

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

In the **Alarm Configuration** window, you can direct alarms to various locations. If you want to do so, you can configure trace for alerts in the IM and Presence Unified RTMT.

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace and Log Central option in the Unified RTMT. You can configure trace parameters for any feature or network service that is available on any IM and Presence node in the cluster. Use the **Trace Configuration** window to specify the parameters that you want to trace for troubleshooting problems. If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the **Troubleshooting Trace Setting** window.

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

Trace Configuration

You can configure trace parameters for any feature or network service that displays in the Serviceability interface. If you have clusters, you can configure trace parameters for any feature or network service that is available on any server in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting problems.

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

If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace window. For more information on troubleshooting trace, see Trace settings.

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in Unified RTMT. For more information regarding trace collection, see Trace collection.

Trace Settings

The Troubleshooting Trace Settings window allows you to choose the services for which you want to set predetermined troubleshooting trace settings. In this window, you can choose a single service or multiple services and change the trace settings for those services to the predetermined trace settings. If you have clusters, you can choose the services on different servers in the cluster, so the trace settings of the chosen services get changed to the predetermined trace settings. You can choose specific activated services for a single server, all activated services for the server, specific activated services for all servers in the cluster, or all activated services for all servers in the cluster. In the window, N/A displays next to inactive services.

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

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

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for that service. From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings, for example, Maximum No. of Files. You can modify these parameters even after you apply troubleshooting trace settings.

Trace Collection

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

Tip Do not use Windows NotePad to view collected trace files to view collected trace files, because Windows NotePad does not properly display line breaks.

Note Cisco Unified Communications Manager only: For devices that support encryption, the Secure Real-time Transport Protocol (SRTP) keying material does not display in the trace file.

For more information about trace collection, see *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Called Party Tracing

Called Party Tracing allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls using the Session Trace Tool.

For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Set Up Trace Configuration

The following procedure provides an overview of the steps to configure and collect trace for feature and network services in the Serviceability interface.

Procedure

Step 1 Configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service) by performing one of these steps:

- Cisco Unified Communications Manager Administration and Cisco Unified IM and Presense: Select **System** > **ServiceParameters** and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

- Cisco Unity Connection only: Select **System Settings** > **Service Parameters**in Cisco Unity Connection Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

Step 2 Configure the trace setting for the service for which you want to collect traces. If you have clusters, you can configure trace for the service on one server or on all servers in the cluster.
To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields.

If you want to run predetermined traces on services, set troubleshooting trace for those services.

Step 3 Install the Cisco Unified Real-Time Monitoring Tool on a local PC.

Step 4 If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in Unified RTMT.
You can find the LogFileSearchStringFound alarm in the LpmTctCatalog. (Select**Alarms** > **Definitions**. In the Find alarms where drop-down list box, choose the **System Alarm Catalog**; in the Equals drop-down list box, choose **LpmTctCatalog**).

Step 5 If you want to automatically capture traces for alerts such as CriticalServiceDownand CodeYellow, check the **Enable Trace Download** check box in the Set Alert/Properties dialog box for the specific alert in Unified RTMT; configure how often that you want the download to occur.

Step 6 Collect the traces.

Step 7 View the log file in the appropriate viewer.

Step 8 If you enabled troubleshooting trace, reset the trace settings services, so the original settings are restored.

Note Leaving troubleshooting trace enabled for a long time increases the size of the trace files and may affect the performance of the services.

Configure Trace

This section provides information for configuring trace settings.

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

Set Up Trace Parameters

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

Tip For Cisco Unity Connection, you may need to run trace in Cisco Unified Serviceability and Cisco Unity Connection Serviceability to troubleshoot Cisco Unity Connection issues. For information on how to run trace in Cisco Unity Connection Serviceability, refer to the *Cisco Unity Connection Serviceability Administration Guide* .

Procedure

Step 1 Select **Trace** > **Configuration**.
The Trace Configuration window displays.

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

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

Tip The Service Groups in Trace Configuration table lists the services and trace libraries that correspond to the options that display in the Service Group drop-down list box.

Step 4 From the Service drop-down list box, select the service for which you want to configure trace and, click **Go**. The drop-down list box displays active and inactive services.

Tip Cisco Unity Connection only: For the Cisco CallManager and CTIManager services, you can configure SDL trace parameters. To do so, open the Trace Configuration window for one of those services, and click the **Go** button that is next to the Related Links drop-down list box.

If you configured Troubleshooting Trace for the service, a message displays at the top of the window that indicates that the Troubleshooting Traces feature is set, which means that the system disables all fields in the Trace Configuration window except for Trace Output Settings. To configure the Trace Output Settings, go to Step 11. To reset Troubleshooting Trace, see the Set up troubleshooting trace settings.

The trace parameters display for the service that you chose. In addition, the Apply to All Nodes check box displays (Cisco Unified Communications Manager only).

Step 5 Unified Communications Manager and IM and Presence only: If you want to do so, you can apply the trace settings for the service or trace library to all servers in the cluster by checking the **Apply to All Nodes** check box; that is, if your configuration supports clusters.

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

Step 7 Cisco Unity Connection only: If you are configuring SDL trace parameters, go to Step 10.

Step 8 Select the level of information that you want traced from the **Debug Trace Level** list box, as described in Debug trace level settings.

Step 9 Check the **Trace Fields** check box for the service that you chose, for example, Cisco Log Partition Monitoring Tool Trace Fields.

Step 10 If the service does not have multiple trace settings where you can specify the traces that you want to activate, check the **Enable All Trace** check box. If the service that you chose has multiple trace settings, check the check boxes next to the trace check boxes that you want to enable, as described in Trace field descriptions.

Step 11 To limit the number and size of the trace files, specify the trace output setting. See Trace Ouput Settings for descriptions.

Step 12 To save your trace parameters configuration, click the **Save** button.
The changes to trace configuration take effect immediately for all services except Cisco Messaging Interface (Cisco Unified Communications Manager only). The trace configuration changes for Cisco Messaging Interface take effect in 3 to 5 minutes.

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

Service Groups in Trace Configuration

The following table lists the services and trace libraries that correspond to the options in the Service Group drop-down list box in the Trace Configuration window.

Table 7: Service Groups in Trace Configuration

Service Group	Services and Trace Libraries	Notes
Cisco Cisco Unified Communications Manager CM Services	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP Phone Service • Cisco DHCP Monitor Service • Cisco Dialed Number Analyzer • Cisco Dialed Number Analyzer Server • Cisco Extended Functions, Cisco Extension Mobility • Cisco Extension Mobility Application • Cisco IP Voice Media Streaming App • Cisco Messaging Interface • Cisco TFTP • Cisco Unified Mobile Voice Access Service	For most services in the CM Services group, you run trace for specific components, instead of enabling all trace for the service. The Trace field descriptions lists the services for which you can run trace for specific components.
Cisco Cisco Unified Communications Manager CTI Services	• Cisco IP Manager Assistant • Cisco Web Dialer Web Service	For these services, you can run trace for specific components, instead of enabling all trace for the service; see the Trace field descriptions.

Service Group	Services and Trace Libraries	Notes
Cisco Cisco Unified Communications Manager CDR Services	• Cisco Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler • Cisco Cisco Unified Communications Manager CDR Analysis and Reporting Web Service • Cisco CDR Agent • Cisco CDR Repository Manager	You enable all trace for each service, instead of running trace for specific components. In Cisco Cisco Unified Communications Manager CDR Analysis and Reporting, when reports are run that call stored procedures, Cisco Unified Communications Manager CDR Analysis and Reporting checks the configured debug trace level for the Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler service and the Cisco Unified Communications Manager CDR Analysis and Reporting Web Service in the Trace Configuration window before stored procedure logging begins. For pregenerated reports, Cisco Unified Communications Manager CDR Analysis and Reporting checks the level for the Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler service; for on-demand reports, Cisco Unified Communications Manager CDR Analysis and Reporting checks the level for the Cisco Cisco Unified Communications Manager CDR Analysis and Reporting Web Service. If you choose Debug from the Debug Trace Level drop-down list box, stored procedure logging gets enabled and continues until you choose another option from the drop-down list box. The following Cisco Unified Communications Manager CDR Analysis and Reporting reports use stored procedure logging: Gateway Utilization report, Route and Line Group Utilization report, Route/Hunt List Utilization report, Route Pattern/Hunt Pilot Utilization report, Conference Call Details report, Conference Call Summary report, Conference Bridge Utilization report, Voice Messaging Utilization report, and the CDR Search report.

Service Group	Services and Trace Libraries	Notes
IM and Presence Services	• Cisco Client Profile Agent • Cisco Config Agent • Cisco Intercluster Sync Agent • Cisco Login Datastore • Cisco OAM Agent • Cisco Presence Datastore • Cisco Presence Engine • Cisco IM and Presence Data Monitor • Cisco Route Datastore • Cisco SIP Proxy • Cisco SIP Registration Datastore • Cisco Server Recovery Manager • Cisco Sync Agent • Cisco XCP Authentication Service • Cisco XCP Config Manager • Cisco XCP Connection Manager • Cisco XCP Directory Service • Cisco XCP Message Archiver • Cisco XCP Router • Cisco XCP SIP Federation Connection Manager • Cisco XCP Text Conference Manager • Cisco XCP Web Connection Manager • Cisco XCP XMPP Federation Connection Manager	See topics related to feature and network services in Cisco Unified IM and Presence Serviceability for a description of these services. • For these services, you should enable all trace for the service, instead of running trace for specific components.

Service Group	Services and Trace Libraries	Notes
Database and Admin Services	Cisco Cisco Unified Communications Manager and Cisco Unity Connection: • Cisco AXL Web Service • Cisco CCM DBL Web Library • Cisco CCMAdmin Web Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco UXL Web Service Cisco Cisco Unified Communications Manager • Cisco Bulk Provisioning Service • Cisco GRT Communications Web Service • Cisco Role-based Security • Cisco TAPS Service • Cisco Unified Reporting Web Service IM and Presence Services: • Cisco AXL Web Service • Cisco Bulk Provisioning Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco GRT Communications Web Service • Cisco IM and Presence Admin • Cisco Unified Reporting Web Service • Platform Administrative Web Service	Choosing the Cisco CCM DBL Web Library option activates the trace for database access for Java applications. For database access for C++ applications, activate trace for Cisco Database Layer Monitor, as described in the Cisco Extended Functions trace fields. Choosing the Cisco Role-based Security option, which supports Cisco Cisco Unified Communications Manager, activates trace for user-role authorization. For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components. **Note** You can control logging for services in the Cisco Unified IM and Presence Serviceability UI. To change the log level, select the System Services group and Cisco CCMService Web Service.

Service Group	Services and Trace Libraries	Notes
Performance and Monitoring Services	Cisco Cisco Unified Communications Manager and Cisco Unity Connection: • Cisco AMC Service • Cisco CCM NCS Web Library • CCM PD Web Service • Cisco CallManager SNMP Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco Audit Event Service • Cisco RisBean Library Cisco Cisco Unified Communications Manager: • Cisco CCM PD Web Service IM and Presence Services: • Cisco AMC Service • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library	Choosing the Cisco CCM NCS Web Library option activates trace for database change notification for the Java client. Choosing the Cisco Unity RTMT Web Service option activates trace for the Unity RTMT servlets; running this trace creates the server-side log for Unity RTMT client queries.
Cisco Cisco Unified Communications Manager Security Services	• Cisco CTL Provider • Cisco Certificate Authority Proxy Function • Cisco Trust Verification Service	You enable all trace for each service, instead of running trace for specific components.

Service Group	Services and Trace Libraries	Notes
Cisco Cisco Unified Communications Manager Directory Services	Cisco DirSync	You enable all trace for this service, instead of running trace for specific components.
Backup and Restore Services	• Cisco DRF Local • Cisco Cisco Unified Communications Manager and Cisco Unity Connection only: Cisco DRF Master	You enable all trace for each service, instead of running trace for specific components.
System Services	Cisco Cisco Unified Communications Manager: • Cisco CCMRealm Web Service • Cisco CCMService Web Service • Cisco Common User Interface • Cisco Trace Collection Service IM and Presence Services: • Cisco CCMService Web Service • Cisco Trace Collection Service	Choosing the Cisco CCMRealm Web Service option activates trace for login authentication. Choosing the Cisco Common User Interface option activates trace for the common code that multiple applications use; for example, Cisco Unified Operating System Administration and Cisco Unified Serviceability. Choosing the Cisco CCMService Web Service option activates trace for the Cisco Unified Serviceability web application (GUI). You enable all trace for each option/service, instead of running trace for specific components.
SOAP Services	• Cisco SOAP Web Service • Cisco SOAPMessage Service	Choosing the Cisco SOAP Web Service option activates the trace for the AXL Serviceability API. You enable all trace for this service, instead of running trace for specific components.
Platform Services	Cisco Unified OS Admin Web Service	The Cisco Unified OS Admin Web Service supports Cisco Unified Operating System Administration, which is the web application that provides management of platform-related functionality such as certificate management, version settings, and installations and upgrades. You enable all trace for this service, instead of running trace for specific components.

Debug Trace Level Settings

The following table describes the debug trace level settings for services.

Table 8: Debug Trace Levels for Services

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

The following table describes the debug trace level settings for servlets.

Table 9: Debug Trace Levels for Servlets

Level	Description
Fatal	Traces very severe error events that may cause the application to abort.
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path.
Warn	Traces potentially harmful situations.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.

Level	Description
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. Trace level that turns on all logging.

Trace Field Descriptions

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

The following services are applicable to Cisco Unified Communications Manager and Cisco Unity Connection:

- Database layer monitor trace fields
- Cisco RIS data collector trace fields

The following services are applicable to Cisco Unified Communications Manager:

- Cisco CallManager SDI trace fields
- Cisco CallManager SDL trace fields
- Cisco CTIManager SDL trace fields
- Cisco Extended Functions trace fields
- Cisco Extension Mobility trace fields
- Cisco IP manager assistant trace fields
- Cisco IP voice media streaming app trace fields
- Cisco TFTP trace fields
- Cisco Web Dialer web service trace fields

Database Layer Monitor Trace Fields

The following table describes the Cisco Database Layer Monitor trace fields. The Cisco Database Layer Monitor service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 10: Cisco Database Layer Monitor Trace Fields

Field Name	Description
Enable DB Library Trace	Activates database library trace for C++ applications.
Enable Service Trace	Activates service trace.

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

Cisco RIS Data Collector Trace Fields

The following table describes the Cisco RIS Data Collector trace fields. The Cisco RIS Data Collector service supports Cisco Unified Communications Manager and Cisco Unity Connection.

Table 11: Cisco RIS Data Collector Trace Fields

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

Cisco CallManager SDI Trace Fields

The following table describes the Cisco CallManager SDI trace fields. The Cisco CallManager service supports Cisco Unified Communications Manager.

Table 12: Cisco CallManager SDI Trace Fields

Field Name	Description
Enable H245 Message Trace	Activates trace of H245 messages.
Enable DT-24+/DE-30+ Trace	Activates the logging of ISDN type of DT-24+/DE-30+ device traces.
Enable PRI Trace	Activates trace of primary rate interface (PRI) devices.
Enable ISDN Translation Trace	Activates ISDN message traces. Used for normal debugging.
Enable H225 & Gatekeeper Trace	Activates trace of H.225 devices. Used for normal debugging.
Enable Miscellaneous Trace	Activates trace of miscellaneous devices. **Note** Do not check this check box during normal system operation.
Enable Conference Bridge Trace	Activates trace of conference bridges. Used for normal debugging.
Enable Music on Hold Trace	Activates trace of music on hold (MOH) devices. Used to trace MOH device status such as registered with Cisco Unified Communications Manager, unregistered with Cisco Unified Communications Manager, and resource allocation processed successfully or failed.
Enable Unified CM Real-Time Information Server Trace	Activates Cisco Unified Communications Manager real-time information traces that the real-time information server uses.
Enable SIP Stack Trace	Activates trace of SIP stack. The default is enabled.
Enable Annunciator Trace	Activates trace for the annunciator, a SCCP device that uses the Cisco IP Voice Media Streaming Application service to enable Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices.

Field Name	Description
Enable CDR Trace	Activates traces for CDR.
Enable Analog Trunk Trace	Activates trace of all analog trunk (AT) gateways.
Enable All Phone Device Trace	Activates trace of phone devices. Trace information includes SoftPhone devices. Used for normal debugging.
Enable MTP Trace	Activates trace of media termination point (MTP) devices. Used for normal debugging.
Enable All Gateway Trace	Activates trace of all analog and digital gateways.
Enable Forward and Miscellaneous Trace	Activates trace for call forwarding and all subsystems that are not covered by another check box. Used for normal debugging.
Enable MGCP Trace	Activates trace for media gateway control protocol (MGCP) devices. Used for normal debugging.
Enable Media Resource Manager Trace	Activates trace for media resource manager (MRM) activities.
Enable SIP Call Processing Trace	Activates trace for SIP call processing.
Enable SCCP Keep Alive Trace	Activates trace for SCCP keepalive trace information in the Cisco CallManager traces. Because each SCCP device reports keepalive messages every 30 seconds, and each keepalive message creates 3 lines of trace data, the system generates a large amount of trace data when this check box is checked.
Enable SIP Keep Alive (REGISTER Refresh) Trace	Activates trace for SIP keepalive (REGISTER refresh) trace information in the Cisco CallManager traces. Because each SIP device reports keepalive messages every 2 minutes, and each keepalive message can create multiple lines of trace data, the system generates a large amount of trace data when this check box is checked.

Cisco CallManager SDL Trace Fields

The following table describes the Cisco CallManager SDL trace filter settings. The Cisco CallManager service supports Cisco Unified Communications Manager.

Note Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Table 13: Cisco CallManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable all Layer 1 traces.	Activates traces for Layer 1.
Enable detailed Layer 1 traces.	Activates detailed Layer 1 traces.
Enable all Layer 2 traces.	Activates traces for Layer 2.
Enable Layer 2 interface trace.	Activates Layer 2 interface traces.
Enable Layer 2 TCP trace.	Activates Layer 2 Transmission Control Program (TCP) traces.
Enable detailed dump Layer 2 trace.	Activates detailed traces for dump Layer 2.
Enable all Layer 3 traces.	Activates traces for Layer 3.
Enable all call control traces.	Activates traces for call control.
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.
Enable message translation signals trace.	Activates traces for message translation signals.
Enable UUIE output trace.	Activates traces for user-to-user informational element (UUIE) output.
Enable gateway signals trace.	Activates traces for gateway signals.
Enable CTI trace.	Activates CTI trace.
Enable network service data trace	Activates network service data trace.
Enable network service event trace	Activates network service event trace.
Enable ICCP admin trace	Activates ICCP administration trace.
Enable default trace	Activates default trace.

The following table describes the Cisco CallManager SDL configuration characteristics.

Table 14: Cisco CallManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for intracluster communication protocol (ICCP) link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP event trace.	Activates SDL TCP event trace.

Cisco CTIManager SDL Trace Fields

The following table describes the Cisco CTIManager SDL configuration trace filter settings. The Cisco CTIManager service supports Cisco Unified Communications Manager.

Tip Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Tip When you choose the CTIManager service from the Service Groups drop-down list box, the Trace Configuration window displays for SDI traces for this service. To activate SDI trace for the Cisco CTI Manager service, check the **Enable All Trace** check box in the Trace Configuration window for the Cisco CTIManager service. To access the SDL Configuration window, choose **SDL Configuration** from the Related Links drop-down list box; the settings that are described in Cisco CTIManager SDL Configuration Trace Filter Settings table and Cisco CTIManager SDL Configuration Trace Characteristics table display.

Table 15: Cisco CTIManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.

Setting Name	Description
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.
Enable CTI trace.	Activates CTI trace.
Enable Network Service Data Trace	Activates network service data trace.
Enable Network Service Event Trace	Activates network service event trace.
Enable ICCP Admin Trace	Activates ICCP administration trace.
Enable Default Trace	Activates default trace.

The following table describes the Cisco CTIManager SDL configuration trace characteristics.

Table 16: Cisco CTIManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for ICCP link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP Event trace	Activates SDL TCP event trace.

Cisco Extended Functions Trace Fields

The following table describes the Cisco Extended Functions trace fields. The Cisco Extended Functions service supports Cisco Unified Communications Manager.

Table 17: Cisco Extended Functions Trace Fields

Field Name	Description
Enable QBE Helper TSP Trace	Activates telephony service provider trace.
Enable QBE Helper TSPI Trace	Activates QBE helper TSP interface trace.
Enable QRT Dictionary Trace	Activates quality report tool service dictionary trace.
Enable DOM Helper Traces	Activates DOM helper trace.
Enable Redundancy and Change Notification Trace	Activates database change notification trace.
Enable QRT Report Handler Trace	Activates quality report tool report handler trace.
Enable QBE Helper CTI Trace	Activates QBE helper CTI trace.
Enable QRT Service Trace	Activates quality report tool service related trace.
Enable QRT DB Traces	Activates QRT DB access trace.
Enable Template Map Traces	Activates standard template map and multimap trace.
Enable QRT Event Handler Trace	Activates quality report tool event handler trace.
Enable QRT Real-Time Information Server Trace	Activates quality report tool real-time information server trace.

Cisco Extension Mobility Trace Fields

The following table describes the Cisco Extension Mobility trace fields. The Cisco Extension Mobility service supports Cisco Unified Communications Manager.

Table 18: Cisco Extension Mobility Trace Fields

Field Name	Description
Enable EM Service Trace	Activates trace for the extension mobility service.

Tip When you activate trace for the Cisco Extension Mobility Application service, you check the Enable All Trace check box in the Trace Configuration window for the Cisco Extension Mobility Application service.

Cisco IP Manager Assistant Trace Fields

The following table describes the Cisco IP Manager Assistant trace fields. The Cisco IP Manager Assistant service supports Cisco Unified Communications Manager Assistant.

Table 19: Cisco IP Manager Assistant Trace Fields

Field Name	Description
Enable IPMA Service Trace	Activates trace for the Cisco IP Manager Assistant service.
Enable IPMA Manager Configuration Change Log	Activates trace for the changes that you make to the manager and assistant configurations.
Enable IPMA CTI Trace	Activates trace for the CTI Manager connection.
Enable IPMA CTI Security Trace	Activates trace for the secure connection to CTIManager.

Cisco IP Voice Media Streaming App Trace Fields

The information in this section does not apply to Cisco Unity Connection.

The following table describes the Cisco IP Voice Media Streaming App trace fields. The Cisco IP Voice Media Streaming App service supports Cisco Unified Communications Manager.

Table 20: Cisco IP Voice Media Streaming Application Trace Fields

Field Name	Description
Enable Service Initialization Trace	Activates trace for initialization information.
Enable MTP Device Trace	Activates traces to monitor the processed messages for media termination point (MTP).
Enable Device Recovery Trace	Activates traces for device-recovery-related information for MTP, conference bridge, and MOH.
Enable Skinny Station Messages Trace	Activates traces for skinny station protocol.
Enable WinSock Level 2 Trace	Activates trace for high-level, detailed WinSock-related information.
Enable Music On Hold Manager Trace	Activates trace to monitor MOH audio source manager.
Enable Annunciator Trace	Activates trace to monitor annunciator.

Field Name	Description
Enable DB Setup Manager Trace	Activates trace to monitor database setup and changes for MTP, conference bridge, and MOH.
Enable Conference Bridge Device Trace	Activates traces to monitor the processed messages for conference bridge.
Enable Device Driver Trace	Activates device driver traces.
Enable WinSock Level 1 Trace	Activates trace for low-level, general, WinSock-related information.
Enable Music on Hold Device Trace	Activates traces to monitor the processed messages for MOH.
Enable TFTP Downloads Trace	Activates trace to monitor the download of MOH audio source files.

Cisco TFTP Trace Fields

The following table describes the Cisco TFTP trace fields. The Cisco TFTP service supports Cisco Unified Communications Manager.

Table 21: Cisco TFTP Trace Fields

Field Name	Description
Enable Service System Trace	Activates trace for service system.
Enable Build File Trace	Activates trace for build files.
Enable Serve File Trace	Activates trace for serve files.

Cisco Web Dialer Web Service Trace Fields

The following table describes the Cisco Web Dialer Web Service trace fields. The Cisco Web Dialer Web Service supports Cisco Unified Communications Manager.

Table 22: Cisco Web Dialer Web Service Trace Fields

Field Name	Description
Enable Web Dialer Servlet Trace	Activates trace for Cisco Web Dialer servlet.
Enable Redirector Servlet Trace	Activates trace for the Redirector servlet.

IM and Presence SIP Proxy Service Trace Filter Settings

The following table below describes the service trace filter settings for the IM and Presence SIP Proxy.

Table 23: IM and Presence SIP Proxy Service Trace Filter Settings

Parameter	Description
Enable Access Log Trace	This parameter enables the proxy access log trace; the first line of each SIP message received by the proxy is logged.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.
Enable Number Expansion Trace	This parameter enables tracing for the Number Expansion module.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable Server Trace	This parameter enables tracing for the Server.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.

Parameter	Description
Enable SIP XMPP IM Gateway Trace	This parameter enables trace for the SIP XMPP IM Gateway.
Enable Presence Web Service Trace	This parameter enables tracing for the Presence Web Service.

IM and Presence Trace Field Descriptions

The following tables provide field descriptions for the services that support trace activation of specific components. For some services, you can activate trace for specific component instead of enabling all trace for the service. If a service is not included in this chapter, Enable All Trace displays for the service in the Trace Configuration window.

Cisco Access Log Trace Fields

The following table describes the Cisco Access Log trace fields.

Table 24: Access Log Trace Fields

Field Name	Description
Enable Access Log Trace	Turns on Access Log trace.

Cisco Authentication Trace Fields

The following table describes the Cisco Authentication trace fields.

Table 25: Authentication Trace Fields

Field Name	Description
Enable Authentication Trace	Turns on authentication trace.

Cisco Calendar Trace Fields

The following table describes the Cisco Calendar trace fields.

Table 26: Calendar Trace Fields

Field Name	Description
Enable Calendar Trace	Turns on Calendar trace.

Cisco CTI Gateway Trace Fields

The following table describes the Cisco CTI Gateway trace fields.

Table 27: CTI Gateway Trace Fields

Field Name	Description
Enable CTI Gateway Trace	Turns on CTI Gateway trace.

Cisco Database Layer Monitor Trace Fields

The following table describes the Cisco Database Layer Monitor trace fields.

Table 28: Cisco Database Layer Monitor Trace Fields

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

Cisco Enum Trace Fields

The following table describes the Cisco Enum trace fields.

Table 29: Enum Trace Fields

Field Name	Description
Enable Enum Trace	Turns on Enum trace.

Cisco Method/Event Trace Fields

The following table describes the Cisco Method/Event trace fields.

Table 30: Method/Event Trace Fields

Field Name	Description
Enable Method/Event Trace	Turns on Method/Event trace.

Cisco Number Expansion Trace Fields

The following table describes the Cisco Number Expansion trace fields.

Table 31: Number Expansion Trace Fields

Field Name	Description
Enable Number Expansion Trace	Activates number expansion trace.

Cisco Parser Trace Fields

The following table describes the Cisco Parser trace fields.

Table 32: Parser Trace Fields

Field Name	Description
Enable Parser Trace	Activates parser trace.

Cisco Privacy Trace Fields

The following table describes the Cisco Privacy trace fields.

Table 33: PrivacyTrace Fields

Field Name	Description
Enable Privacy Trace	Activates Privacy trace.

Cisco Proxy Trace Fields

The following table describes the Cisco proxy trace fields.

Table 34: Proxy Trace Fields

Field Name	Description
Add Proxy	Turns on Proxy trace.

Cisco RIS Data Collector Trace Fields

The following table describes the Cisco RIS Data Collector trace fields.

Table 35: Cisco RIS Data Collector Trace Fields

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

Cisco Registry Trace Fields

The following table describes the Cisco Registry trace fields.

Table 36: Registry Trace Fields

Field Name	Description
Enable Registry Trace	Activates Registry trace.

Cisco Routing Trace Fields

The following table describes the Cisco Routing trace fields.

Table 37: Routing Trace Fields

Field Name	Description
Enable Routing Trace	Activates Routing trace.

Cisco Server Trace Fields

The following table describes the Cisco Server trace fields.

Table 38: Server Trace Fields

Field Name	Description
Enable Server Trace	Activates Server trace.

Cisco SIP Message and State Machine Trace Fields

The following table describes the Cisco SIP Message and State Machine trace fields.

Table 39: SIP Message and State Machine Trace Fields

Field Name	Description
Enable SIP Message and State Machine Trace	Activates SIP Message and State Machine trace.

Cisco SIP TCP Trace Fields

The following table describes the Cisco SIP TCP trace fields.

Table 40: SIP TCP Trace Fields

Field Name	Description
Enable SIP TCP Trace	Activates SIP TCP trace.

Cisco SIP TLS Trace Fields

The following table describes the Cisco SIP TLS trace fields.

Table 41: SIP TLS Trace Fields

Field Name	Description
Enable SIP TLS Trace	Activates SIP TLS trace.

Cisco Web Service Trace Fields

The following table describes the Cisco Web Service trace fields.

Table 42: Web Service Trace Fields

Field Name	Description
Enable Presence Web Service Trace	Activates Presence Web Service trace.

Trace Output Settings

The following table contains the trace log file descriptions.

Caution When you change either the Maximum No. of Files or the Maximum File Size settings in the Trace Configuration window, the system deletes all service log files except for the current file, that is, if the service is running; if the service has not been activated, the system deletes the files immediately after you activate the service. Before you change the Maximum No. of Files setting or the Maximum File Size setting, download and save the service log files to another server if you want to keep a record of the log files; to perform this task, use Trace and Log Central in Unity RTMT.

Table 43: Trace Output Settings

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

Trace Setting Troubleshooting

Troubleshoot Trace Settings Window

The **Troubleshooting Trace Settings** window allows you to select the services in the Serviceability GUI for which you want to set predetermined troubleshooting trace settings. In this window, you can select the services on different nodes in the cluster. This populates the trace settings changes for all the services you choose. You can select specific active services for a single node, all active services for the node, specific active services for all nodes in the cluster, or all active services for all nodes in the cluster. In the window, N/A displays next to inactive services.

Note For IM and Presence the predetermined troubleshooting trace settings for an IM and Presence feature or network service include SDI and Log4j trace settings. Before the troubleshooting trace settings are applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings are restored.

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

After you apply Troubleshooting Trace Setting to a service, the **Trace Configuration** window displays a message that troubleshooting trace is set for that service. From the **Related Links** list box, you can select the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the **Trace Configuration** window displays all the settings as read-only, except for some parameters of trace output settings, for example, Maximum No. of Files.

Troubleshoot Trace Settings

Before You Begin

Review the tasks Set up trace configuration and Set up trace parameters.

Procedure

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

Step 2 Select the server where you want to troubleshoot trace settings from the **Server** list box.

Step 3 Select **Go**.
A list of services display. The services that are not active display as N/A.

Step 4 Perform one of the following actions:

a) To monitor specific services on the node that you selected from the **Server** list box, check the service in the **Services** pane.
For example, the Database and Admin Services, Performance and Monitoring Services, or the Backup and Restore Services pane (and so on).

This task affects only the node that you selected from the **Server** list box.

b) To monitor all services on the node that you selected from the **Server** list box, check **Check All Services**.

c) Cisco Unified Communications Manager and IM and Presence clusters only: To monitor specific services on all nodes in a cluster, check **Check Selected Services on All Nodes**.
This setting applies for all nodes in the cluster where the service is active.

d) Cisco Unified Communications Manager and IM and Presence clusters only: To monitor all services for all nodes in the cluster, check **Check All Services on All Nodes**.

Step 5 Select **Save**.

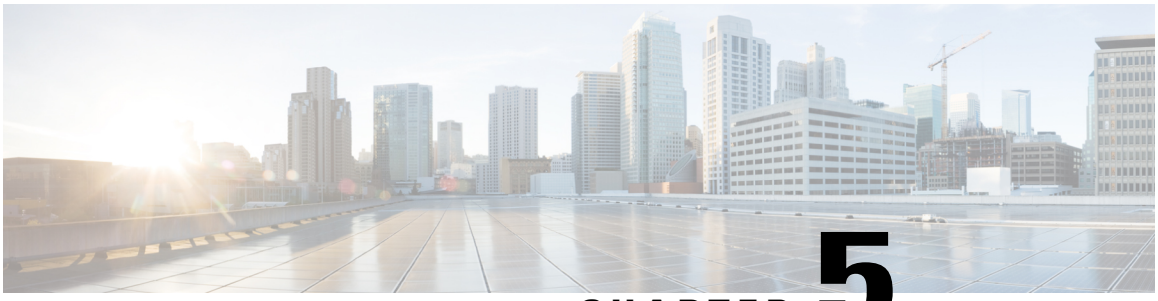
Step 6 Select one of the following buttons to restore the original trace settings:

a) **Reset Troubleshooting Traces—**Restores the original trace settings for the services on the node that you chose in the Server list box; also displays as an icon that you can select.

b) Cisco Unified Communications Manager and IM and Presence clusters only: **Reset Troubleshooting Traces On All Nodes—**Restores the original trace settings for the services on all nodes in the cluster.
The Reset Troubleshooting Traces button displays only if you have set troubleshooting trace for one or more services.

Note Leaving troubleshooting trace enabled for a long time increases the size of the trace files and may affect the performance of the services.

After you select the **Reset** button, the window refreshes and the service check boxes display as unchecked.



CHAPTER 5

Services

- Feature Services, page 61
- Network Services, page 72
- Services setup, page 82

Feature Services

Use the Serviceability GUI to activate, start, and stop Cisco Unified Communications Manager and IM and Presence services. Activation turns on and starts a service. You must manually activate the feature service for all features that you want to use. For service-activation recommendations, see topics related to service activation.

Note If you try to access a Cisco Unified Communications Manager server from an IM and Presence node or vice versa, you may encounter the following error: "Connection to the Server cannot be established (unable to access Remote Node)" . If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager* .

Note Devices using IM and Presence are configured to use a Postgres external database to support persistent chat, compliance, and file transfer. However, the connection between IM and Presence server and Postgres is not secured and the data passes without any check. For the services or devices that do not support TLS, there is another way to provide secure communication by configuring IP Sec, which is a standard protocol for secure communications by authenticating and encrypting each IP packet of a communication session.

After you activate a service in the **Service Activation** window, you do not need to start it in the **Control Center - Feature Services** window. If the service does not start for any reason, you must start it in the **Control Center - Feature Services** window.

After the system is installed, it does not automatically activate feature services, You need to activate the feature service to use your configuration features, for example, the Serviceability Reports Archive feature.

Cisco Unified Communications Manager and Cisco Unified IM and Presence Service only: If you are upgrading Cisco Unified Communications Manager, those services that you activated on the system before the upgrade automatically start after the upgrade.

After you activate feature services, you can modify service parameter settings using the administrative GUI for your product:

- Cisco Unified Communications Manager Administration
- Cisco Unity Connection Administration

Feature Services Categories

In Cisco Unified Serviceability, the **Service Activation** window and the **Control Center - Feature Services** window categorize feature services into the following groups:

- Database and administration services
- Performance and monitoring services
- CM services
- CTI services
- CDR services
- Security services
- Directory services
- Voice quality reporter services

In Cisco Unified IM and Presence Serviceability, the **Service Activation** window and the **Control Center - Feature Services** window categorize feature services into the following groups:

- Database and administration services
- Performance and monitoring services
- IM and Presence Service services

Database and Administration Services

Locations Bandwidth Manager

This service is not supported by IM and Presence Service.

The Locations Bandwidth Manager service assembles a network model from configured Location and Link data in one or more clusters, determines the Effective Paths between pairs of Locations, determines whether to admit calls between a pair of Locations based on the availability of bandwidth for each type of call, and deducts (reserves) bandwidth for the duration of each call that is admitted.

Cisco AXL Web Service

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

In an IM and Presence Service system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

Cisco UXL Web Service

This service is not supported by IM and Presence Service.

The TabSync client in Cisco IP Phone Address Book Synchronizer uses the Cisco UXL Web Service for queries to the Cisco Unified Communications Manager database, which ensures that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them. The Cisco UXL Web Service performs the following functions:

- Conducts authentication checks by verifying the end-user username and password when an end user logs in to Cisco IP Phone Address Book Synchronizer.
- Conducts a user authorization check by only allowing the user that is currently logged in to Cisco IP Phone Address Book Synchronizer to perform functions such as listing, retrieving, updating, removing, and adding contacts.

Cisco Bulk Provisioning Service

This service does not support Cisco Unity Connection.

If your configuration supports clusters (Cisco Unified Communications Manager only), you can activate the Cisco Bulk Provisioning Service only on the first server. If you use the Cisco Unified Communications Manager Bulk Administration Tool to administer phones and users, you must activate this service.

Cisco TAPS Service

This service does not support Cisco Unity Connection or IM and Presence Service.

The Cisco Tools for Auto-Registered Phones Support (TAPS) Service supports the Cisco Unified Communications Manager Auto-Register Phone Tool, which allows a user to upload a customized configuration on an auto registered phone after a user responds to Interactive Voice Response (IVR) prompts.

If your configuration supports clusters (Cisco Unified Communications Manager only), you activate this service on the first server. When you want to create dummy MAC addresses for the tool, ensure that the Cisco Bulk Provisioning Service is activated on the same server.

Tip The Cisco Unified Communications Manager Auto-Register Phone Tool relies on Cisco Customer Response Solutions (CRS). Before the tool can work as designed, verify that the CRS server is configured and running, as described in the CRS documentation.

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

Performance and monitoring services

Cisco Serviceability Reporter

The Cisco Serviceability Reporter service generates daily reports. For details, see topics that are related to the serviceability reports archive.

If your configuration supports clusters (Cisco Unified Communications Manager only), this service is installed on all the Cisco Unified Communications Manager servers in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco Unified Serviceability from the Tools menu. Each summary report comprises different charts that display the statistics for that particular report. After you activate the service, report generation may take up to 24 hours.

Related Topics

Serviceability Reports Archive, on page 93

Cisco CallManager SNMP Service

This service does not support IM and Presence Service and Cisco Unity Connection.

This service, which implements the CISCO-CCM-MIB, provides SNMP access to provisioning and statistics information that is available for Cisco Unified Communications Manager.

If your configuration supports clusters (Cisco Unified Communications Manager only), activate this service on all servers in the cluster.

CM Services

This section describes the CM Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CallManager

The Cisco CallManager Service provides software-only call processing as well as signaling and call control functionality for Cisco Cisco Unified Communications Manager.

Tip Cisco Cisco Unified Communications Manager clusters only: Before you activate this service, verify that the Cisco Cisco Unified Communications Manager server displays in the Find and List Cisco Cisco Unified Communications Managers window in Cisco Cisco Unified Communications Manager Administration. If the server does not display, add the Cisco Cisco Unified Communications Manager server before you activate this service. For information on how to find and add the server, see the *Administration Guide for Cisco Unified Communications Manager* .

Cisco Cisco Unified Communications Manager clusters only: If you deactivate the Cisco CallManager or CTIManager services in Service Activation, the Cisco Cisco Unified Communications Manager server where you deactivated the service no longer exists in the database, which means that you cannot choose that Cisco Cisco Unified Communications Manager server for configuration operations in Cisco Cisco Unified Communications Manager Administration because it does not display in the graphical user interface (GUI). If you then reactivate the services on the same Cisco Cisco Unified Communications Manager server, the database creates an entry for Cisco Cisco Unified Communications Manager again and adds a "CM_" prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager or CTIManager service on a server with an IP address of 172.19.140.180, then CM_172.19.140.180 displays in Cisco Cisco Unified Communications Manager Administration. You can now choose the server, with the new "CM_" prefix, in Cisco Cisco Unified Communications Manager Administration.

The following services rely on Cisco CallManager service activation:

- CM Services
- CDR Services

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files that are consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

Cisco Unified Communications Manager only: A configuration file includes a list of Cisco Unified Communications Managers to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (DHCP) server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. The device requests a configuration file from the TFTP server. The configuration file contains a list of Cisco Unified Communications Managers and the TCP port through which the device connects to those Cisco Unified Communications Managers. The configuration file contains a list of Cisco Unified Communications Managers and the TCP port through which the device connects to those Cisco Unified Communications Managers.

Cisco Unified Mobile Voice Access Service

The Cisco Unified Voice Access Service starts the mobile voice access capability within Cisco Unified Mobility; mobile voice access, which is an integrated voice response (IVR) system, allows Cisco Unified Mobility users to perform the following tasks:

- Make calls from the cellular phone as if the call originated from the desk phone.
- Turn Cisco Unified Mobility on.

- Turn Cisco Unified Mobility off.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for Cisco Unified Communications Manager for use with Media Termination Point (MTP), conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from Cisco Unified Communications Manager to the IP voice media streaming driver, which handles Real-Time Protocol (RTP) streaming.

The Cisco IP Voice Media Streaming Application service does not generate the Call Management Record (CMR) files for call legs that involve any IP Voice Media Streaming Application components like conference, MOH, annunciator, or MTP.

Cisco CTIManager

The Cisco CTI Manager contains the CTI components that interact with applications. This service allows applications to monitor or control phones and virtual devices to perform call control functionality.

Cisco Unified Communications Manager clusters only: With CTI Manager, applications can access resources and functionality of all Cisco Unified Communications Managers in the cluster and have improved failover capability. Although one or more CTI Managers can be active in a cluster, only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can use only one connection at a time to open a device with media termination.

Cisco Extension Mobility

This service, which supports the Cisco Extension Mobility feature, performs the login and automatic logout functionality for the feature.

Cisco Dialed Number Analyzer

The Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. When activated, this application consumes a lot of resources, so activate this service only during off-peak hours when minimal call-processing interruptions may occur.

Cisco Unified Communications Manager clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

Cisco Dialed Number Analyzer Server

The Cisco Dialed Number Analyzer Server service along with The Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

Cisco Unified Communications Manager clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

Cisco DHCP Monitor Service

Cisco DHCP Monitor Service monitors IP address changes for IP phones in the database tables. When a change is detected, it modifies the /etc./dhcpd.conf file and restarts the DHCPD daemon.

Cisco Intercluster Lookup Service

The Intercluster Lookup Service (ILS) runs on a cluster-wide basis. ILS allows you to create networks of remote Cisco Cisco Unified Communications Manager clusters. The ILS cluster discovery feature allows Cisco Cisco Unified Communications Manager to connect to remote clusters without the need for an administrator having to manually configure connections between each cluster. The ILS Global Dial Plan Replication feature enables clusters in the ILS network with the ability to exchange global dial plan data with the other clusters in an ILS network.

ILS can be activated from the ILS Configuration window that can be accessed in Cisco Cisco Unified Communications Manager Administration by selecting **Advanced Features** > **ILS Configuration**.

Cisco UserSync Service

Cisco UserSync service synchronizes the data from Cisco Unified Communications Manager end-user table to the LDAP database.

Cisco UserLookup Web Service

Cisco UserLookup Web service routes the commercial calls (calls through external gateways) to an alternate internal number of the called party in order to avoid the commercial cost of calling an external number.

If a caller within a Cisco Unified Communications Manager network makes a call on an external number, Cisco Unified Communications Manager checks if an internal number exists for the called party in the LDAP database. If an internal number exists, the call is routed to that internal number. If the internal number is not found in the LDAP database, the call is routed to the original (external) number.

IM and Presence Services

IM and Presence services apply only to IM and Presence Service.

Cisco SIP Proxy

The Cisco SIP Proxy service is responsible for providing the SIP registrar and proxy functionality. This includes request routing, requestor identification, and transport interconnection.

Cisco Presence Engine

The Cisco Presence Engine collects, aggregates, and distributes user capabilities and attributes using the standards-based SIP and SIMPLE interface. It collects information about the availability status and communications capabilities of a user.

Cisco XCP Text Conference Manager

The Cisco XCP Text Conference Manager supports the chat feature. The chat feature allows users to communicate with each other in online chat rooms. It supports chat functionality using ad hoc (temporary) and permanent chat rooms, which remain on a Cisco-supported external database until they are deleted.

Cisco XCP Web Connection Manager

The Cisco XCP Web Connection Manager service enables browser-based clients to connect to IM and Presence Service.

Cisco XCP Connection Manager

The Cisco XCP Text Conference Manager supports the chat feature. The chat feature allows users to communicate with each other in online chat rooms. It supports chat functionality using ad hoc (temporary) and permanent chat rooms, which remain on a Cisco-supported external database until they are deleted.

Cisco XCP SIP Federation Connection Manager

The Cisco XCP SIP Federation Connection Manager supports interdomain federation with Microsoft OCS over the SIP protocol. You must also turn on this service when your deployment contains an intercluster connection between an IM and Presence Service Release 9.0 cluster, and a Cisco Unified Presence Release 8.6 cluster.

Cisco XCP XMPP Federation Connection Manager

The Cisco XCP XMPP Federation Connection Manager supports interdomain federation with third party enterprises such as IBM Lotus Sametime, Cisco Webex Meeting Center, and GoogleTalk over the XMPP protocol, as well as supports interdomain federation with another IM and Presence Service enterprise over the XMPP protocol.

Cisco XCP Message Archiver

The Cisco XCP Message Archiver service supports the IM Compliance feature. The IM Compliance feature logs all messages sent to and from the IM and Presence Service server, including point-to-point messages, and messages from ad hoc (temporary) and permanent chat rooms for the Chat feature. Messages are logged to an external Cisco-supported database.

Cisco XCP Directory Service

The Cisco XCP Directory Service supports the integration of XMPP clients with the LDAP directory to allow users to search and add contacts from the LDAP directory.

Cisco XCP Authentication Service

The Cisco XCP Authentication Service handles all authentication requests from XMPP clients that are connecting to IM and Presence Service.

CTI Services

This section describes the CTI Services and does not apply to Cisco Unity Connection or IM and Presence Service.

Cisco IP Manager Assistant

This service supports Cisco Unified Communications Manager Assistant. After service activation, Cisco Unified Communications Manager Assistant enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified Communications Manager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

Cisco WebDialer Web Service

Cisco WebDialer Web Service for Cisco Unified Communications Manager Systems

Cisco Web Dialer provides click-to-dial functionality. It allows users inside a Cisco Unified Communications Manager cluster to initiate a call to other users inside or outside the cluster by using a web page or a desktop application. Cisco Web Dialer provides a web page that enables users to call each other within a cluster. Cisco Web Dialer comprises two components: Web Dialer servlet and Redirector servlet.

The Redirector servlet provides the ability for third-party applications to use Cisco Web Dialer. The Redirector servlet finds the appropriate Cisco Unified Communications Manager cluster for the Cisco Web Dialer user and redirects the request to the Cisco Web Dialer in that cluster. The Redirector functionality applies only for HTTP/HTML-based Web Dialer client applications because it is not available for Simple Object Access Protocol (SOAP)-based Web Dialer applications.

Self-Provisioning IVR

With the introduction of Self-Provisioning IVR Service, the autoregistered IP phones on the Cisco Unified Communications Manager are assigned to users quickly with less effort. When you dial the CTI RP DN, that is configured on the Self-Provisioning page, from an extension of a user that uses the IVR service, the phone connects to the Self-Provisioning IVR application and prompts you to provide the Self-Service credentials.

Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phones to the users.

You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.

To enable the Self-Provisioning IVR service, you must also enable the Cisco CTI Manager service.

For more information about how to configure self-provisioning, see the *Administration Guide for Cisco Unified Communications Manager* .

CDR Services

This section describes the CDR Services and does not apply to IM and Presence Service and Cisco Unity Connection.

CAR Web Service

The Cisco CAR Web Service loads the user interface for CAR, a web-based reporting application that generates either CSV or PDF reports by using CDR data.

Cisco SOAP - CDROnDemand Service

The Cisco SOAP - CDROnDemand Service, a SOAP/HTTPS-based service, runs on the CDR Repository server. It receives SOAP requests for CDR filename lists that are based on a user-specified time interval (up to a maximum of 1 hour) and returns a list of filenames that fit the time duration that is specified in the request. This service also receives requests for delivery of a specific CDR/CMR file with the filename and the transfer method (SFTP/FTP, server name, login info, directory) that is specified in the request.

If you are using a third-party billing application that accesses CDR data through an HTTPS/SOAP interface, activate this service.

Security Services

This section describes the Security Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CTL Provider

Cisco Unified Communications Manager only: The Cisco Certificate Trust List (CTL) Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Cisco Unified Communications Manager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster.

You can install and configure the Cisco CTL Client or the CLI command set **utils ctl**, and then activate this service for the clusterwide security mode to change from nonsecure to secure.

After you activate the service, the Cisco CTL Provider service reverts to the default CTL port, which is 2444. If you want to change the port, see the *Cisco Unified Communications Manager Security Guide* for more information.

Cisco Certificate Authority Proxy Function (CAPF)

Working in conjunction with the Cisco Certificate Authority Proxy Function (CAPF) application, the CAPF service can perform the following tasks, depending on your configuration:

- Issue locally significant certificates to supported Cisco Unified IP Phone models.
- Upgrade existing certificates on the phones.
- Retrieve phone certificates for troubleshooting.
- Delete locally significant certificates on the phone.

Note Cisco Unified Communications Manager only: When you view real-time information in the Real-Time Monitoring Tool (RTMT), the CAPF service displays only for the first server.

Directory Services

This section describes the Directory Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco DirSync

Cisco Unified Communications Manager: The Cisco DirSync service ensures that the Cisco Unified Communications Manager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Cisco Unified Communications Manager, the Cisco DirSync service migrates the user data to the Cisco Unified Communications Manager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.

Note Users with duplicate email IDs are not synchronized and the administrator receives no notification about the list of users which are not synced. These IDS are shown in the DirSync error logs from Unified RTMT.

Cisco Unity Connection: When Cisco Unity Connection is integrated with an LDAP directory, the Cisco DirSync service synchronizes a small subset of user data (first name, last name, alias, phone number, and so on) in the Cisco Unified Communications Manager database on the Cisco Unity Connection server with the corresponding data in the LDAP directory. Another service (CuCmDbEventListener) synchronizes data in the Cisco Unity Connection user database with data in the Cisco Unified Communications Manager database. When a Cisco Unity Connection cluster is configured, the Cisco DirSync service runs only on the publisher server.

Location Based Tracking Services

This section describes Location Based Tracking Services.

Cisco Wireless Controller Synchronization Service

This service supports the Location Awareness feature, which provides a status of your network's wireless access points and associated mobile devices.

This service must be running to synchronize Cisco Unified Communications Manager with a Cisco wireless access point controller. When the service is running, and synchronization is configured, Cisco Unified Communications Manager syncs its database with a Cisco wireless access point controller and saves status information for the wireless access points that the controller manages. You can schedule syncs to occur at regular intervals so that the information stays current.

Note Make sure that this service is running when adding a new Cisco wireless access point controller.

Voice Quality Reporter Services

This section describes the Voice Quality Reporter Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco Extended Functions

The Cisco Extended Functions service provides support for Cisco Unified Communications Manager voice-quality features, including Quality Report Tool (QRT). For more information about individual features, see the *System Configuration Guide for Cisco Unified Communications Manager* and the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*.

Network Services

Installed automatically, network services include services that the system requires to function, for example, database and platform services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Control Center - Network Services window.

After the installation of your application, network services start automatically, as noted in the Control Center - Network Services window. The serviceability GUI categorizes services into logical groups.

Performance and Monitoring Services

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT servlet supports the IM and Presence Real-Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor system performance and performance counters, and so on.

Cisco RTMT Reporter Servlet

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

Cisco Log Partition Monitoring Tool

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

Cisco Tomcat Stats Servlet

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

Cisco RIS Data Collector

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

Cisco AMC Service

Used for the Real-Time Monitoring Tool (RTMT), this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server (or on all servers in the cluster).

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any administrative configuration change to the Cisco Unified Communications Manager or IM and Presence system by a user or as a result of the user action. The Cisco Audit Event Service also monitors and logs end user events such as login, logout, and IM chat room entry and exit.

Backup and Restore Services

Cisco DRF Master

This does not apply to IM and Presence Service.

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

Cisco DRF Local

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

System Services

Cisco CallManager Serviceability

The Cisco CallManager Serviceability service supports Cisco Unified Serviceability and the IM and Presence Service serviceability GUIs, which are web application/interfaces that you use to troubleshoot issues and manage services. This service, which is installed automatically, allows you access to the serviceability GUIs. If you stop this service on the server, you cannot access the serviceability GUI when you browse into that server.

Cisco CDP

Cisco Discovery Protocol (CDP) advertises the voice application to other network management applications, so the network management application, for example, SNMP or Cisco Unified Operations Manager, can perform network management tasks for the voice application.

Cisco Trace Collection Servlet

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

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

Cisco Trace Collection Service

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

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

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

Platform Services

A Cisco DB

A Cisco DB service supports the Progres database engine on Cisco Cisco Unified Communications Manager. On IM and Presence Service, A Cisco DB service supports the IDS database engine.

A Cisco DB Replicator

Cisco Unified Communications Manager and IM and Presence only: The A Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent servers in the cluster.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

SNMP Master Agent

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

Tip After you complete SNMP configuration in the serviceability GUI, you must restart the SNMP Master Agent service in the **Control Center—Network Features** window.

MIB2 Agent

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

Host Resources Agent

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

Native Agent Adaptor

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

For IM and Presence Service and Cisco Cisco Unified Communications Manager, this service will not be present if installed on a Virtual Machine.

System Application Agent

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

Cisco CDP Agent

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

Cisco Syslog Agent

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

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

Cisco Certificate Change Notification

This service keep certificates of components like Tomcat, CallManager, and XMPP automatically synchronized across all nodes in the cluster. When the service is stopped and you regenerate certificates, then you have manually upload them to Certificate Trust on the other nodes.

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate is close to its expiration date. For Cisco Cisco Unified Communications Manager, you manage the certificates that use this service in Cisco Unified Operating System Administration. For IM and Presence Service, you manage the certificates that use this service in Cisco Unified IM and Presence Operating System Administration.

Cisco License Manager

This service is not supported by IM and Presence Service and Cisco Unity Connection.

Cisco License Manager keeps track of the Cisco Cisco Unified Communications Manager-related licenses that a customer purchases and uses. It controls license checkins and checkouts, and it takes responsibility for issuing and reclaiming Cisco Cisco Unified Communications Manager-related licenses. For Cisco Cisco Unified Communications Manager, Cisco License Manager manages the Cisco Cisco Unified Communications Manager application and the number of IP phone unit licenses. When the number of phones exceeds the number of licenses, it issues alarms.

Cisco Cisco Unified Communications Manager clusters only: This service runs on all the servers, but the service on the first server has the responsibility for issuing and reclaiming licenses.

Security Services

Cisco Trust Verification Service

This service is not supported by IM and Presence Service.

Cisco Trust Verification Service is a service running on a CallManager server or a dedicated server, that authenticates certificates on behalf of phones and other endpoints. It associates a list of roles for the owner of the certificate. A certificate or the owner can be associated with one or many roles.

The protocol between phones and Trust Verification Service allows phones to request for verification. Trust Verification Service validates the certificate and returns a list of roles associated with it. The protocol allows Trust Verification Service to authenticate a request and conversely, a phone to authenticate the response from Trust Verification Service. The protocol protects the integrity of the request and the response. Confidentiality of the request and the response is not required.

Multiples instances of Cisco Trust Verification Service run on different servers in the cluster to provide scalability. These servers may or may not be the same as the ones hosting the Cisco Unified CallManager. Phones obtain a list of Trust Verification Services in the network and connect to one of them using a selection algorithm (example: Round Robin). If the contacted Trust Verification Service does not respond, the phone switches to the next Trust Verification Service in the list.

Database Services

Cisco Database Layer Monitor

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

Note Cisco Unified Communications Manager uses Automatic Update Statistics, an intelligent statistics update feature that monitors the changes that are made in the database tables and updates only tables that need statistic updates. This feature saves considerable bandwidth, especially on VMware deployments of Cisco Unified Communications Manager. Automatic Update Statistics is the default indexing method.

SOAP Services

Cisco SOAP-Real-Time Service APIs

IM and Presence Service only: The Cisco SOAP-Real-Time Service APIs support client login and third-party APIs for presence data.

Cisco Unified Communications Manager and Cisco Unity Connection only: The Cisco SOAP-Real-Time Service APIs allow you to collect real-time information for devices and CTI applications. This service also provides APIs for activating, starting, and stopping services.

Cisco SOAP-Performance-Monitoring APIs

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

Cisco SOAP-Log-Collection APIs

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

SOAP-Diagnostic Portal Database Service

The Cisco Unified Real-Time Monitoring Tool (RTMT) uses the SOAP-Diagnostic Portal Database Service to access the RTMT Analysis Manager hosting database. RTMT gathers call records based on operator-defined filter selections. If this service is stopped, RTMT cannot collect the call records from the database.

CM Services

This section describes the Cisco Unified Communications Manager CM Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco Extension Mobility Application

The Cisco Extension Mobility Application service allows you to define login settings such as duration limits on phone configuration for the Cisco Extension Mobility feature.

Cisco Unified Communications Manager only: The Cisco Extension Mobility feature allows users within a Cisco Unified Communications Manager cluster to temporarily configure another phone in the cluster as their own phone by logging in to that other phone. After a user logs in, the phone adopts the personal phone numbers, speed dials, services links, and other user-specific properties of the user. After logout, the phone adopts the original user profile.

Cisco User Data Services

Cisco User Data Services provides Cisco Unified IP Phones with the ability to access user data from the Cisco Unified Communications Manager database. Cisco User Data Services provides support for Cisco Personal Directory.

IM and Presence Service Services

IM and Presence Service services apply only to IM and Presence Service.

Cisco Login Datastore

The Cisco Login Datastore is a real-time database for storing client sessions to the Cisco Client Profile Agent.

Cisco Route Datastore

The Cisco Route Datastore is a real-time database for storing a cache of route information and assigned users for the Cisco SIP Proxy and the Cisco Client Profile Agent.

Cisco Config Agent

The Cisco Configuration Agent is a change-notification service that notifies the Cisco SIP Proxy of configuration changes in the IM and Presence Service IDS database.

Cisco Sync Agent

The Cisco Sync Agent keeps IM and Presence data synchronized with Cisco Unified Communications Manager data. It sends SOAP requests to the Cisco Unified Communications Manager for data of interest to IM and Presence and subscribes to change notifications from Cisco Unified Communications Manager and updates the IM and Presence IDS database.

Cisco OAM Agent

The Cisco OAM Agent service monitors configuration parameters in the IM and Presence Service IDS database that are of interest to the Presence Engine. When a change is made in the database, the OAM Agent writes a configuration file and sends an RPC notification to the Presence Engine.

Cisco Client Profile Agent

The Cisco Client Profile Agent service provides a secure SOAP interface to or from external clients using HTTPS.

Cisco Intercluster Sync Agent

The Cisco Intercluster Sync Agent service provides the following: DND propagation to Cisco Unified Communications Manager and syncs end user information between IM and Presence Service clusters for intercluster SIP routing.

Cisco XCP Router

The XCP Router is the core communication functionality on the IM and Presence Service server. It provides XMPP-based routing functionality on IM and Presence Service; it routes XMPP data to the other active XCP services on IM and Presence Service, and it accesses SDNS to allow the system to route XMPP data to IM and Presence Service users. The XCP router manages XMPP sessions for users, and routes XMPP messages to and from these sessions.

After IM and Presence Service installation, the system turns on Cisco XCP Router by default.

Note If you restart the Cisco XCP Router, IM and Presence Service automatically restarts all active XCP services. Note that you must select the Restart option to restart the Cisco XCP Router; this is not the same as turning off and turning on the Cisco XCP Router. If you turn off the Cisco XCP Router, rather than restart this service, IM and Presence Service stops all other XCP services. Subsequently when you turn on the XCP router, IM and Presence Service does not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

Cisco XCP Config Manager

The Cisco XCP Config Manager service monitors the configuration and system topology changes made through the administration GUI (as well as topology changes that are synchronized from an InterCluster Peer) that affect other XCP components (for example, Router and Message Archiver), and updates these components as needed. The Cisco XCP Config Manager service creates notifications for the administrator indicating when an XCP component requires a restart (due to these changes), and it automatically clears the notifications after the restarts are complete.

Cisco Server Recovery Manager

The Cisco Server Recovery Manager (SRM) service manages the failover between nodes in a presence redundancy group. The SRM manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual). Once you turn on high availability in a presence redundancy group, the SRM on each node establishes heartbeat connections with the peer node and begins to monitor the critical processes.

Cisco IM and Presence Data Monitor

The Cisco IM and Presence Data Monitor monitors IDS replication state on the IM and Presence Service. Other IM and Presence services are dependent on the Cisco IM and Presence Data Monitor. These dependent services use the Cisco service to delay startup until such time as IDS replication is in a stable state.

The Cisco IM and Presence Data Monitor also checks the status of the Cisco Sync Agent sync from Cisco Unified Communications Manager. Dependent services are only allowed to start after IDS replication has set

up and the Sync Agent on the IM and Presence database publisher node has completed its sync from Cisco Unified Communications Manager. After the timeout has been reached, the Cisco IM and Presence Data Monitor on the Publisher node will allow dependent services to start even if IDS replication and the Sync Agent have not completed.

On the subscriber nodes, the Cisco IM and Presence Data Monitor delays the startup of feature services until IDS replication is successfully established. The Cisco IM and Presence Data Monitor only delays the startup of feature services on the problem subscriber node in a cluster, it will not delay the startup of feature services on all subscriber nodes due to one problem node. For example, if IDS replication is successfully established on node1 and node2, but not on node3, the Cisco IM and Presence Data Monitor allows feature services to start on node1 and node2, but delays feature service startup on node3.

Cisco Presence Datastore

The Cisco Presence Datastore is a real-time database for storing transient presence data and subscriptions.

Cisco SIP Registration Datastore

The Cisco Presence SIP Registration Datastore is a real-time database for storing SIP Registration data.

Cisco RCC Device Selection

The Cisco RCC Device Selection service is the Cisco IM and Presence user device selection service for Remote Call Control.

CDR Services

This section describes the CDR Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CDR Repository Manager

This service maintains and moves the generated Call Detail Records (CDRs) that are obtained from the Cisco CDR Agent service. In a system that supports clusters (Cisco Unified Communications Manager only), the service exists on the first server.

Cisco CDR Agent

Note Cisco Unified Communications Manager supports Cisco CDR Agent in Cisco Unified Communications Manager systems.

This service does not support IM and Presence Service and Cisco Unity Connection.

The Cisco CDR Agent service transfers CDR and CMR files that are generated by Cisco Unified Communications Manager from the local host to the CDR repository server, where the CDR Repository Manager service runs over a SFTP connection.

This service transfers CDR and CMR files generated from the local host to the CDR repository server in a cluster. The CDR Agent in the CDR Repository Node standalone server transfers the files that are generated by the standalone server to the Cisco CDR Repository Manager over a SFTP connection. The CDR Agent maintains and moves the files.

For this service to work, activate the Cisco CallManager service on the server and ensure that it is running. If your configuration supports clusters (Cisco Unified Communications Manager only), activate the Cisco CallManager service on the first server.

Cisco CAR Scheduler

The Cisco CDR Analysis and Reporting (CAR) Scheduler service does not support IM and Presence Service and Cisco Unity Connection.

The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database.

Cisco SOAP-CallRecord Service

The Cisco SOAP-CallRecord service runs by default on the publisher as a SOAP server, so that the client can connect to CAR database through the SOAP API. This connection happens through the use of the CAR connector (with a separate CAR IDS instance).

Cisco CAR DB

Cisco CAR DB manages the Informix instance for the CAR database, which allows Service Manager to start or stop this service and to bring up or shut down the CAR IDS instance respectively. This is similar to the Unified Communications Manager database that is used to maintain the CCM IDS instance.

The Cisco CAR DB service is activated on the publisher by default. The CAR DB instances are installed and actively run on the publisher, to maintain the CAR database. This network service is used only on the publisher and is not available on the subscribers.

Admin Services

This section describes the Admin Services and does not apply to Cisco Unity Connection.

Cisco CallManager Admin

The Cisco CallManager Admin service is not supported by IM and Presence Service and Cisco Unity Connection.

The Cisco CallManager Admin service supports Cisco Unified CM Administration, the web application/interface that you use to configure Cisco Cisco Unified Communications Manager settings. After the Cisco Cisco Unified Communications Manager installation, this service starts automatically and allows you to access the graphical user interface (GUI). If you stop this service, you cannot access the Cisco Unified CM Administration graphical user interface when you browse into that server.

Cisco IM and Presence Admin

The Cisco IM and Presence Admin service is not supported by Cisco Cisco Unified Communications Manager and Cisco Unity Connection.

The Cisco IM and Presence Admin service supports Cisco Unified CM IM and Presence Administration, the web application/interface that you use to configure IM and Presence Service settings. After the IM and Presence Service installation, this service starts automatically and allows you to access the GUI. If you stop this service, you cannot access the Cisco Unified CM IM and Presence Administration GUI when you browse into that server.

Services setup

Control Center

From Control Center in the serviceability GUI, you can view status and start and stop one service at a time. To start, stop, and restart network services, access the Control Center - Network Services window. To start, stop, and restart feature services, access the Control Center - Feature Services window.

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

Cisco Unified Communications Manager and IM and Presence only: In a cluster configuration, you can view status and start and stop services for one server in the cluster at a time.

Cisco Unified Communications Manager only: Starting and stopping a feature service causes all Cisco Unified IP Phones and gateways that are currently registered to that service to fail over to their secondary service. Devices and phones need to restart only if they cannot register with their secondary service. Starting and stopping a service may cause other installed applications (such as a conference bridge or Cisco Messaging Interface) that are homed to that Cisco Unified Communications Manager to start and stop as well.

Caution Cisco Unified Communications Manager only: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, but other types of calls drop.

Set Up Services

You can perform the following tasks when working with services:

Procedure

Step 1 Activate the feature services that you want to run.

Step 2 Configure the appropriate service parameters.

Step 3 If necessary, troubleshoot problems by using the serviceability GUI trace tools.

Service Activation

Note You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in the serviceability GUI. You can view, start, and stop Cisco Unified Communications Manager services from an IM and Presence node and vice versa. You may encounter the following error: "Connection to the Server cannot be established (unable to access Remote Node)". If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager*.

Note Starting with Cisco Unified Communications Manager Release 6.1.1, end users can no longer access Cisco Unified Serviceability to start and stop services.

Feature services are activated in automatic mode and the serviceability GUI checks for service dependencies based on a single-node configuration. When you choose to activate a feature service, you are prompted to select all the other services, if any, that depend on that service to run. When you click **Set Default**, the serviceability GUI chooses those services that are required to run on the server.

Cisco Unified Communications Manager and IM and Presence Service only: Even in a configuration that supports clusters, this process is based on a single-server configuration.

Activating a service automatically starts the service. You start and stop services from Control Center.

ClusterServiceActivationRecommendationsforCiscoUnifiedCommunications Manager

Before you activate services in a cluster, review the following table, which provides service recommendations for multiserver Cisco Unified Communications Manager configurations.

Table 44: Cisco Unified Communications Manager Service Activation Recommendations

Service/Servlet	Activation Recommendations
CM Services	
Cisco CallManager	This service supports Cisco Unified Communications Manager. In the Control Center - Network Services, ensure that the Cisco RIS Data Collector service and Database Layer Monitor service are running on the node. **Tip** Before you activate this service, verify that the Cisco Unified Communications Manager server displays in the Cisco Unified Communications Manager Find/List window in Cisco Unified Communications Manager Administration. If the server does not display, add the Cisco Unified Communications Manager server before you activate this service. For information on how to add a server, see the *System Configuration Guide for Cisco Unified Communications Manager*.

Service/Servlet	Activation Recommendations
Cisco Messaging Interface	Activate only if using an SMDI integration to a third-party Voicemail system using a server-attached USB-to-serial adapter.
Cisco Unified Mobile Voice Access Service	For mobile voice access to work, you must activate this service on the first node in the cluster after you configure the H.323 gateway to point to the first VXML page. In addition, make sure that the Cisco CallManager and the Cisco TFTP services run on one server in the cluster, not necessarily the same server where the Cisco Unified Mobile Voice Access Service runs.
Cisco IP Voice Media Streaming App	If you have more than one node in the cluster, activate on one or two servers per cluster. You may activate on a node that is dedicated specifically for music on hold. This service requires that you activate Cisco TFTP on one node in the cluster. Do not activate this service on the first node or on any nodes that run the Cisco CallManager service.
Cisco CTIManager	Activate on each node to which JTAPI/TAPI applications will connect. CTIManager activation requires the Cisco CallManager service also to be activated on the node. See topics related to CM services for more information on CTIManager and Cisco CallManager services interaction.
Cisco Extension Mobility	Activate on all nodes in the cluster.
Cisco Extended Functions	Activate this service, which supports the Quality Report Tool (QRT), on one or more servers that run the Cisco RIS Data Collector. Make sure that you activate the Cisco CTIManager service on a node in the cluster.
Cisco DHCP Monitor Service	When the DHCP Monitor service is enabled, it detects changes in the database that affect IP addresses for the IP phones, modifies the /etc/dhcpd.conf file, and stops and restarts the DHCPD daemon with the updated configuration file. Activate this service on the node that has DHCP enabled.
Cisco Location Bandwidth Manager	If you plan to use Cisco Location Call Admission Control functionality to manage bandwidth allocation for audio and video calls, you must activate this service. This service works in conjunction with the Cisco CallManager service. It is recommended to run the Cisco Location Bandwidth Manager on the same server that runs the Cisco CallManager service. If the Location Bandwidth Manager is not running on the same server as the CallManager service, ensure that you configure the Location Bandwidth Manager Group correctly.
Cisco Intercluster Lookup Service	If you plan to propagate the URI and numeric routing information between multiple Cisco Unified Communications Manager clusters, you must activate this service on the publisher of the cluster that participates in this exchange.
Cisco Dialed Number Analyzer Server	If you have more than one node in the cluster, activate this service on one node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

Service/Servlet	Activation Recommendations
Cisco Dialed Number Analyzer	If you are planning to use Cisco Unified Communications Manager Dialed Number Analyzer, activate this service. This service may consume a lot of resources, so only activate this service on the node with the least amount of call-processing activity or during off-peak hours.
Cisco TFTP	If you have more than one node in the cluster, activate this service on one node that is dedicated specifically for the Cisco TFTP service. Configure Option 150 if you activate this service on more than one node in the cluster.
CTI Services	
Cisco IP Manager Assistant	If you are planning to use Cisco Unified Communications Manager Assistant, activate this service on any two servers (Primary and Backup) in the cluster. Ensure that Cisco CTI Manager service is activated in the cluster. See the *Feature Configuration Guide for Cisco Unified Communications Manager* for more details on Cisco IP Manager Assistant.
Cisco WebDialer Web Service	Activate on one node per cluster.
Self-Provisioning IVR	To enable the Self-Provisioning IVR service, you must also enable the Cisco CTI Manager service. You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.
CDR Services	
Cisco SOAP-CDRonDemand Service	You can activate the Cisco SOAP-CDROnDemand Service only on the first server, and it requires that the Cisco CDR Repository Manager and Cisco CDR Agent services are running on the same server.
Cisco CAR Web Service	You can activate the Cisco CAR Web Service only on the first server, and it requires that the Cisco CAR Scheduler service is activated and running on the same server and that the CDR Repository Manager service also is running on the same server.
Database and Admin Services	
Cisco AXL Web Service	Following installation, Cisco AXL Web Service is enabled by default on all cluster nodes. Cisco recommends that you always leave the service activated on the publisher node. This ensures that you are able to configure products that are dependent on AXL, such as Unified Provisioning Manager. Based on your needs, you can activate or deactivate the service on specific subscriber nodes in Cisco Unified Serviceability under Feature Services.

Service/Servlet	Activation Recommendations
Cisco Bulk Provisioning Service	You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.
Cisco UXL Web Service	This service performs authentication and user authorization checks. The TabSync client in Cisco IP Phone Address Book Synchronizer uses the Cisco UXL Web Service for queries to the Cisco Unified Communications Manager database. If you plan to use the Cisco IP Phone Address Book Synchronizer, you must activate this service on one node, preferably publisher. If you are not using Cisco IP Phone Address Book Synchronizer, then Cisco recommends that you deactivate this service . By default, this service is deactivated.
Cisco Platform Administrative Web Service	You must activate this service if you plan to use a Cisco Prime Collaboration Deployment (PCD) server to manage upgrades, switch version, restart or readdress operations. Platform Administrative Web Service (PAWS) allows SOAP communication between the Call Manager and Prime Collaboration Deployment (PCD). If you have more than one node in the cluster, you must activate this service on each server in the cluster.
Cisco TAPS Service	Before you can use the Cisco Unified Communications Manager Auto-Register Phone Tool, you must activate this service on the first node. When you create dummy MAC addresses for the Cisco Unified Communications Manager Auto-Register Phone Tool, ensure that the Cisco Bulk Provisioning Service is activated on the same node.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Activate on only the first node. **Note** The service only generates reports on the first node even if you activate the service on other nodes.
Cisco CallManager SNMP Service	If you use SNMP, activate this service on all servers in the cluster.
Security Services	
Cisco CTL Provider	Activate on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	Activate on only the first node.
Directory Services	
Cisco DirSync	Activate only on the first node.

Cluster Service Activation Recommendations for IM and Presence Service

Caution Before you turn on any services for a feature, you must complete all the required configuration on IM and Presence for that feature. See the relevant documentation for each IM and Presence feature.

Before you turn on services in a cluster, review the following table, which provides service recommendations for multinode IM and Presence configurations.

Table 45: IM and Presence Service Activation Recommendations

Service/Servlet	Recommendations
Database and Admin Services	
Cisco AXL Web Service	Following installation, Cisco AXL Web Service is enabled by default on all cluster nodes. Cisco recommends that you always leave the service activated on the IM and Presence Service database publisher node. This ensures that you are able to configure products that are dependent on AXL. If intercluster communication is configured, this service must be enabled on both nodes in the sub-cluster where remote peers are configured to sync from. If this service is not enabled on both nodes presence and IM capabilities will be lost in failover scenarios. Based on your needs, you can activate or deactivate the service on specific IM and Presence subscriber nodes in Cisco Unified Serviceability under Feature Services.
Cisco Bulk Provisioning Service	• You turn on the Cisco Bulk Provisioning Service only on the first node. • If you use the Bulk Administration Tool (BAT) to administer users, you must turn on this service.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Turn on this service on the publisher node only. **Note** The service only generates reports on the publisher node even if you turn on the service on other nodes.
IM and Presence Services	
Cisco SIP Proxy	Turn on this service on all nodes in the cluster.

Service/Servlet	Recommendations
Cisco Presence Engine	Turn on this service on all nodes in the cluster.
Cisco Sync Agent	Turn on this service on all nodes in the cluster.
Cisco XCP Text Conference Manager	• Turn on this service if you deploy the chat feature on IM and Presence. • Turn on this service on each node that runs the chat feature. **Note** The permanent chat feature requires an external database. If you enable the permanent chat feature, you must also configure an external database before starting the Text Conference Manager service. The Text Conference Manager service will not start if the permanent chat feature is enabled and an external database is not configured. See the *Database Setup Guide for IM and Presence on Cisco Cisco Unified Communications Manager*.
Cisco XCP Web Connection Manager	• Turn on this service if you integrate web clients with IM and Presence. • Turn on this service on all nodes in the cluster.
Cisco XCP Connection Manager	• Turn on this service if you integrate XMPP clients with IM and Presence. • Turn on this service on all nodes in the cluster.
Cisco XCP SIP Federation Connection Manager	Turn on this service if you deploy any of the following configurations: • Interdomain federation over the SIP protocol on IM and Presence. Turn on this service on each node that runs SIP federation. • Intercluster deployment between a IM and Presence Release 9.x cluster and a Cisco Unified Presence Release 8.6(x) cluster. Turn on this service on all nodes in the Release 9.x cluster.

Service/Servlet	Recommendations
Cisco XCP XMPP Federation Connection Manager	• Turn on this service only if you deploy interdomain federation over the XMPP protocol on IM and Presence. • Turn on this service on each node that runs XMPP federation. **Note** Before you turn on the XMPP Federation Connection Manager service on a node, you must turn on XMPP Federation in Cisco Cisco Unified Communications Manager IM and Presence Administration on that node. See *Interdomain Federation for IM and Presence on Cisco Cisco Unified Communications Manager*.
Cisco XCP Message Archiver	• Turn on this service if you deploy the Compliance feature on IM and Presence. • Turn on this service on any node that runs the IM Compliance feature. **Note** If you turn on the Message Archiver before you configure an external database, the service will not start. Also, if the external database is not reachable, the service will not start. See the *Database Setup Guide for IM and Presence on Cisco Cisco Unified Communications Manager*.
Cisco XCP Directory Service	• Turn on this service if you integrate XMPP clients on IM and Presence with an LDAP directory. • Turn on this service on all nodes in the cluster. **Note** If you turn on the Directory Service before you configure the LDAP contact search settings for third-party XMPP clients, the service will start, and then stop again. See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.
Cisco XCP Authentication Service	• Turn on this service if you integrate XMPP clients with IM and Presence. • Turn on this service on all nodes in the cluster.

Activate Feature Services

You activate and deactivate feature services in the **Service Activation** window in the serviceability GUI. Services that display in the **Service Activation** window do not start until you activate them.

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

Tip Cisco Unified Communications Manager and IM and Presence Service only: Before you activate services in the Service Activation window, review topics related to cluster service activation recommendations.

Procedure

Step 1 Choose **Tools** > **Service Activation**.
The **Service Activation** window displays.

Step 2 Select the server (node) from the **Server** drop-down list, and then click **Go**.
You can access Cisco Unified Communications Manager services from an IM and Presence Service node and vice versa. You may encounter the following error when trying to access a remote node: "Connection to the Server cannot be established (unable to connect to Remote Node)". If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager*.

Step 3 Perform one of the following actions to turn on or turn off services:

a) To turn on the default services required to run on a single server, select **Set to Default**.
Note This option selects default services based on the configuration of a single server, and checks for service dependencies.

b) To turn on all services, check **Check All Services**.

c) To turn on a specific service, check the check box for the service that you want to turn on

d) To turn off a service, uncheck the check box for the services that you want to turn off.

Step 4 Cisco Unified Communications Manager and IM and Presence Service only: For a cluster configuration, review the cluster service activation recommendations, and then check the check boxes next to the services that you want to activate.

Step 5 After you check the check boxes for the services that you want to activate, click **Save**.
Tip To deactivate services that you activated, uncheck the check boxes next to the services that you want to deactivate; then, click **Save**.
Tip To obtain the latest status of the services, click the **Refresh** button.

Related Topics

Cluster Service Activation Recommendations for Cisco Unified Communications Manager, on page 83
Cluster Service Activation Recommendations for IM and Presence Service, on page 87

Start, Stop, and Restart Services in Control Center or CLI

To perform these tasks, the serviceability GUI provides two Control Center windows. To start, stop, and restart network services, access the **Control Center—Network Services** window. To start, stop, and restart feature services, access the **Control Center—Feature Services** window.

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

Start, Stop, and Restart Services in Control Center

Control Center in the serviceability GUI allows you to:

- view status
- refresh status
- start, stop, and restart feature and network services on a particular server, or for a server in a cluster in a cluster configuration

When a service is stopping, you cannot start it until after the service is stopped.

Caution Cisco Unified Communications Manager only: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone remain connected; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also remain connected, but other types of calls get dropped.

Procedure

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

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

  Tip Before you can start, stop, or restart a feature service, it must be activated.

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

Step 2 Choose the server from the Server drop-down list, and then click **Go**.
The window displays the following items:

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

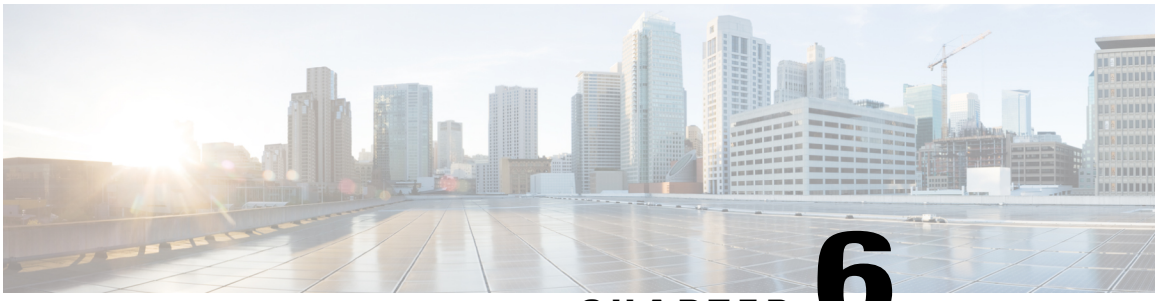
Step 3 Perform one of the following tasks:

- Click the radio button next to the service that you want to start, and then click **Start**. The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to stop, and then click **Stop**. The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to restart, and then click **Restart**. A message indicates that restarting may take a while. Click **OK**.
- Click **Refresh** to get the latest status of the services.
- To go to the **Service Activation** window or to the other Control Center window, choose an option from the Related Links drop-down list, and then click **Go**.

Start, Stop, and Restart Services Using Command Line Interface

You can start and stop some services through the CLI. For a list of services that you can start and stop through the CLI and for information on how to perform these tasks, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Tip You must start and stop most services from Control Center in the serviceability GUI.



CHAPTER 6

Tools and Reports

- Serviceability Reports Archive, page 93
- CDR Repository Manager, page 113
- Locations, page 118

Serviceability Reports Archive

The Cisco Serviceability Reporter service generates daily reports containing charts that display a summary of the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

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

The reports contain 24-hour data for the previous day. A suffix that is added to the report names shows the date for which Reporter generated them; for example, AlertRep_mm_dd_yyyy.pdf. The Serviceability Reports Archive window uses this date to display the reports for the relevant date only. The reports generate from the data that is present in the log files, with the timestamp for the previous day. The system considers log files for the current date and the previous two days for collecting data.

The time that is shown in the report reflects the server "System Time."

You can retrieve log files from the server while you are generating reports.

Note The Cisco Unified Reporting web application provides snapshot views of data into one output and runs data checks. The application also allows you to archive generated reports. See the *Cisco Unified Reporting Administration Guide* for more information.

Serviceability Report Archive Considerations for Cluster Configurations

This section applies to Cisco Unified Communications Manager and IM and Presence Service only.

- Because the Cisco Serviceability Reporter is only active on the first server, at any time, Reporter generates reports only on the first server, not the other servers.

- The time that is shown in the report reflects the first server “System Time.” If the first server and subsequent servers are in different time zones, the first server “System Time” shows in the report.
- The time zone differences between the server locations in a cluster are taken into account when data is collected for the reports.
- You can select log files from individual servers or from all servers in the cluster when you generate reports.
- Cisco Unified Reporting web application output and data checks include cluster data from all accessible servers.

Serviceability Reporter Service Parameters

Cisco Serviceability Reporter uses the following service parameters:

- RTMT Reporter Designated Node - Specifies the designated node on which RTMT Reporter runs. This default equals the IP address of the server on which the Cisco Serviceability Reporter service is first activated.

  Cisco Unified Communications Manager only: Because the Serviceability Reporter service is CPU intensive, Cisco recommends that you specify a non-call-processing node.
- Report Generation Time - Specifies the number of minutes after midnight. Reports are generated at this time for the most recent day. The minimum value equals 0 and the maximum value equals 1439.
- Report Deletion Age - Specifies the number of days that the report must be kept on the disk. The system deletes reports that are older than the specified age. The minimum value equals 0, and the maximum value equals 30.

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

For more information about service parameter configuration, see the following guides:

- Cisco Unified Communications Manager only: *System Configuration Guide for Cisco Unified Communications Manager*
- Connection only: *System Administration Guide for Cisco Unity Connection*

Note Cisco Unified Communications Manager only: If a node is removed completely from the network and does not appear in the list of servers in Cisco Unified Communications Manager Administration, Reporter does not include that node when it generates reports, even if the log file contains the data for that node.

Device Statistics Report

The Device Statistics Report does not apply to IM and Presence Service and Cisco Unity Connection.

The Device Statistics Report provides the following line charts:

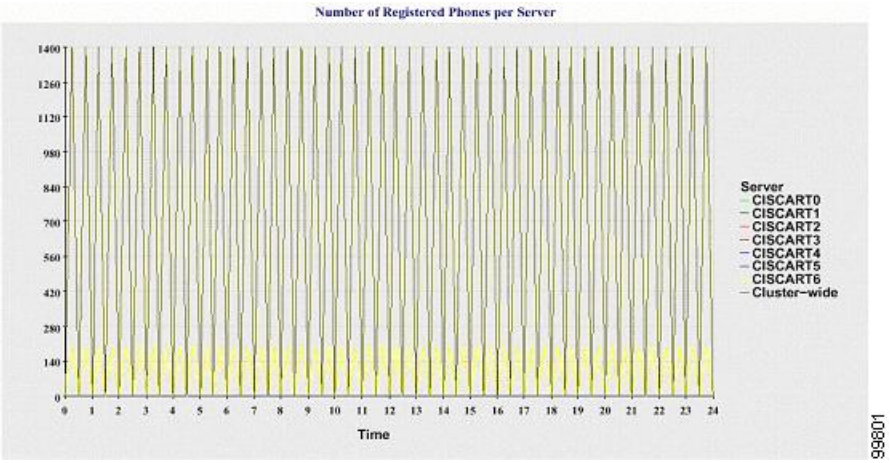
- Number of Registered Phones per Server
- Number of H.323 Gateways in the Cluster
- Number of Trunks in the Cluster

Number of Registered Phones Per Server

A line chart displays the number of registered phones for each Cisco Unified Communications Manager server (and cluster in a Cisco Unified Communications Manager cluster configuration). Each line in the chart represents the data for a server for which data is available, and one extra line displays the clusterwide data (Cisco Unified Communications Manager clusters only). Each data value in the chart represents the average number of phones that are registered for a 15-minute duration. If a server shows no data, Reporter does not generate the line that represents that server. If no data exists for the server (or for all servers in a Cisco Unified Communications Manager cluster configuration), for registered phones, Reporter does not generate the chart. The message "No data for Device Statistics report available" displays.

The following figure shows an example of a line chart representing the number of registered phones per Cisco Unified Communications Manager server in a Cisco Unified Communications Manager cluster configuration.

Figure 1: Line Chart That Depicts Number of Registered Phones Per Server

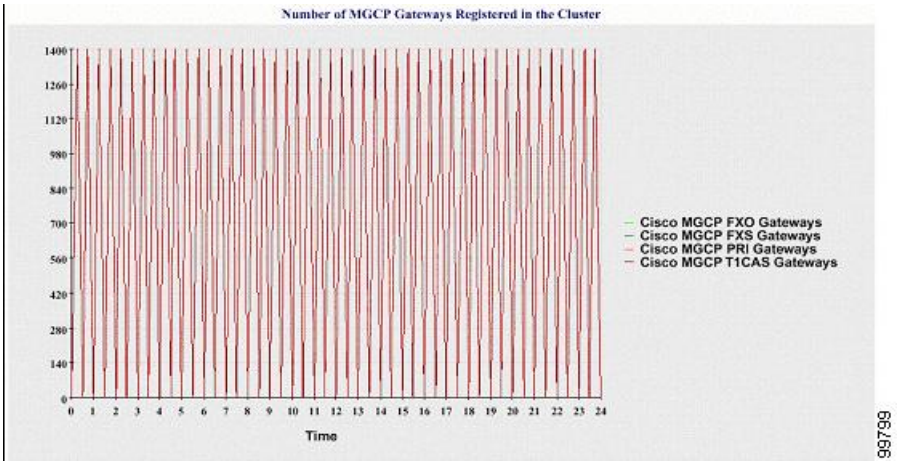


Number of MGCP Gateways Registered in the Cluster

A line chart displays the number of registered MGCP FXO, FXS, PRI, and T1CAS gateways. Each line represents data only for the Cisco Unified Communications Manager server (or cluster in a Cisco Unified Communications Manager cluster configuration); so, four lines show server (or clusterwide) details for each gateway type. Each data value in the chart represents the average number of MGCP gateways that are registered for a 15-minute duration. If no data exists for a gateway for the server (or all the servers in a cluster), Reporter does not generate the line that represents data for that particular gateway. If no data exists for all gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

The following figure shows an example of a line chart representing the number of registered gateways per cluster, in a Cisco Unified Communications Manager cluster configuration.

Figure 2: Line Chart That Depicts Number of Registered Gateways Per Cluster

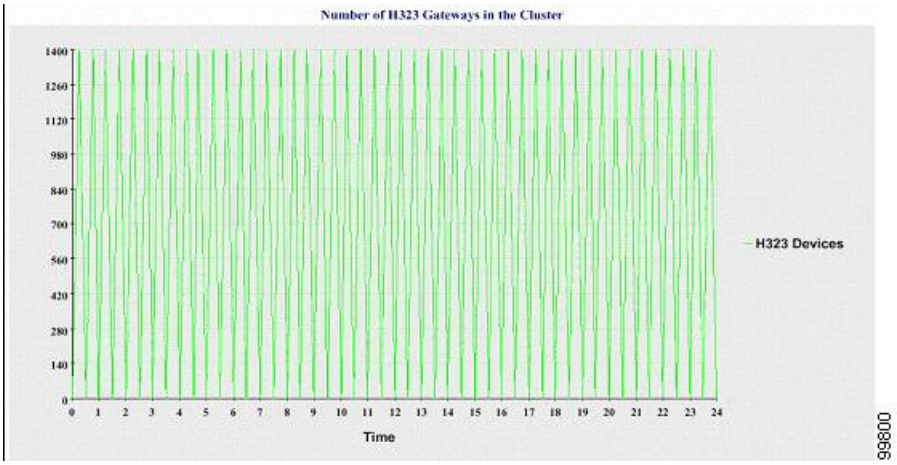


Number of H.323 Gateways in the Cluster

A line chart displays the number of H.323 gateways. One line represents the details of the H.323 gateways (or the clusterwide details in a Cisco Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 gateways for a 15-minute duration. If no data exists for H.323 gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

The following figure shows an example line chart representing the number of H.323 gateways per cluster in a Cisco Unified Communications Manager cluster configuration.

Figure 3: Line Chart That Depicts Number of Registered H.323 Gateways Per Cluster



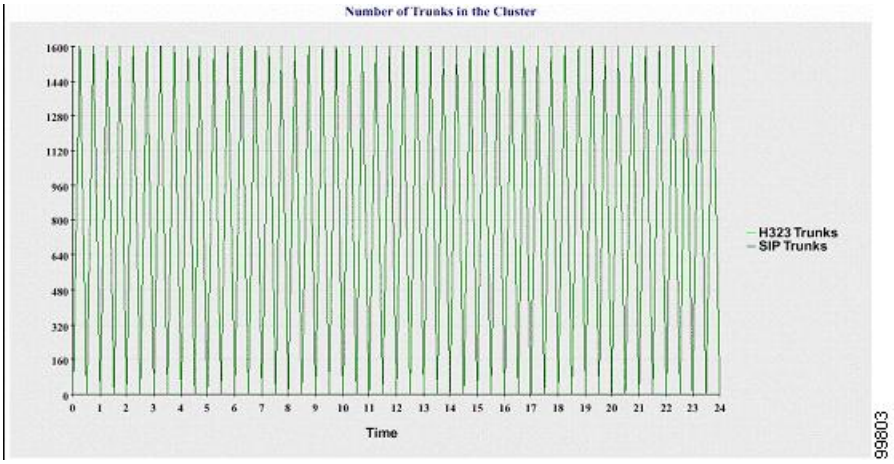
Number of Trunks in the Cluster

A line chart displays the number of H.323 and SIP trunks. Two lines represent the details of the H.323 trunks and SIP trunks (or the clusterwide details in a Cisco Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 and SIP trunks for a 15-minute duration.

If no data exists for H.323 trunks for the server (or for all servers in a cluster), Reporter does not generate the line that represents data for the H.323 trunks. If no data exists for SIP trunks for the server (or for all servers in the cluster), Reporter does not generate the line that represents data for SIP trunks. If no data exists for trunks at all, Reporter does not generate the chart.

The following figure shows an example line chart representing the number of trunks per cluster in a Cisco Unified Communications Manager cluster configuration.

Figure 4: Line Chart That Depicts Number of Trunks Per Cluster



The server (or each server in the cluster) contains log files that match the filename pattern DeviceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Number of registered phones on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of registered MGCP FXO, FXS, PRI, and T1CAS gateways on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of registered H.323 gateways on the server (or on each server in a Cisco Unified Communications Manager cluster)
- Number of SIP trunks and H.323 trunks

Server Statistics Report

The Server Statistics Report provides the following line charts:

- Percentage of CPU per Server
- Percentage of Memory Usage per Server
- Percentage of Hard Disk Usage of the Largest Partition per Server

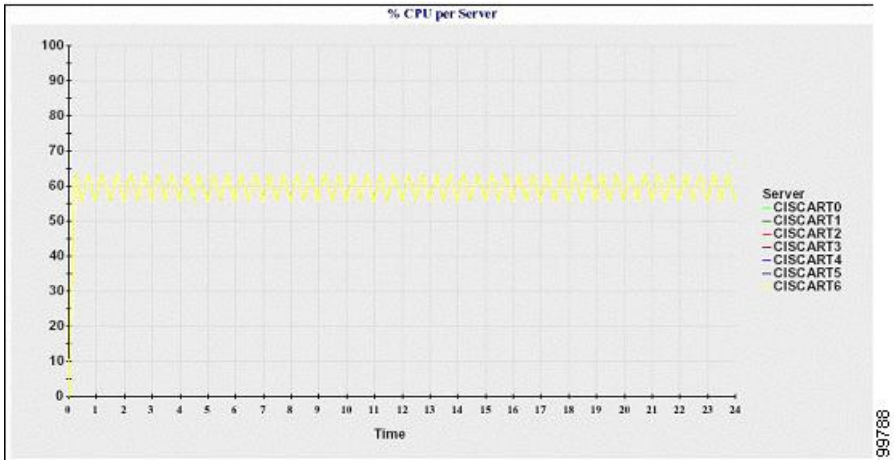
Cluster-specific statistics are only supported by Cisco Unified Communications Manager and IM and Presence Service.

Percentage of CPU Per Server

A line chart displays the percentage of CPU usage for the server (or for each server in a cluster). The line in the chart represents the data for the server (or one line for each server in a cluster) for which data is available. Each data value in the chart represents the average CPU usage for a 15-minute duration. If no data exists for the server (or for any one server in a cluster), Reporter does not generate the line that represents that server. If there are no lines to generate, Reporter does not create the chart. The message "No data for Server Statistics report available" displays.

The following figure shows a line chart example representing the percentage of CPU usage per server in a Cisco Unified Communications Manager cluster configuration.

Figure 5: Line Chart That Depicts the Percentage of CPU Per Server

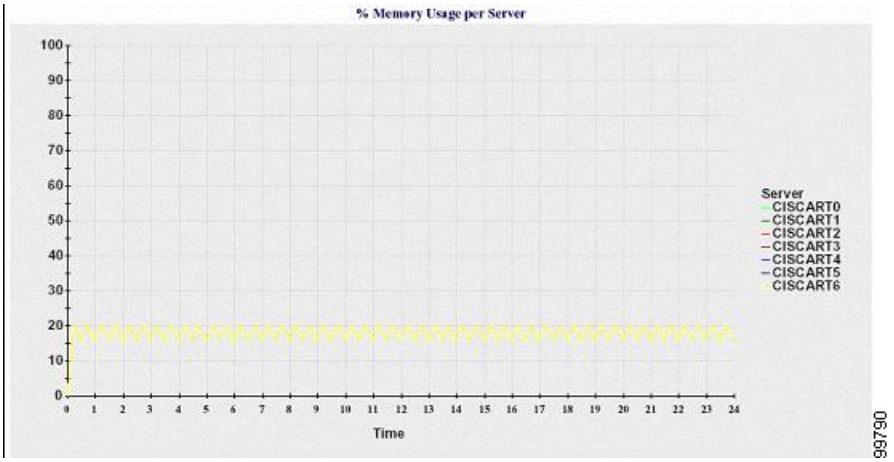


Percentage of Memory Usage Per Server

A line chart displays the percentage of Memory Usage for the Cisco Unified Communications Manager server (%MemoryInUse). In a Cisco Unified Communications Manager cluster configuration, there is one line per server in the cluster for which data is available. Each data value in the chart represents the average memory usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any server in a cluster configuration, Reporter does not generate the line that represents that server.

The following figure shows a line chart example representing the percentage of memory usage per Cisco Unified Communications Manager server in a cluster configuration.

Figure 6: Line Chart That Depicts Percentage of Memory Usage Per Server

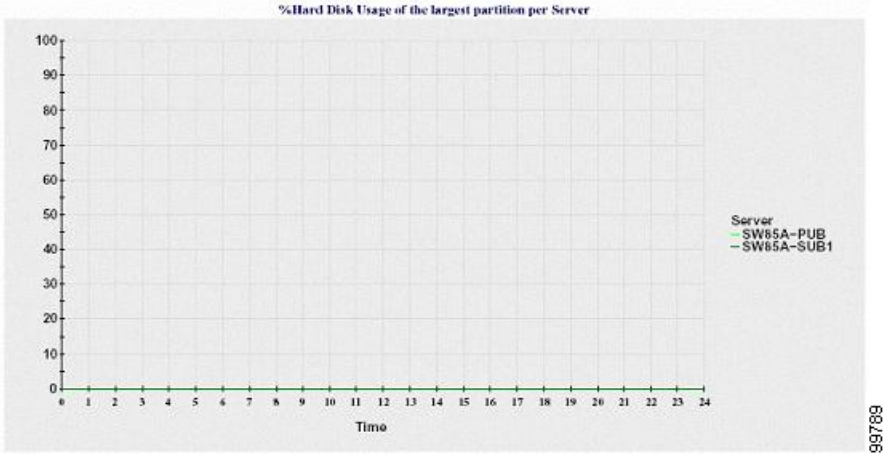


Percentage of Hard Disk Usage of the Largest Partition Per Server

A line chart displays the percentage of disk space usage for the largest partition on the server (%DiskSpaceInUse), or on each server in a cluster configuration. Each data value in the chart represents the average disk usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a cluster configuration, Reporter does not generate the line that represents that server.

The following figure shows a line chart example representing the percentage of hard disk usage for the largest partition per server in a Cisco Unified Communications Manager cluster configuration.

Figure 7: Line Chart That Depicts Percentage of Hard Disk Usage of the Largest Partition Per Server



The server (or each server in a cluster configuration) contains log files that match the filename pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Percentage of CPU usage on the server (or each server in a cluster)

- Percentage of Memory usage (%MemoryInUse) on the server (or on each server in a cluster)
- Percentage of Hard disk usage of the largest partition (%DiskSpaceInUse) on the server (or on each server in a cluster)

Service Statistics Report

The Service Statistics Report does not support IM and Presence Service and Cisco Unity Connection.

The Service Statistics Report provides the following line charts:

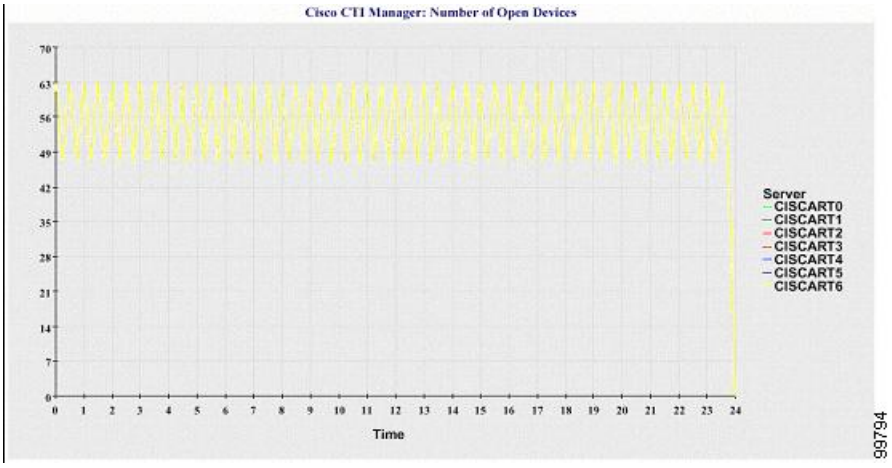
- Cisco CTI Manager: Number of Open Devices
- Cisco CTI Manager: Number of Open Lines
- Cisco TFTP: Number of Requests
- Cisco TFTP: Number of Aborted Requests

Cisco CTI Manager: Number of Open Devices

A line chart displays the number of CTI Open Devices for the CTI Manager (or for each CTI Manager in a Cisco Unified Communications Manager cluster configuration). Each line chart represents the data for the server (or on each server in a Cisco Unified Communications Manager cluster) on which service is activated. Each data value in the chart represents the average number of CTI open devices for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server. The message “No data for Service Statistics report available” displays.

The following figure shows a line chart example representing the number of open devices per Cisco CTI Manager in a Cisco Unified Communications Manager cluster configuration.

Figure 8: Line Chart That Depicts Cisco CTI Manager: Number of Open Devices



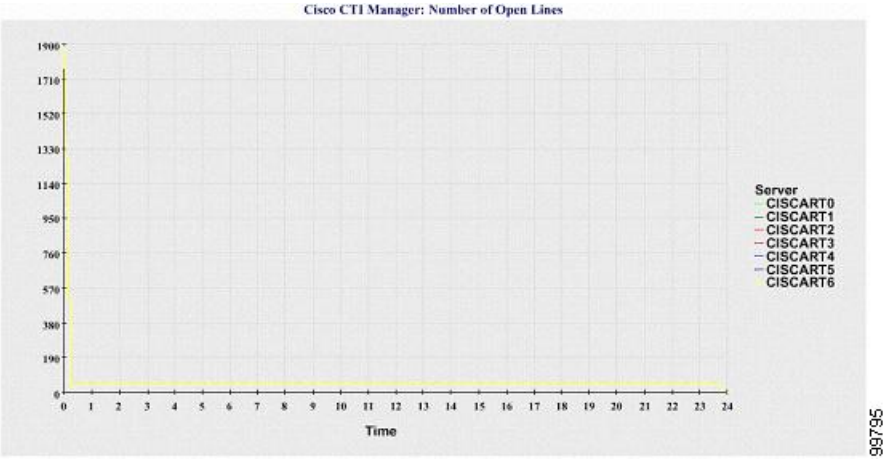
Cisco CTI Manager: Number of Open Lines

A line chart displays the number of CTI open lines for the CTI Manager (or per CTI Manager in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server

(or one line for each server in a Cisco Unified Communications Manager cluster configuration) where the Cisco CTI Manager service is activated. Each data value in the chart represents the average number of CTI open lines for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

The followings figure shows a line chart example representing the number of open lines per Cisco CTI Manager in a Cisco Unified Communications Manager cluster configuration.

Figure 9: Line Chart That Depicts Cisco CTI Manager: Number of Open Lines

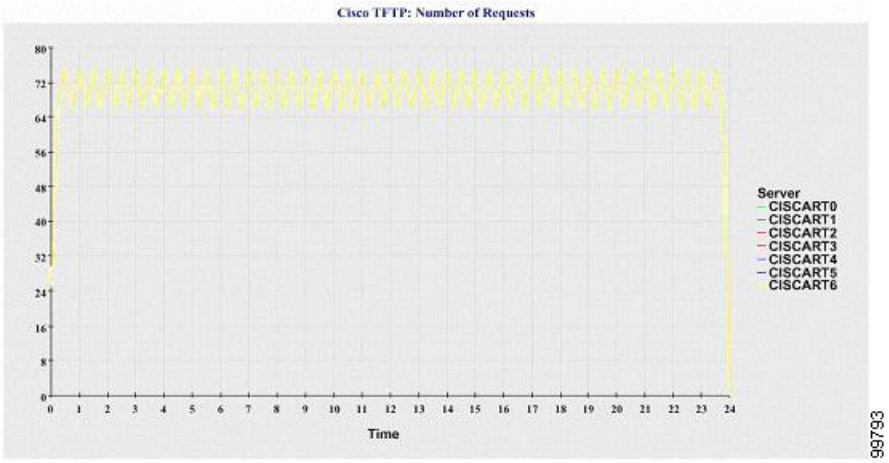


Cisco TFTP: Number of Requests

A line chart displays the number of Cisco TFTP requests for the TFTP server (or per TFTP server in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the average number of TFTP requests for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

The following figure shows a line chart example representing the number of Cisco TFTP requests per TFTP server.

Figure 10: Line Chart That Depicts Cisco TFTP: Number of Requests

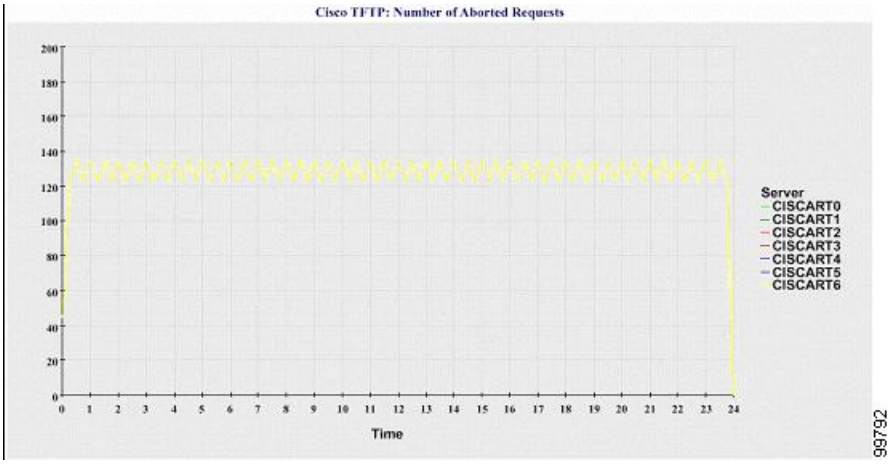


Cisco TFTP: Number of Aborted Requests

A line chart displays the number of Cisco TFTP requests that were aborted for the TFTP server (or per TFTP server in a Cisco Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Cisco Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the average of TFTP requests that were aborted for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Cisco Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

The following figure shows a line chart example that represents the number of Cisco TFTP requests that were aborted per TFTP server.

Figure 11: Line Chart That Depicts Cisco TFTP: Number of Aborted Requests



The server (or each server in a Cisco Unified Communications Manager cluster) contains log files that match the filename pattern ServiceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- For each CTI Manager - Number of open devices
- For each CTI Manager - Number of open lines
- For each Cisco TFTP server - TotalTftpRequests
- For each Cisco TFTP server - TotalTftpRequestsAborted

Call Activities Report

The Call Activities Report does not support IM and Presence Service and Cisco Unity Connection.

The Call Activities Report provides the following line charts:

- Cisco Unified Communications Manager Call Activity for a cluster
- H.323 Gateways Call Activity for the Cluster
- MGCP Gateways Call Activity for the Cluster
- MGCP Gateways
- Trunk Call Activity for the Cluster

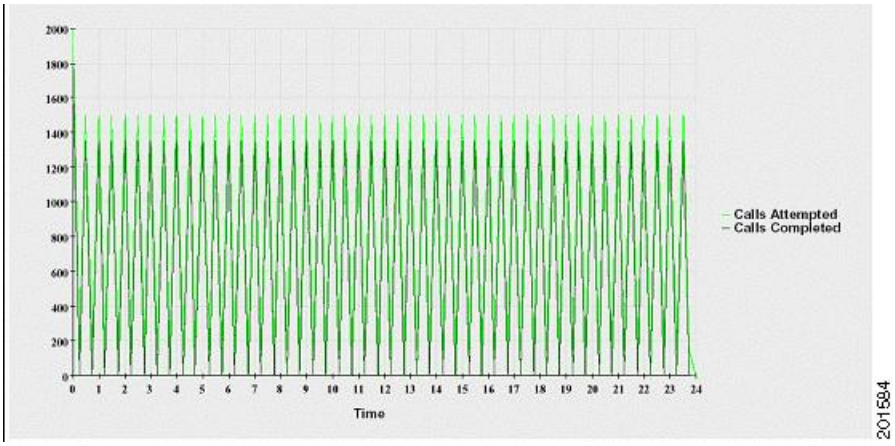
Cisco Unified Communications Manager Call Activity for the Cluster

A line chart displays the number of Cisco Unified Communications Manager calls that were attempted and calls that were completed. In a Cisco Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration.

If no data exists for Cisco Unified Communications Manager calls that were completed, Reporter does not generate the line that represents data for the calls that were completed. If no data exists for Cisco Unified Communications Manager calls that were attempted, Reporter does not generate the line that represents data for the calls that were attempted. In a Cisco Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for Cisco Unified Communications Manager call activities at all, Reporter does not generate the chart. The message “No data for Call Activities report available” displays.

The following figure shows a line chart representing the number of attempted and completed calls for a Cisco Unified Communications Manager cluster.

Figure 12: Line Chart That Depicts Cisco Unified Communications Manager Call Activity for a Cluster

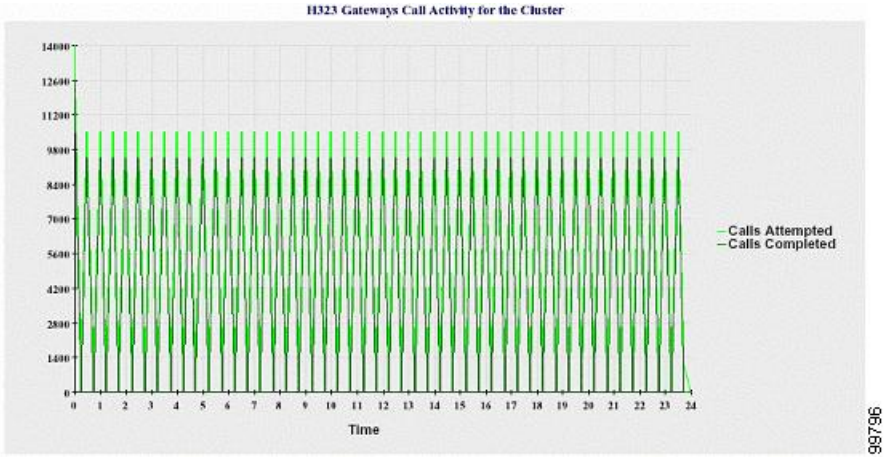


H.323 Gateways Call Activity for the Cluster

A line chart displays the number of calls that were attempted and calls that were completed for H.323 gateways. In a Cisco Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which equals the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration. If no data exists for H.323 gateways calls that were completed, Reporter does not generate the line that represents data for calls that were completed. If no data exists for H.323 gateways calls that were attempted, Reporter does not generate the line that represents data for calls that were attempted. In a Cisco Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for H.323 gateways call activities at all, Reporter does not generate the chart.

The following figure shows a line chart representing the H.323 gateway call activity for a Cisco Unified Communications Manager cluster.

Figure 13: Line Chart That Depicts H.323 Gateways Call Activity for the Cluster

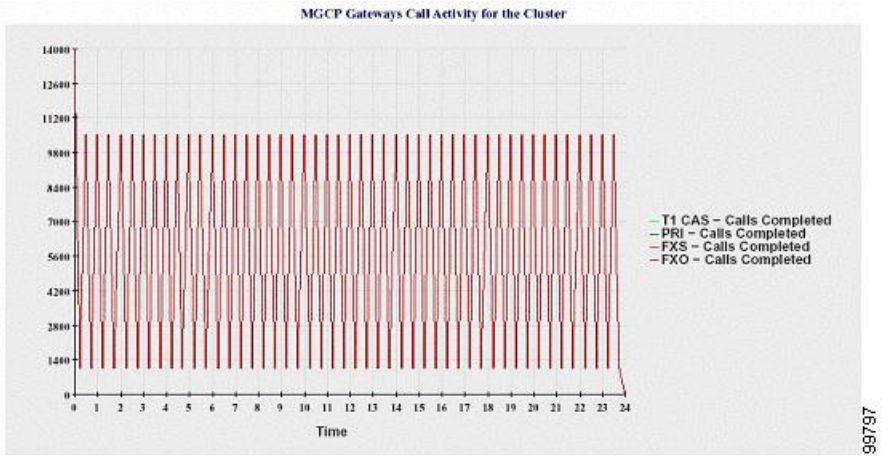


MGCP Gateways Call Activity for the Cluster

A line chart displays the number of calls that were completed in an hour for MGCP FXO, FXS, PRI, and T1CAS gateways. In a Cisco Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed for the entire Cisco Unified Communications Manager cluster. The chart comprises four lines at the most, one for the number of calls that were completed for each of the gateway types (for which data is available). Each data value in the chart represents the total number of calls that were completed for a 15-minute duration. If no data exists for a gateway, Reporter does not generate the line that represents data for calls that were completed for a particular gateway. If no data exists for all gateways, Reporter does not generate the chart.

The following figure shows a line chart representing the MGCP gateways call activity for a Cisco Unified Communications Manager cluster.

Figure 14: Line Chart That Depicts MGCP Gateways Call Activity for the Cluster

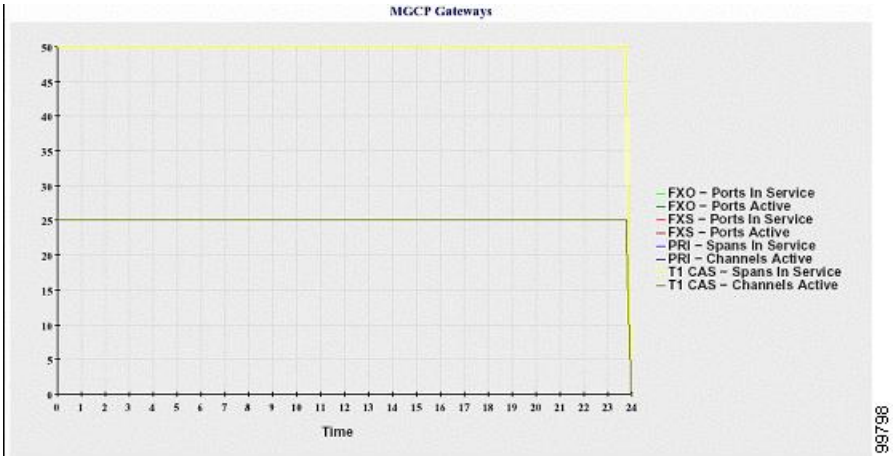


MGCP Gateways

A line chart displays the number of Ports In Service and Active Ports for MGCP FXO, FXS gateways and the number of Spans In Service or Channels Active for PRI, T1CAS gateways. For a Cisco Unified Communications Manager cluster configuration, the chart displays the data for the entire Cisco Unified Communications Manager cluster. The chart comprises eight lines, two lines each for the number of Ports In Service for MGCP FXO and FXS, and two lines each for the number of Active Ports for MGCP FXO and FXS. Four more lines for the number of Spans In Service and Channels Active for PRI and T1CAS gateways exist. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all servers in the cluster (for which data is available). Each data value in the chart represents the total Number of Ports In Service, Number of Active Ports, Spans In Service or Channels Active for a 15-minute duration. If no data exists for the number of Spans In Service or the Channels Active for a gateway (MGCP PRI, T1CAS) for all servers, Reporter does not generate the line that represents data for that particular gateway.

The following figure shows a line chart representing the MGCP gateways.

Figure 15: Line Chart That Depicts MGCP Gateways

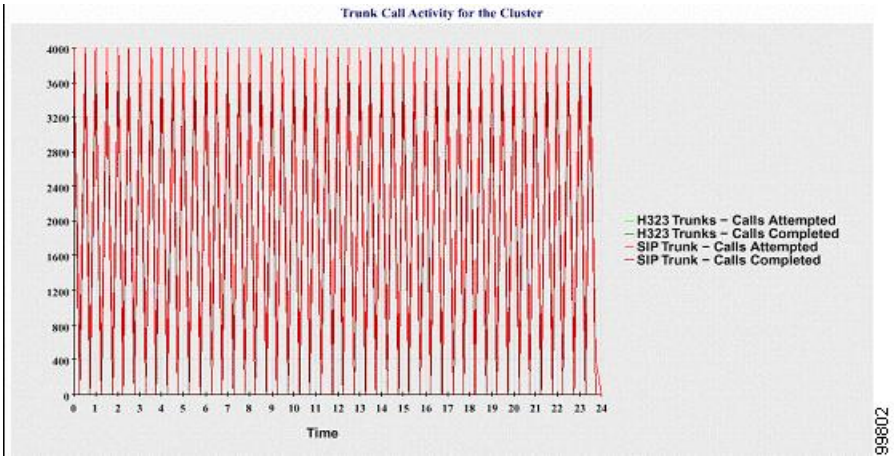


Trunk Call Activity for the Cluster

A line chart displays the number of calls that were completed and calls that were attempted in an hour for SIP trunk and H.323 trunk. For a Cisco Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed and calls that were attempted for the entire Cisco Unified Communications Manager cluster. The chart comprises four lines, two for the number of calls that were completed for each SIP and H.323 trunk (for which data is available) and two for the number of calls that were attempted. For a Cisco Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all nodes in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were completed or number of calls that were attempted for a 15-minute duration. If no data exists for a trunk, Reporter does not generate the line that represents data for the calls that were completed or the calls that were attempted for that particular trunk. If no data exists for both trunk types, Reporter does not generate the chart.

The following figure shows a line chart representing the trunk call activity for a Cisco Unified Communications Manager cluster.

Figure 16: Line Chart That Depicts Trunk Call Activity for the Cluster



The server (or each server in a Cisco Unified Communications Manager cluster configuration) contains log files that match the filename pattern CallLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Calls that were attempted and calls that were completed for Cisco Unified Communications Manager (or for each server in a Cisco Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for the H.323 gateways (or for the gateways in each server in a Cisco Unified Communications Manager cluster)
- Calls that were completed for the MGCP FXO, FXS, PRI, and T1CAS gateways (or for the gateways in each server in a Cisco Unified Communications Manager cluster)
- Ports in service, active ports for MGCP FXO and FXS gateways and spans in service, channels active for PRI, and T1CAS gateways (in each server in a Cisco Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for H.323 trunks and SIP trunks

Alert Summary Report

The Alert Summary Report provides the details of alerts that are generated for the day.

Cluster-specific statistics are supported only by Cisco Unified Communications Manager and IM and Presence Service.

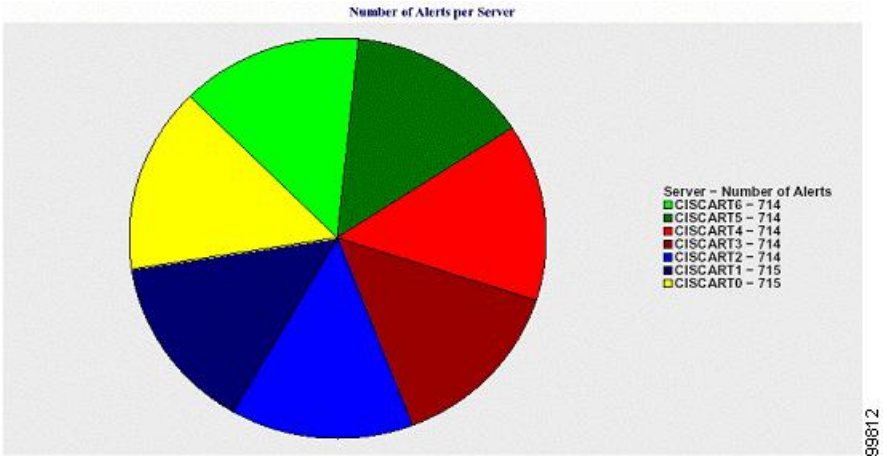
Number of Alerts Per Server

A pie chart provides the number of alerts per node in a cluster. The chart displays the serverwide details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated for a particular server in the cluster. The chart includes as many number of sectors as there are servers (for which Reporter generates alerts in the day) in the cluster. If no data exists for a server, no sector in the chart represents that server. If no data exists for all servers, Reporter does not generate the chart. The message “No alerts were generated for the day” displays.

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

The following chart shows a pie chart example that represents the number of alerts per server in a Cisco Unified Communications Manager cluster.

Figure 17: Pie Chart That Depicts Number of Alerts Per Server

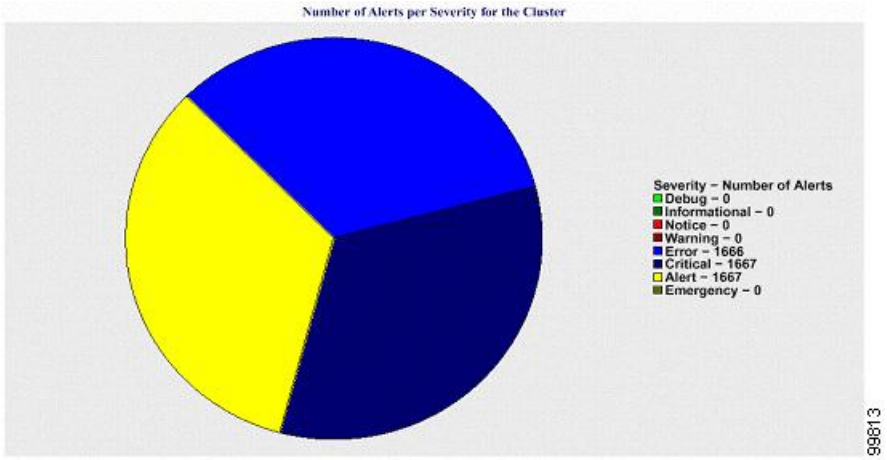


Number of Alerts Per Severity for the Cluster

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

The following chart shows a pie chart example that represents the number of alerts per severity for a Cisco Unified Communications Manager cluster.

Figure 18: Pie Chart That Depicts Number of Alerts Per Severity for the Cluster

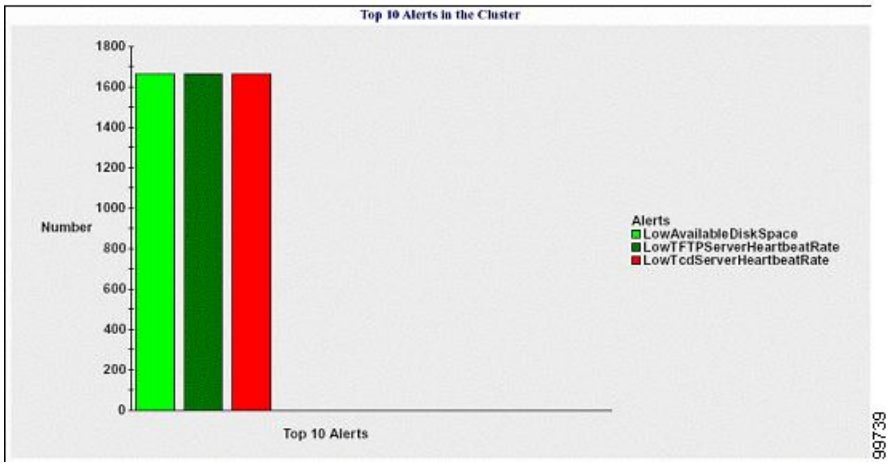


Top Ten Alerts in the Cluster

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

The following chart shows a bar chart example that represents the top ten alerts in a Cisco Unified Communications Manager cluster.

Figure 19: Bar Chart That Depicts Top 10 Alerts in the Cluster



The server (or each server in a cluster) contains log files that match the filename pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

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

Performance Protection Report

The Performance Protection Report does not support IM and Presence Service and Cisco Unity Connection.

The Performance Protection Report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

The Performance Protection Report provides trend analysis information on default monitoring objects for the last seven that allows you to track information about Cisco Intercompany Media Engine. The report includes the Cisco IME Client Call Activity chart that shows the total calls and fallback call ratio for the Cisco IME client.

The Performance Protection report comprises the following charts:

- Cisco Unified Communications Manager Call Activity
- Number of registered phones and MGCP gateways
- System Resource Utilization
- Device and Dial Plan Quantities

Cisco Unified Communications Manager Call Activity

A line chart displays the hourly rate of increase or decrease for number of calls that were attempted and calls that were completed as the number of active calls. For a Cisco Unified Communications Manager cluster configuration, the data is charted for each server in the cluster. The chart comprises three lines, one for the number of calls that were attempted, one for the calls that were completed, and one for the active calls. If no data exists for call activity, Reporter does not generate the chart.

Number of Registered Phones and MGCP Gateways

A line chart displays the number of registered phones and MGCP gateways. For a Cisco Unified Communications Manager cluster configuration, the chart displays the data for each server in the cluster.The chart comprises two lines, one for the number of registered phones and another for the number of MGCP gateways. If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

System Resource Utilization

A line chart displays the CPU load percentage and the percentage of memory that is used (in bytes) for the server (or for the whole cluster in a Cisco Unified Communications Manager cluster configuration). The chart comprises two lines, one for the CPU load and one for the memory usage. In a Cisco Unified Communications Manager cluster, each line represents the cluster value, which is the average of the values for all the servers in the cluster (for which data is available). If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

Device and Dial Plan Quantities

Two tables display information from the Cisco Unified Communications Manager database about the numbers of devices and number of dial plan components. The device table shows the number of IP phones, Cisco Unity Connection ports, H.323 clients, H.323 gateways, MGCP gateways, MOH resources, and MTP resources. The dial plan table shows the number of directory numbers and lines, route patterns, and translation patterns.

Set Up Serviceability Reports Archive Overview

The following steps provide information for configuring the serviceability report archive feature.

Procedure

Step 1 Activate the Cisco Serviceability Reporter service.

Step 2 Configure the Cisco Serviceability Reporter service parameters.

Step 3 View the reports that the Cisco Serviceability Reporter service generates.

Related Topics

Activate Feature Services, on page 90
Serviceability Reporter Service Parameters, on page 94

Set Up Serviceability Reports Archive

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

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

Before You Begin

Activate the Cisco Serviceability Reporter service, which is CPU intensive. After you activate the service, report generation may take up to 24 hours.

Cisco Unified Communications Manager only: Cisco recommends that you activate the service on a non-call-processing server.

Procedure

Step 1 Choose **Tools** > **Serviceability Reports Archive**.
The Serviceability Reports Archive window displays the month and year for which the reports are available.

Step 2 From the Month-Year pane, choose the month and year for which you want to display reports.
A list of days that correspond to the month displays.

Step 3 To view reports, click the link that corresponds to the day for which reports were generated.
The report files for the day that you chose display.

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

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

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

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

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

Access to Serviceability Reports Archive

Activate Serviceability Reports Archive

Procedure

Step 1 Select **Tools** > **Service Activation**.
Step 2 Select the required server from the **Server** list box, and then select **Go**.
Step 3 Navigate to the **Performance and Monitoring** services pane.
Step 4 Check the **Cisco Serviceability Reporter** service checkbox, and then select **Save**.
Step 5 Select **Tools** > **Control Center - Feature Services**.
Step 6 Select the required server from the **Server** list box, and then select **Go**.
Step 7 Navigate to the **Performance and Monitoring** services pane and locate the Cisco Serviceability Reporter.
Step 8 Verify that the status of the Cisco Serviceability Reporter is Started and Activated. If the Cisco Serviceability Reporter is not running, select the Cisco Serviceability Reporter and select **Start**.

What to Do Next

If you opened Cisco Unified IM and Presence Serviceability by entering the server name in the browser, you must sign in to Cisco Unified IM and Presence Serviceability before you can view the report.

The Cisco Unified IM and Presence Serviceability service generates reports only on the first node, even if you turn on the service on other nodes.

Access Serviceability Reports Archive

Before You Begin

Activate the Cisco Serviceability Reporter service. After you activate the service, report generation may take up to 24 hours.

Procedure

Step 1 Select **Tools** > **Serviceability Reports Archive**.
Step 2 Select the month and year for which you want to display reports in the **Month-Year** section.
Step 3 Select the link that corresponds to the day for which reports were generated to view the required report.
Step 4 Select the link of the report that you want to view to view a particular PDF report.
The section in the Trace Filter Settings area that relates to devices is not relevant to IM and Presence.

Tip If you opened Cisco Unified IM and Presence Serviceability by entering the server name in the browser, you must sign in to Cisco Unified IM and Presence Serviceability before you can view the report.

CDR Repository Manager

This section does not apply to IM and Presence Service.

Use the CDR Management Configuration window to set the amount of disk space to allocate to call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs. The CDR Repository Manager service repeatedly attempts to deliver CDR and CMR files to the billing servers that you configure in the CDR Management Configuration window until it delivers the files successfully, until you change or delete the billing application server on the CDR Management Configuration window, or until the files fall outside the preservation window and are deleted.

Note To access the Enterprise Parameters Configuration window, open Cisco Unified Communications Manager Administration and choose **System** > **Enterprise Parameters**. The **CDR File Time Interval** parameter specifies the time interval for collecting CDR data. For example, if this value is set to 1, each file will contain 1 minute of CDR data (CDRs and CMRs, if enabled). The external billing server and CAR database will not receive the data in each file until the interval has expired, so consider how quickly you want access to the CDR data when you decide what interval to set for this parameter. For example, setting this parameter to 60 means that each file will contain 60 minutes worth of data, but that data will not be available until the 60-minute period has elapsed, and the records are written to the CAR database. and the CDR files are sent to the configured billing servers. The default value equals 1. The minimum value specifies 1, and the maximum value specifies 1440. The unit of measure for this required field represents a minute.

Both the CDR Agent and the CDR Repository Manager process files with an interval that is independent of the CDR File Time Interval. The CDR Repository Manager sends all existing CDR files to the billing application servers, sleeps for 6 seconds before checking the new files to send, and continues that 6-second interval. If the destination (the external billing application servers) does not respond, the system attempts the process again by using a doubled length of the sleep interval (12 seconds). Each delivery failure results in double the sleep time (6, 12, 24, 48,and so on, seconds) until 2 minutes occurs, then stays at 2-minute intervals until successful delivery occurs. After successful delivery, the 6-second interval automatically resumes.

Users cannot configure the 6-second processing time, with the sleep time interval doubling in case of failure. Users can configure only the **CDR File Time Interval** enterprise parameter. No alert gets sent after the first file delivery failure. By default, the system generates the CDRFileDeliveryFailed alert after the second delivery failure of the Cisco CDR Repository Manager service to deliver files to any billing application server. You can configure the alert to send you an e-mail or to page you. For information on configuring alerts, see the "Working with Alerts" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

The system generates the CDRFileDeliveryFailureContinues syslog alarm upon subsequent failures to deliver the files to the billing application servers.

The CDR Agent behaves in almost the same manner. First, it sends all the existing CDR files to the publisher. If no additional files to send exist, the CDR Agent sleeps for 6 seconds before checking for new files. Each delivery failure results in the immediate change of the sleep interval to 1 minute, then says at 1-minute intervals until successful delivery. After the first successful delivery of files, the 6-second interval resumes.

The system sends no alert after the first file delivery failure by the CDR Agent. By default, the system generates the CDRAgentSendFileFailed alert after the second delivery failure of the CDR Agent. You can configure the alert to send you an email or to page you. For information on configuring alerts, see the "Working with Alerts" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*

The system generates the CDRAgentSendFileFailedContinues syslog alarm upon subsequent failures to deliver the files.

If you need to start or restart the file transfer timer, you can restart the Cisco CDR Repository Manager or CDR Agent process by going to the Cisco Unified Serviceability window and selecting **Tools** > **Control Center** > **Network Services**.

When you enable the file deletion based on high water mark parameter, the CDR repository manager service monitors the amount of disk space that CDR and CMR files use. If disk usage exceeds the high water mark that you configure, the system purges the CDR and CMR files that have been successfully delivered to all destinations and loaded into the CAR database (if CAR is activated) until the disk space reaches the low water mark or the system deletes all successfully delivered files. If disk usage still exceeds the high water mark after the system deletes all successfully delivered files, it does not delete any more files, unless the disk usage still exceeds the disk allocation that you configure. If the disk usage still exceeds the disk allocation that you configure, the system purges files beginning with the oldest, regardless of whether the files fall within the preservation window or have been successfully delivered, until the disk usage falls below the high water mark.

Note Regardless of whether you enable the deletion of files based on the high water mark parameter, if disk usage exceeds the disk allocation that you configure, the CDR repository manager service deletes CDR and CMR files, beginning with the oldest files, until disk utilization falls below the high water mark.

The Cisco Log Partition Monitoring Tool service monitors the disk usage of CDR and CMR flat files that have not been delivered to the CDR repository manager.

Cisco Unified Communications Manager only: If the disk usage of the log partition on a server exceeds the configured limit and the service has deleted all other log and trace files, the log partition monitor service deletes CDR/CMR files on the subsequent nodes that have not been delivered to the CDR repository manager.

For more information about log partition monitoring, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Set Up General Parameters

To set disk utilization and file preservation parameters for CDRs, perform the following procedure.

Procedure

Step 1 Choose **Tools** > **CDR Management**.
The CDR Management window displays.

Step 2 Click the CDR Manager general parameter value that you want to change.

Step 3 Enter the appropriate CDR Repository Manager general parameter settings.

Step 4 Click **Update**.

Tip At any time, you can click **Set Default** to specify the default values. After you set the defaults, click **Update** to save the default values.

Related Topics

General Parameter Settings, on page 115

General Parameter Settings

The following table describes the available settings in the General Parameters section of the CDR Management Configuration window.

Table 46: CDR Repository Manager General Parameter Settings

Field	Description
Disk Allocation (MB)	Choose the number of megabytes that you want to allocate to CDR and CMR flat file storage. The default disk allocation and range vary depending on the size of the server hard drive. **Note** The maximum CAR database size equals 3328 MB for a Cisco Unified Communications Manager server. If disk usage exceeds the allocated maximum disk space for CDR files, the system generates the CDRMaximumDiskSpaceExceeded alert and deletes all successfully processed files (those delivered to billing servers and loaded to CAR). If disk usage still exceeds the allocated disk space, the system deletes undelivered files and files within the preservation duration, starting with the oldest, until disk utilization falls below the high water mark. If you have a large system and do not allocate enough disk space, the system may delete the CDR and CMR files before the CAR Scheduler loads the files into the CAR database. For example, if you configure the CAR Scheduler to run once a day and you set the disk allocation to a value that is not large enough to hold the CDR and CMR files that are generated in a day, the system will delete the files before they are loaded into the CAR database.
High Water Mark (%)	This field specifies the maximum percentage of the allocated disk space for CDR and CMR files. For example, if you choose 2000 megabytes from the Disk Allocation field and 80% from the High Water Mark (%) field, the high water mark equals 1600 megabytes. In addition to the high water mark percentage, the number of CDRs in the CAR database cannot exceed two million records for a Cisco Unified Communications Manager server. When the disk usage exceeds the percentage that you specify, or the total number of CDRs is exceeded, and the Disable CDR/CMR Files Deletion Based on HWM check box is unchecked, the system automatically purges all successfully processed CDR and CMR files (those delivered to billing servers and loaded to CAR) beginning with the oldest files to reduce disk usage to the amount that you specify in the Low Water Mark (%) drop-down list box. If the disk usage still exceeds the low water mark or high water mark, the system does not delete any undelivered or unloaded files, unless the disk usage exceeds the disk allocation. If you check the Disable CDR/CMR Files Deletion Based on HWM check box, the system does not delete CDRs and CMRs based on the percentage that you specify in this field. **Note** If CDR disk space exceeds the high water mark, the system generates the CDRHWMExceeded alert.

Field	Description
Low Water Mark (%)	This field specifies the percentage of disk space that is allocated to CDR and CMR files that is always available for use. For example, if you choose 2000 megabytes from the Disk Allocation field and 40% from the Low Water Mark (%) field, the low water mark equals 800 megabytes.
CDR / CMR Files Preservation Duration (Days)	Choose the number of days that you want to retain CDR and CMR files. The CDR Repository Manager deletes files that fall outside the preservation window. **Note** If you continuously receive the CDRMaximumDiskSpaceExceeded alarm, you either must increase the disk allocation or lower the number of preservation days.
Disable CDR/CMR Files Deletion Based on HWM	**Note** Regardless of whether you enable the deletion of files based on the high-water mark parameter, if disk usage exceeds the disk allocation that you configure, the maximum database size, or the maximum number of records for your installation, the CDR repository manager service deletes CDR and CMR files, beginning with the oldest files, until disk utilization falls below the high water mark. If you do not want to delete CDRs and CMRs even if disk usage exceeds the percentage that you specify in the High Water Mark (%) field, check this check box. By default, this check box remains unchecked, so the system deletes CDRs and CMRs if disk usage exceeds the high water mark.
CDR Repository Manager Host Name	This field lists the hostname of the CDR repository manager server.
CDR Repository Manager Host Address	This field lists the IP address of the CDR repository manager server.

Set Up Application Billing Servers

Use the following procedure to configure application billing servers to which you want to send CDRs. You can configure up to three billing servers.

Procedure

Step 1 Choose **Tools** > **CDR Management Configuration**.
The CDR Management Configuration window displays.

Step 2 Perform one of the following tasks:

- To add a new application billing server, click the **Add New** button.
- To update an existing application billing server, click the server hostname/IP address.

Step 3 Enter the application billing server parameter settings.

Step 4 Click **Add** or **Update**.

Related Topics

Application Billing Server Parameter Settings, on page 117

Application Billing Server Parameter Settings

The following table describes the available settings in the Billing Application Server Parameters section of the CDR Management Configuration window.

Table 47: Application Billing Server Parameter Settings

Field	Description
Host Name/IP Address	Enter the hostname or IP address of the application billing server to which you want to send CDRs. If you change the value in this field, a prompt asks whether you want to send the undelivered files to the new destination. Perform one of the following tasks: • To deliver the files to the new server, click **Yes**. • To change the server hostname/IP address without sending undelivered files, click **No**. The CDR Management service marks the CDR and CMR files as delivered.
User Name	Enter the username of the application billing server.
Protocol	Choose the protocol, either FTP or SFTP, that you want to use to send the CDR files to the configured billing servers.
Directory Path	Enter the directory path on the application billing server to which you want to send the CDRs. You should end the path that you specify with a "/" or "\", depending on the operating system that is running on the application billing server. **Note** Make sure the FTP user has write permission to the directory.
Password	Enter the password that is used to access the application billing server.

Field	Description
Resend on Failure	When you check the Resend on Failure box, this option informs CDRM to send outdated CDR and CMR files to the billing server after the FTP or SFTP connection is restored. When the box is checked, the Resend on Failure flag is set to True. When the box is not checked, the Resend on Failure flag is set to False. There are several different scenarios that can occur. When the billing server Resend on Failure flag is set to True, all CDR files get moved to the billing server. When the Resend On Failure flag is set to False, CDR files that get generated during shutdown of the billing server get moved to the processed folder, but do not get moved to the billing server. When the Resend on Failure flag gets set to True at the beginning, and then gets changed several times, the result is that the CDR files get moved to the billing server whenever the Resend on Failure box gets checked.
Generate New Key	Click on the **Reset** button to generate new keys and reset the connection to the SFTP server.

Delete Application Billing Servers

Use the following procedure to delete an application billing server.

Procedure

Step 1 Choose **Tools** > **CDR Management**.
The CDR Management Configuration window displays.

Step 2 Check the check box next to the application billing server that you want to delete and click **Delete Selected**.
A message displays that indicates that if you delete this server, any CDR or CMR files that have not been sent to this server will not be delivered to this server and will be treated as successfully delivered files.

Tip When you delete a server, the system does not generate the CDRFileDeliveryFailed alert for the files that are not sent to that server.

Step 3 To complete the deletion, click **OK**.

Locations

This section does not apply to IM and Presence Service.

This section explains the Locations feature (**Tools > Locations**) in Cisco Unified Serviceability. This feature enables an administrator to view details of the configured locations in an enterprise, understand the link and intralocation discrepancies, view effective path between the two locations, and identify disconnected groups of locations.

Locations Topology

Cisco Unified Serviceability Locations Topology provides details of configured locations in your enterprise. Location Topology refers to a modeled topology representing the flow of media in a network.

The following are some commonly used terms and their definitions:

Assertion

An assertion refers to the location and link bandwidth and weight values configured in a cluster. Asserted values may be replicated to another cluster.

Discrepancy

A discrepancy occurs if there is a difference in the location bandwidth values or link bandwidth and weight values asserted across various clusters.

Effective Path

An Effective Path is a sequence of intermediate locations connecting two end locations, with weight assigned to each link between each adjacent pair of locations. The Effective Path, as determined by the least cumulative weight, is the only path used for bandwidth deductions between any two end locations.

View Locations Topology

Cisco Unified Serviceability Locations Topology helps an administrator view the graphical locations topology in a tabular format. The administrator can filter required location names using the **Find** filter. The locations topology data includes the intralocation details and link details for a selected location.
This section describes how to search and view location topology in Cisco Unified Serviceability.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Topology**.
The Locations Topology window appears.

Step 2 From the Find Locations Where Location Name drop-down box, choose the filter criteria.

Step 3 Enter the search string in the Find Locations Where Location Name field and then click **Find**.

Note The Find Locations Where Location Name field is not casesensitive.

The list of locations is displayed for the chosen filter criteria.

Step 4 In the list, click to expand any location to view its intralocation details and link details.
The intralocation details include audio, video, and immersive bandwidth whereas the link details contain the details of the link connecting two locations such as its weight, audio, video and immersive bandwidth.

Tip If the list of locations is long, it may run into multiple pages. To view another page, click the appropriate navigation button at the bottom of the Locations Topology window or enter a page number in the Page field. To change the number of locations that display in the window, choose a different value from the Rows Per Page drop-down box.

Tip If a location is highlighted by a Caution symbol, this indicates a discrepancy. To view the details of this discrepancy, click **View Assertion Details** link.

Step 5 To view the assertion details of any location, click **View Assertion Details** link at the bottom of the expanded details section.

The Assertion Details window appears.

Step 6 To return to the Locations Topology window, click **Close.**

Note To download the locations topology data in XML format, click **Download Topology** at the bottom of the Locations Topology window or **Download Topology** icon in the toolbar at the top.

For more information about the topology data in XML format, see the *Cisco Unified Communications Manager XML Developers Guide*.

View Assertion Details

Use the serviceability GUI to view the following assertion details:

- Intralocation configuration assertions—Includes the intralocation assertion details such as Asserted by Cluster, Audio, Video and Immersive bandwidth. Asserted by Cluster column lists the names of all the clusters that assert a particular location.
- Link assertions—Includes the assertion details of the link that connects two locations, such as Asserted by Cluster, Weight, Audio, Video, and Immersive bandwidth.

Procedure

Step 1 Select **Tools** > **Locations** > **Locations Topology**.

Step 2 Click the **View Assertion Details** link in the **Locations Topology** window.

Locations Discrepancy

The Locations Discrepancy screen displays the conflicts in assertions for various locations configurations.

The following details are displayed:

- Link Configuration Discrepancy—Includes the discrepancy details of the link that connects two locations, such as Weight, Audio, Video and Immersive bandwidth.
- Intralocation Configuration Discrepancy—Includes intralocation discrepancy details such as Audio, Video, and Immersive bandwidth.

View Locations Discrepancy

This section describes how to view a location discrepancy in Cisco Unified Serviceability.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Discrepancy**.

The Location Discrepancy window appears.

Step 2 The list of link configuration discrepancies and intralocation configuration discrepancies is displayed.

Note The Link Configuration Discrepancy section lists only those link names where discrepancy has been detected. Link names are listed in the format *<Location Name 1> <--> <Location Name 2>*. The Intralocation Configuration Discrepancy section lists only those location names where such discrepancy has been detected. The elements in the list are sorted in lexical order.

If no discrepancies are found, the following status message is displayed:

```
No discrepancies found
```

Step 3 In the list, click on a link name or location name to expand and view its configuration details as asserted by different clusters, in a tabular view.

The bottom row displays the effective values considered for audio, video, and immersive bandwidth pools and weight (in the case of links). The values that do not match with the effective values are highlighted in red.

Note The Effective Value is the least of the values in a particular column. For example, the Effective Value of audio bandwidth is the minimum value in the Audio Bandwidth column.

Effective Path

The Cisco Unified Serviceability Effective Path screen provides details of the effective path that media takes for audio, video, or immersive calls made between two locations provided by the administrator. This screen displays the Available bandwidth and the Configured bandwidth across each link and intralocation in the effective path. An administrator can use this report to determine bandwidth availability across a link and intra-location when there are bandwidth issues in making calls. Cisco Unified Serviceability Effective Path can also be used to troubleshoot bandwidth issues in making calls and find out where the bandwidth availability is low.

The Cisco Unified Serviceability Effective Path screen displays the following details between two selected locations:

- Quick Path Overview —Displays the cumulative weight and the least of the configured and available Audio, Video, and Immersive Bandwidth values across the effective path.
- Detailed Path View—Displays the weight and bandwidth values (Available and Configured) for Audio, Video, and Immersive calls for locations and links constituting the effective path, in a tabular view ordered from source location at top to the destination location at bottom.

Note The Available bandwidth values displayed in the report are the value at the time of viewing the Effective Path. You can view the real-time values in the Cisco Unified Real-Time Monitoring Tool.

View Effective Path

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Effective Path**.
The Effective Path window appears.

Step 2 From the **Location** drop-down boxes, select any two locations between which effective path is required and then click **Find.**
Alternatively, start typing the location name in the input box to shortlist the matching location names and then click **Find.**

The effective path details, which include the Quick Path Overview and Detailed Path View sections, are displayed. If there is no path between the two selected locations, the following status message is displayed:

```
No path exists between <From_Location> and <To_Location>.
```

Disconnected Groups

Cisco Unified Serviceability Disconnected Groups screen enables an administrator to view and analyze any disconnect between the locations that are part of the topology. It displays a list of disconnected groups of locations, which helps an administrator understand which locations need to be connected.

The disconnect in the topology can occur when a link between two locations is not configured or a shared location name is misspelled.

Note The Disconnected Groups screen displays and compares only disconnected groups of locations. For information on connecting locations, see topics related to location configuration in *Administration Guide for Cisco Unified Communications Manager*.

View Disconnected Groups

This section describes how to view disconnected groups in Cisco Unified Serviceability.

Procedure

In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Disconnected Groups**.
The Disconnected Groups screen appears.

The following table describes the settings that are displayed on the Disconnected Groups screen.

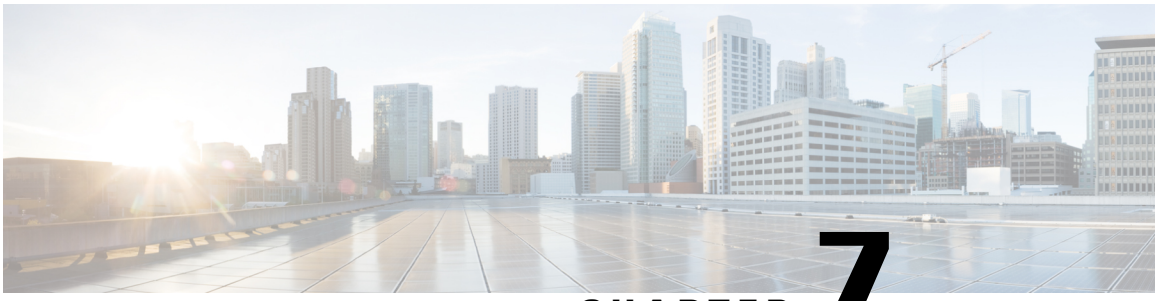
Table 48: Settings on the Disconnected Groups Screen

Setting	Description
List of Disconnected Groups	
Select	Check this box to select a disconnected group to be compared with another disconnected group. **Caution** You can select only two groups for comparison.
Group ID	Auto-generated unique identification number of the selected group is displayed here.
Description	The names of the first and last location (as per the alphabetical order) in the group are displayed here. **Note** If a disconnected group has only one node, only the name of that node is displayed here.
No of Locations	The number of locations in a group is displayed here.
Compare Selected Groups	Click this button to display and compare the selected groups. After you click this button, the details that pertain to the selected groups are displayed. For every group you select, names of the locations that are part of that group and the corresponding clusters that assert a location are displayed. See Comparison view for the selected groups below.
Comparison view for the selected groups	
Location Name	The names of all the locations that are part of a group are listed in this column.
Asserted by Cluster	The names of all the clusters that assert a particular location are listed in this column.

If there are no disconnected groups of locations, the following status message is displayed:

```
No disconnected groups of locations found
```

Note The List of Disconnected Groups can be sorted by any column. By default, the groups are sorted by the No. of Locations column.



CHAPTER 7

Audit Logs

- Audit Logs, page 125

Audit Logs

With audit logging, configuration changes to the system get logged in separate log files for auditing.

Audit Logging (Standard)

When audit logging is enabled, but the detailed audit logging option is not selected, the system is configured for standard audit logging.

With standard audit logging, configuration changes to the system get logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center - Network Services in the serviceability GUI, monitors and logs any configuration changes to the system that are made by a user or as a result of the user action.

You access the **Audit Log Configuration** window in the serviceability GUI to configure the settings for the audit logs.

Standard audit logging contains the following parts:

- Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging.

  The following example displays an API that a Cisco Cisco Unified Communications Manager component can use to send an alarm:

  ```
  User ID: CCMAdministratorClient IP Address: 172.19.240.207
  Severity: 3
  EventType: ServiceStatusUpdated
  ResourceAccessed: CCMService
  EventStatus: Successful
  Description: CallManager Service status is stopped
  ```

- Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is
stopped App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node
ID:sa-cm1-3
```

Tip Be aware that audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed, and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.

Cisco Unified Serviceability Standard Events Logging

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR management. (Cisco Cisco Unified Communications Manager only)
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node. (Cisco Cisco Unified Communications Manager only)

Cisco Unified Real-Time Monitoring Tool Standard Events Loggin

Cisco Unified Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension
- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action
- Clear alert
- Enable alert
- Remove alert action
- Remove alert

Cisco Unified Communications Manager Standard Events Logging

Cisco CDR Analysis and Reporting (CAR) creates audit logs for these events:

- Loader scheduling
- Daily, weekly, and monthly reports scheduling
- Mail parameters configuration
- Dial plan configuration
- Gateway configuration
- System preferences configuration
- Autopurge configuration
- Rating engine configurations for duration, time of day, and voice quality
- QoS configurations
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configuration

Cisco Unified CM Administration Standard Events Logging

The following events get logged for various components of Cisco Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and Cisco Cisco Unified Communications Manager server additions or deletions)

Cisco Unified Communications Self Care Portal Standard Events Logging

User logging (user login and user logout) events are logged for Cisco Unified Communications Self Care Portal.

Command-Line Interface Standard Events Logging

All commands issued via the command-line interface are logged (for both Cisco Cisco Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration Standard Events Logging

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts)
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony
- Task management (enabling or disabling a task)

- Bulk Administration Tool (bulk creates, bulk deletes)
- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA) Standard Events Logging

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts)
- All configuration changes made via the Messaging Assistant

Cisco Unity Connection Serviceability Standard Events Logging

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs Events Logging

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface.

Cisco Unified IM and Presence Serviceability Standard Events Logging

Cisco Unified IM and Presence Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service
- Changes in trace configurations and alarm configurations
- Changes in SNMP configurations
- Review of any report in the Serviceability Reports Archive (this log gets viewed on the reporter node)

Cisco Unified IM and Presence Real-Time Monitoring Tool Standard Events Logging

Cisco Unified IM and Presence Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension
- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action

- Clear alert
- Enable alert
- Remove alert action
- Remove alert

Cisco IM and Presence Administration Standard Events Logging

The following events get logged for various components of Cisco Cisco Unified Communications Manager IM and Presence Administration:

- Administrator logging (logins and logouts on IM and Presence interfaces such as Administration, OS Administration, Disaster Recovery System, and Reporting)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and IM and Presence server additions or deletions)

IM and Presence Application Standard Events Logging

The following events get logged by the various components of the IM and Presence Application:

- End user logging on IM clients (user logins, user logouts, and failed login attempts)
- User entry to and exit from IM Chat Rooms
- Creation and destruction of IM Chat Rooms

Command Line Interface Standard Events Logging

All commands issued through the command line interface are logged.

Audit Logging (Detailed)

Detailed audit logging is an optional feature that logs additional configuration modifications that are not stored in standard (default) audit logs. In addition to all of the information that is stored in standard audit logs, detailed audit logging also includes configuration items that were added, updated, and deleted, including the modified values. Detailed audit logging is disabled by default, but you can enable it in the **Audit Log Configuration** window.

Audit Log Types

System Audit Logs

System audit logs track activities such as the creation, modification, or deletion of Linux OS users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due

to the high volume of data gathered. To enable this function, you must manually enable utils auditd using the CLI. After you have enabled the system audit log feature, you can collect, view, download, or delete selected logs through Trace & Log Central from the Real-Time Monitoring Tool. System audit logs take on the format of `vos-audit.log`.

For information about how to enable this feature, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

Application Audit Logs

The Application Audit logs monitor and record any configuration changes to the system that were made by a user or as a result of the user action.

Note The Application Audit Logs (Linux auditd) can be enabled or disabled only through the CLI. Other than the collection of vos-audit.log through the Real-Time Monitoring Tool, you can not change any settings for this type of audit log.

Database Audit Logs

Database Audit Logs track all activities associated with access to the Informix Database, such as logins.

Audit Log Configuration Task Flow

Complete the following tasks to configure audit logging.

Procedure

	Command or Action	Purpose
Step 1	Set up Audit Logging, on page 131	Set up your audit log configuration in the Audit Log Configuration window. You can configure whether you want to use remote audit logging and whether you want the Detailed Audit Logging option.
Step 2	Configure Remote Audit Log Transfer Protocol, on page 131	Optional. If you have remote audit logging configured, configure the transfer protocol. The system default in normal operating mode is UDP, but you can also configure TCP.
Step 3	Configure Email Server for Alert Notifications, on page 132	Optional. In RTMT, set up the email server for email alerts.
Step 4	Enable Email Alerts, on page 132	Optional. If you have remote audit logging configured with TCP, set up the email notification for the **TCPRemoteSyslogDeliveryFailed** alert.

	Command or Action	Purpose
Step 5	Configure Remote Audit Logging for Platform Logs, on page 133	Set up remote audit logging for platform audit logs and remote server logs. For these types of audit logs, you must configure a FileBeat client and external logstash server.

Set up Audit Logging

Before You Begin

For remote audit logging, you must have already set up your remote syslog server and configured IPSec between each cluster node and the remote syslog server, including connections to any gateways in between. For IPSec configuration, see the *Cisco IOS Security Configuration Guide*.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Audit Log Configuration**.

Step 2 From the **Server** drop-down menu, select any server in the cluster and click **Go**.

Step 3 To log all cluster nodes, check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the **Detailed Audit Logging** check box.

Step 6 Complete the remaining fields in the **Audit Log Configuration** window. For help with the fields and their descriptions, see the online help.

Step 7 Click **Save**.

What to Do Next

Configure Remote Audit Log Transfer Protocol, on page 131

Configure Remote Audit Log Transfer Protocol

Use this procedure to change the transfer protocol for remote audit logs. The system default is UDP , but you can reconfigure to TCP.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

- To configure TCP, run the **utils remotesyslog set protocol tcp** command.

- To configure UDP, run the **utils remotesyslog set protocol udp** command.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Cisco Unified Communications Manager and IM and Presence Service cluster nodes.

What to Do Next

Configure Email Server for Alert Notifications, on page 132

Configure Email Server for Alert Notifications

Use this procedure to set up your email server for alert notifications.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to Do Next

Enable Email Alerts, on page 132

Enable Email Alerts

If you have remote audit logging with TCP configured, use this procedure to set up an email alert for the **TCPRemoteSyslogDeliveryFailed** alert to notify you of transmission failures.

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 In the **Alert Central** window, select **TCPRemoteSyslogDeliveryFailed**.

Step 3 Choose **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 5 In the **Alert Action** popup, **Add** a recipient.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.

Configure Remote Audit Logging for Platform Logs

Complete these tasks to add remote audit logging support for platform audit logs, remote support logs, and Bulk Administration csv files. For these types of logs, the FileBeat client and logstash server get used.

Before You Begin

Make sure that you have set up an external logstash server.

Procedure

	Command or Action	Purpose
Step 1	Configure Logstash Server Information, on page 133	Configure the FileBeat client with the external logstash server details, such as IP addresses, ports and file types.
Step 2	Configure the FileBeat Client, on page 133	Enable the FileBeat client for remote audit logging.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before You Begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and Bulk Administration csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Step 4 Repeat this procedure on each node.
Do not run any of these commands on all nodes simultaneously.

Audit Log Configuration Settings

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, for Cisco Cisco Unified Communications Manager, the CCMAdministrator possesses the audit role after fresh installs and upgrades. The CCMAdministrator can assign any user that has auditing privileges to the Standard Audit Users group in the User Group Configuration window in Cisco Cisco Unified Communications Manager Administration. If you want to do so, you can then remove CCMAdministrator from the Standard Audit Users group.

For IM and Presence Service, the administrator possesses the audit role after fresh installs and upgrades, and can assign any user that has auditing privileges to the Standard Audit Users group.

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, IM and Presence Real-Time Monitoring Tool, Trace Collection Tool, Real-Time Monitoring Tool (RTMT) Alert Configuration, Control Center - Network Services in the serviceability user interface, RTMT Profile Saving, Audit Configuration in the serviceability user interface, and a resource that is called Audit Traces.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified RTMT, Trace Collection Tool, RTMT Alert Configuration, Control Center - Network Services in Cisco Unified Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified Serviceability, and a resource that is called Audit Traces.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified RTMT.

For information on roles, users, and user groups in Cisco Cisco Unified Communications Manager, refer to the *Administration Guide for Cisco Unified Communications Manager*.

For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For information on roles, users, and user groups in IM and Presence, refer to *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

The following table describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability.

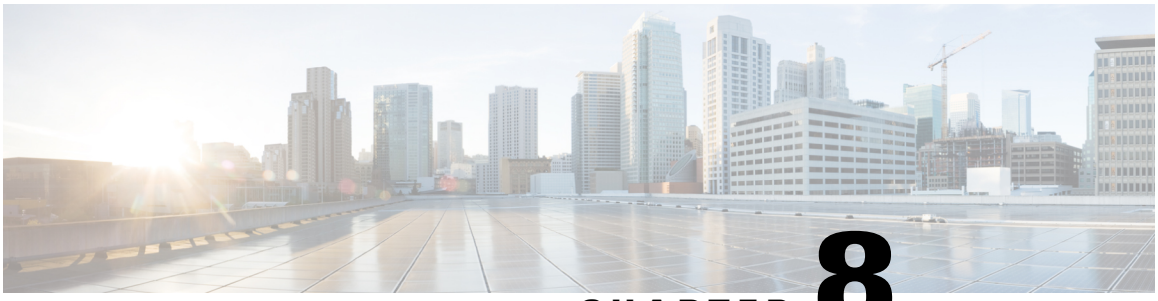
Table 49: Audit Log Configuration Settings

Field	Description
Select Server	
Server	Choose the server (node) where you want to configure audit logs; then, click **Go**.
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to all Nodes** check box.
Application Audit Log Settings	
Enable Audit Log	When you check this check box, an audit log gets created for the application audit log. For Cisco Cisco Unified Communications Manager, the application audit log supports configuration updates for Cisco Cisco Unified Communications Manager user interfaces, such as Cisco Cisco Unified Communications Manager Administration, Cisco Unified RTMT, Cisco Cisco Unified Communications Manager CDR Analysis and Reporting, and Cisco Unified Serviceability. For IM and Presence Service, the application audit log supports configuration updates for IM and Presence user interfaces, such as Cisco Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool, and Cisco Unified IM and Presence Serviceability. For Cisco Unity Connection, the application audit log supports configuration updates for Cisco Unity Connection user interfaces, including Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant, and clients that use the Connection REST APIs. This setting displays as enabled by default. **Note** The Network Service Audit Event Service must be running.
Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the Enable Purging check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central** > **Audit Logs** in RTMT. **Note** The Network Service Cisco Log Partitions Monitoring tool must be running.

Field	Description
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files is reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.
Detailed Audit Logging	When this check box is checked, the system is enabled for detailed audit logs. Detailed audit logs provide the same items as regular audit logs, but also include configuration changes. For example, the audit log includes items that were added, updated, and deleted, including the modified values.
Server Name	Enter the name or IP address of the remote syslog server that you want to use to accept syslog messages. If server name is not specified, Cisco Unified IM and Presence Serviceability does not send the syslog messages. Do not specify a Cisco Cisco Unified Communications Manager node as the destination because the Cisco Cisco Unified Communications Manager node does not accept syslog messages from another server. This applies to IM and Presence Service only.
Remote Syslog Audit Event Level	Select the desired syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to the remote syslog. This applies to IM and Presence Service only.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1 MB and 10 MB. You must specify a number between 1 and 10.
Warning Threshold for Approaching Log Rotation Overwrite (%)	The system can alert you when the audit logs are approaching the level where they will be overwritten. Use this field to set the threshold at which the system sends you an alert. For example, if you use the default settings of 250 files of 2 MB and a warning threshold of 80%, the system sends you an alarm when 200 files (80%) of audit logs have accumulated. If you want to keep the audit history, you can use RTMT to retrieve the logs before the system overwrites them. RTMT provides an option to delete the files after you collect them. Enter a value between 1 and 99%. The default is 80%. When you set this field, you must also check the **Enable Log Rotation** option. **Note** The total disk space allocated to audit logs is the Maximum No. of Files multiplied by the Maximum File Size. If the size of audit logs on the disk exceeds this percentage of total disk space allocated, the system raises an alarm in Alert Central.
Database Audit Log Filter Settings	

Field	Description
Enable Audit Log	When you check this check box, an audit log gets created for the Cisco Cisco Unified Communications Manager and Cisco Unity Connection databases. Use this setting in conjunction with the Debug Audit Level setting, which allows you create a log for certain aspects of the database.
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, choose one of the following options. Be aware that each audit log filter level is cumulative. • **Schema** - Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks** - Tracks all administrative changes to the Cisco Cisco Unified Communications Manager system (for example, any changes to maintain the system) plus all **Schema** changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates** - Tracks all changes to the database plus all **schema** changes and all **administrative tasks** changes. • **Database Reads** - Tracks every read to the system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Cisco Cisco Unified Communications Manager, IM and Presence Service, or Cisco Unity Connection system. This level uses significant amounts of system resources and should be used only for a short time.
Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the Audit Enable Rotation option check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting check box is unchecked, audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the Max No. of Files setting; for example, if you enter 40 in the Maximum No. of Files field, the highest number that you can enter in the No. of Files Deleted on Log Rotation field is 38.

Caution When enabled, database logging can generate large amounts of data in a short period, particularly if the debug audit level is set to **Database Updates** or **Database Reads**. This can result in a significant performance impact during heavy usage periods. In general, we recommend that you keep database logging disabled. If you do need to enable logging to track changes in the database, we recommend that you do so only for short periods of time, by using the **Database Updates** level. Similarly, administrative logging does impact on the overall performance of the web user interface, especially when polling database entries (for example, pulling up 250 devices from the database).



CHAPTER 8

Simple Network Management Protocol

- Simple Network Management Protocol Support, page 139
- SNMP Trace Configuration, page 161
- SNMP V1 and V2c Setup, page 161
- SNMP V3 Setup, page 168
- MIB2 System Group, page 176
- SNMP Trap Settings, page 177

Simple Network Management Protocol Support

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

Note Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information about which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (http://sshwindows.sourceforge.net/)
- Cygwin (http://www.cygwin.com/)
- Titan (http://www.titanftp.com/)

For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

You use the serviceability GUI to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. The SNMP settings that you configure apply to the local node; however, if your system configuration supports clusters, you can apply settings to all servers in the cluster with the "Apply to All Nodes" option in the SNMP configuration windows.

Tip Unified Communications Manager only: SNMP configuration parameters that you specified in Cisco Unified CallManager or Cisco Unified Communications Manager 4.X do not migrate during a Cisco Unified Communications Manager 6.0 and later upgrade. You must perform the SNMP configuration procedures again in Cisco Unified Serviceability.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

SNMP Basics

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

- Managed device - A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  Unified Communications Manager and IM and Presence Service only: In a configuration that supports clusters, the first node in the cluster acts as the managed device.

- Agent - A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

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

The Cisco Unified Communications Manager subagent interacts with the local Cisco Unified Communications Manager only. The Cisco Unified Communications Manager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

The IM and Presence Service subagent interacts with the local IM and Presence Service only. The IM and Presence Service subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- Network Management System (NMS) - An SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. The following NMSs are supported:
  - CiscoWorks LAN Management Solution
  - HP OpenView
  - Third-party applications that support SNMP and Cisco Unified Communications Manager SNMP interfaces

SNMP Management Information Base

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

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

Observe the following limitations:

- Cisco Cisco Unified Communications Manager does not support CISCO-UNITY-MIB.
- Cisco Unity Connection does not support CISCO-CCM-MIB.
- IM and Presence Service does not support CISCO-CCM-MIB and CISCO-UNITY-MIB.

The SNM) extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In the case of a cluster configuration, the SNMP extension agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such

as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables the SNMP managed device to advertise themself to other Cisco devices on the network.

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

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

Note The CISCO-CDP-MIB is dependent on the presence of the following MIBs: CISCO-SMI, CISCO-TC, CISCO-VTP-MIB.

SYSAPPL-MIB

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

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

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt

- sysApplElmtRun

Table 50: SYSAPPL-MIB Commands

Command	Description
Device-Related Queries	
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.
sysApplElmPastRunUser	Provides the process owner's login name (for example, root).
Memory, Storage, and CPU-Related Queries	
sysApplElmPastRunMemory	Provides the last-known total amount of real system memory measured in kilobytes that was allocated to this process before it terminated.
sysApplElmtPastRunCPU	Provides the last known number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may increment by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallElmtCurSizeLow	Provides the current file size modulo 2^32 bytes. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplInstallElmtSizeLow	Provides the installed file size modulo 2^32 bytes. This is the size of the file on disk immediately after installation. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplElmRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.

sysApplElmRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
Process-Related Queries	
sysApplElmtRunState	Provides the current state of the running process. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).
sysApplElmtRunNumFiles	Provides the number of regular files currently opened by the process. Transport connections (sockets) should *not* be included in the calculation of this value, nor should operating-system-specific special file types.
sysApplElmtRunTimeStarted	Provides the time the process was started.
sysApplElmtRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.
sysApplElmtPastRunInstallID	Provides the index into the installed element table. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a previously executed process.
sysApplElmtPastRunUser	Provides the process owner's login name (for example, root).
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplRunStarted	Provides the date and time that the application was started.
sysApplElmtRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.

Software Component-Related Queries	
sysApplInstallPkgProductName	Provides the name that the manufacturer assigned to the software application package.
sysApplElmtRunParameters	Provides the starting parameters for the process.
sysApplElmtRunName	Provides the full path and filename of the process. For example, '/opt/MYYpkg/bin/myyproc' would be returned for process 'myyproc' whose execution path is 'opt/MYYpkg/bin/myyproc'.
sysApplInstallElmtName	Provides the name of this element, which is contained in the application.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplInstallElmtPath	Provides the full path to the directory where this element is installed. For example, the value would be '/opt/EMPuma/bin' for an element installed in the directory '/opt/EMPuma/bin'. Most application packages include information about the elements that are contained in the package. In addition, elements are typically installed in subdirectories under the package installation directory. In cases where the element path names are not included in the package information itself, the path can usually be determined by a simple search of the subdirectories. If the element is not installed in that location and no other information is available to the agent implementation, then the path is unknown and null is returned.

sysApplMapInstallPkgIndex	Provides the value of this object and identifies the installed software package for the application of which this process is a part. Provided that the parent application of the process can be determined, the value of this object is the same value as the sysApplInstallPkgIndex for the entry in the sysApplInstallPkgTable that corresponds to the installed application of which this process is a part. If, however, the parent application cannot be determined (for example, the process is not part of a particular installed application), the value for this object is then '0', signifying that this process cannot be related back to an application, and in turn, an installed software package.
sysApplElmtRunInstallID	Provides the index into the sysApplInstallElmtTable. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a running instance. If this process cannot be associated with an installed executable, the value should be '0'.
sysApplRunCurrentState	Provides the current state of the running application instance. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5). This value is based on an evaluation of the running elements of this application instance (see sysApplElmRunState) and their Roles as defined by sysApplInstallElmtRole. An agent implementation may detect that an application instance is in the process of exiting if one or more of its REQUIRED elements are no longer running. Most agent implementations will wait until a second internal poll is completed to give the system time to start REQUIRED elements before marking the application instance as exiting.
sysApplInstallPkgDate	Provides the date and time this software application was installed on the host.
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.

sysApplInstallElmtType	Provides the type of element that is part of the installed application.
Date/Time-Related Queries	
sysApplElmtRunCPU	The number of centi-seconds of the total system CPU resources consumed by this process **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallPkgDate	Provides the date and time this software application is installed on the host.
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplRunStarted	Provides the date and time that the application was started.

MIB-II

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

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

Table 51: MIB-II Commands

Command	Description
Device-Related Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully qualified domain name of the node. If the name is unknown, the value is the zero-length string.

sysDescr	Provides a textual description of the entity. This value should include the full name and version identification of the system hardware type, software operating-system, and networking software.
SNMP Diagnostic Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully-qualified domain name of the node. If the name is unknown, the value is the zero-length string.
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.
snmpInTotalReqVars	Provides the total number of MIB objects that were retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpOutPkts	Provides the total number of SNMP Messages that were passed from the SNMP entity to the transport service.
sysServices	Provides a value that indicates the set of services that this entity potentially offers. The value is a sum. This sum initially takes the value zero, then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which is a host offering application services would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). **Note** In the context of the Internet suite of protocols, calculate: layer 1 physical (for example, repeaters), layer 2 datalink/subnetwork (for example, bridges), layer 3 internet (supports IP), layer 4 end-to-end (supports TCP), layer 7 applications (supports SMTP). For systems including OSI protocols, you can also count layers 5 and 6.

snmpEnableAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** Cisco strongly recommends that this object be stored in nonvolatile memory so that it remains constant across reinitializations of the network management system.
Syslog-Related Queries	
snmpEnabledAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** Cisco strongly recommends that this object be stored in a nonvolatile memory so that it remains constant across reinitializations of the network management system.
Date/Time-Related Queries	
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.

HOST-RESOURCES MIB

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

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

Table 52: HOST-RESOURCES MIB Commands

Command	Description
Device-Related Queries	
hrFSMountPoint	Provides the path name of the root of this file system.

hrDeviceDescr	Provides a textual description of this device, including the device manufacturer and revision, and optionally, the serial number.
hrStorageDescr	Provides a description of the type and instance of the storage.
Memory, Storage, and CPU Related Queries	
hrMemorySize	Provides the amount of physical read-write main memory, typically RAM, that the host contains.
hrStorageSize	Provides the size of the storage, in units of hrStorageAllocationUnits.This object is writable to allow remote configuration of the size of the storage area in those cases where such an operation makes sense and is possible on the underlying system. For example, you can modify the amount of main memory allocated to a buffer pool or the amount of disk space allocated to virtual memory.
Process-Related Queries	
hrSWRunName	Provides a textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software is installed locally, it must be the same string as used in the corresponding hrSWInstalledName.
hrSystemProcesses	Provides the number of process contexts that are currently loaded or running on this system.
hrSWRunIndex	Provides a unique value for each piece of software that is running on the host. Wherever possible, use the native, unique identification number of the system.
Software Component-Related Queries	
hrSWInstalledName	Provides a textual description of this installed piece of software, including the manufacturer, revision, the name by which it is commonly known, and optionally, the serial number.
hrSWRunPath	Provides a description of the location of long-term storage (for example, a disk drive) from which this software was loaded.
Date/Time-Related Queries	
hrSystemDate	Provides the host local date and time of day.

hrFSLastPartialBackupDate	Provides the last date at which a portion of this file system was copied to another storage device for backup. This information is useful for ensuring that backups are being performed regularly. If this information is not known, then this variable will have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Note The CISCO-SYSLOG-MIB is dependent on the presence of the CISCO-SMI MIB.

Table 53: CISCO-SYSLOG-MIB Commands

Command	Description
Syslog-Related Queries	
clogNotificationEnabled	Indicates whether clogMessageGenerated notifications will be sent when the device generates a syslog message. Disabling notifications does not prevent syslog messages from being added to the clogHistoryTable.
clogMaxSeverity	Indicates which syslog severity levels will be processed. The agent will ignore any syslog message with a severity value greater than this value. **Note** Severity numeric values increase as their severity decreases. For example, error (4) is more severe than debug (8).

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the Cisco Cisco Unified Communications Manager and its associated devices, such as phones, gateways, and so on,

that are visible on this Cisco Cisco Unified Communications Manager node. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

Note Cisco Cisco Unified Communications Manager supports this MIB in Cisco Cisco Unified Communications Manager systems. IM and Presence Service and Cisco Unity Connection do not support this MIB.

To view the support lists for the CISCO-CCM-MIB and MIB definitions, go to the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

To view MIB dependencies and MIB contents, including obsolete objects, across Cisco Cisco Unified Communications Manager releases, go to the following link: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

Dynamic tables get populated only if the Cisco CallManager service is up and running (or the local Cisco CallManager service in the case of a Cisco Cisco Unified Communications Manager cluster configuration); static tables get populated when the Cisco CallManager SNMP Service is running.

Table 54: Cisco-CCM-MIB Dynamic Tables

Table(s)	Contents
ccmTable	This table stores the version and installation ID for the local Cisco Cisco Unified Communications Manager. The table also stores information about all the Cisco Cisco Unified Communications Manager in a cluster that the local Cisco Cisco Unified Communications Manager knows about but shows “unknown” for the version detail. If the local Cisco Cisco Unified Communications Manager is down, the table remains empty, except for the version and installation ID values.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match Cisco Cisco Unified Communications Manager/RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone. The ccmPhoneExtnTable uses a combined index, ccmPhoneIndex and ccmPhoneExtnIndex, for relating the entries in the ccmPhoneTable and ccmPhoneExtnTable.
ccmCTIDevice, ccmCTIDeviceDirNum	The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Cisco Cisco Unified Communications Manager MIB get updated.
ccmSIPDevice	The CCMSIPDeviceTable stores each SIP trunk as one device.

Table(s)	Contents
ccmH323Device	The ccmH323DeviceTable contains the list of H.323 devices for which Cisco Cisco Unified Communications Manager contains information (or the local Cisco Cisco Unified Communications Manager in the case of a cluster configuration). For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Cisco Cisco Unified Communications Manager. Cisco Cisco Unified Communications Manager generates the H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H.323 trunk information.
ccmVoiceMailDevice, ccmVoiceMailDirNum	For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable includes one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisco Cisco Unified Communications Manager MIB get updated.
ccmGateway	The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively. Cisco Cisco Unified Communications Manager generates alarms at the device or port level. The ccmGatewayTable, based on CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports. Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.
ccmMediaDeviceInfo	The table contains a list of all media devices which have tried to register with the local Cisco Cisco Unified Communications Manager at least once.
ccmGroup	This tables contains the Cisco Cisco Unified Communications Manager groups in a Cisco Cisco Unified Communications Manager cluster.
ccmGroupMapping	This table maps all Cisco Cisco Unified Communications Managers in a cluster to a Cisco Cisco Unified Communications Manager group. The table remains empty when the local Cisco Cisco Unified Communications Manager node is down.

Table 55: CISCO-CCM-MIB Static Tables

Table(s)	Content
ccmProductType	The table contains the list of product types that are supported with Cisco Cisco Unified Communications Manager (or cluster, in the case of a Cisco Cisco Unified Communications Manager cluster configuration), including phone types, gateway types, media device types, H.323 device types, CTI device types, voice-messaging device types, and SIP device types.
ccmRegion, ccmRegionPair	ccmRegionTable contains the list of all geographically separated regions in a Cisco Communications Network (CCN) system. The ccmRegionPairTable contains the list of geographical region pairs for a Cisco Cisco Unified Communications Manager cluster. Geographical region pairs are defined by Source region and Destination region.
ccmTimeZone	The table contains the list of all time zone groups in a Cisco Cisco Unified Communications Manager cluster.
ccmDevicePool	The tables contains the list of all device pools in a Cisco Cisco Unified Communications Manager cluster. Device pools are defined by Region, Date/Time Group, and Cisco Cisco Unified Communications Manager Group.

Note 'The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that are described.

CISCO-UNITY-MIB

The CISCO-UNITY-MIB uses the Connection SNMP Agent to get information about Cisco Unity Connection.

To view the CISCO-UNITY-MIB definitions, go to the following link and click **SNMP V2 MIBs**:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note Cisco Unity Connection supports this MIB. Cisco Cisco Unified Communications Manager and IM and Presence Service do not support this MIB.

The Connection SNMP Agent supports the following objects.

Table 56: CISCO-UNITY-MIB Objects

Object	Description
ciscoUnityTable	This table contains general information about the Cisco Unity Connection servers such as hostname and version number.
ciscoUnityPortTable	This table contains general information about the Cisco Unity Connection voice messaging ports.
General Unity Usage Info objects	This group contains information about capacity and utilization of the Cisco Unity Connection voice messaging ports.

Set Up SNMP

The following procedures provides an overview of the steps for configuring SNMP.

Before You Begin

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

Procedure

Step 1 Install and configure the SNMP NMS.

Step 2 In the **Control Center - Network Services** window, verify that the system started the SNMP services.

Step 3 Unified Communications Manager: In the **Service Activation** window, activate the Cisco CallManager SNMP service. Cisco Unity Connection only: The Connection SNMP Agent service automatically activates.

Step 4 If you are using SNMP V1/V2c, configure the community string.

Step 5 If you are using SNMP V3, configure the SNMP user.

Step 6 Configure the notification destination for traps or informs.

Step 7 Configure the system contact and location for the MIB2 system group.

Step 8 Configure trap settings for CISCO-SYSLOG-MIB.

Step 9 Unified Communications Manager only: Configure trap settings for CISCO-CCM-MIB.

Step 10 Restart the Master Agent service.

Step 11 On the NMS, configure the Cisco Unified Communications Manager trap parameters.

Troubleshooting SNMP

Review this section for troubleshooting tips. Make sure that all of the feature and network services are running.

Problem

You cannot poll any MIBs from the system.

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system. By default, no community string or user is configured on the system.

Solution

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

Problem

You cannot receive any notifications from the system.

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

Solution

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

SNMP Configuration Requirements

The system provides no default SNMP configuration. You must configure SNMP settings after installation to access MIB information. Cisco supports SNMP V1, V2c, and V3 versions.

SNMP agent provides security with community names and authentication traps. You must configure a community name to access MIB information. The following table provides the required SNMP configuration settings.

Table 57: SNMP Configuration Requirements

Configuration	Cisco Unified Serviceability Page
V1/V2c Community String	**SNMP** > **V1/V2c** > **Community String**
V3 Community String	**SNMP** > **V3** > **User**
System Contact and Location for MIB2	**SNMP** > **SystemGroup** > **MIB2 System Group**
Trap Destinations (V1/V2c)	**SNMP** > **V1/V2c** > **Notification Destination**
Trap Destinations (V3)	**SNMP** > **V3** > **Notification Destination**

SNMP Version 1 Support

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

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

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

In the serviceability GUI, you configure SNMPv1 support in the **V1/V2c Configuration** window.

SNMP Version 2c Support

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

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

In the serviceability GUI, you configure SNMPv2c support in the **V1/V2c Configuration** window.

SNMP Version 3 Support

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

Instead of using community strings like SNMPv1 and v2, SNMPv3 uses SNMP users.

In the serviceability GUI, you configure SNMPv3 support in the **V3 Configuration** window.

SNMP Services

The services in the following table support SNMP operations.

Note SNMP Master Agent serves as the primary service for the MIB interface. You must manually activate Cisco CallManager SNMP service; all other SNMP services should be running after installation.

Table 58: SNMP Services

MIB	Service	Window
CISCO-CCM-MIB	Cisco CallManager SNMP service	**Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**. Choose a server; then, choose Performance and Monitoring category.

MIB	Service	Window
SNMP Agent	SNMP Master Agent	**Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category. **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category.
CISCO-CDP-MIB	Cisco CDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
Hardware MIBs	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**Cisco Unity Connection Serviceability** > **Tools** > **Service Management.** Choose a server; then, choose Base Services category.

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

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMPv1 and v2c only.

SNMPv3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In the serviceability GUI, no default community string or user exists.

SNMP Traps and Informs

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

Note Cisco Unified Communications Manager supports SNMP traps in Cisco Unified Communications Manager and IM and Presence Service systems.

For SNMP notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, alarms and system level log messages get sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages get logged locally in the syslog files and also get converted into SNMP traps/notifications.

The following list contains Cisco Unified Communications Manager SNMP trap/inform messages that are sent to a configured trap destination:

- Cisco Unified Communications Manager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

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

You configure the SNMP trap destination by choosing **SNMP** > **V1/V2** > **Notification Destination** or **SNMP** > **V3** > **Notification Destination** in the serviceability GUI.

The following table provides information about trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in the table by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note All the parameters that are listed in the table are part of CISCO-CCM-MIB except for the last two parameters. The last two, clogNotificationsEnabled and clogMaxSeverity, comprise part of CISCO-SYSLOG-MIB.

For IM and Presence Service, you configure only clogNotificationsEnabled and clogMaxSeverity trap/inform parameters on the NMS.

Table 59: Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Although you can configure a Cisco ATA 186 device as a phone in Cisco Unified Communications Manager Administration, when Cisco Unified Communications Manager sends SNMP traps for the Cisco ATA device, it sends a gateway type trap; for example, ccmGatewayFailed.	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.
ccmQualityReportAlarmEnable	True	This trap gets generated only if the Cisco Extended Functions service is activated and running on the server, or, in the case of a cluster configuration (Cisco Unified Communications Manager only), on the local Cisco Unified Communications Manager server. ccmQualityReport	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when applications generate a syslog message with at least a warning severity level.

Related Topics

CISCO-CCM-MIB Trap Parameters, on page 182
CISCO-SYSLOG-MIB Trap Parameters, on page 181

SNMP Trace Configuration

For Cisco Unified Communications Manager, you can configure trace for the Cisco CallManager SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco CallManager SNMP Service in the Performance and Monitoring Services service group. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you use the CLI to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For Cisco Unity Connection, you can configure trace for the Cisco Unity Connection SNMP agent in the Trace Configuration window in Cisco Unity Connection Serviceability by choosing the Connection SNMP Agent component.

SNMP V1 and V2c Setup

This section describes how to configure the SNMP managed device for SNMP V1/V2c.

Find Community String

To find a community string, perform the following procedure.

Before You Begin

Review the tasks in the overview procedure to set up SNMP.

Procedure

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

Step 2 Select the specific search criteria that you want to use for the community string from the **Find Community Strings where** Name list box.

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

Step 4 Select the hostname or IP address of the server where the community string exists in the **Server** list box.

Step 5 Select **Find**.

Step 6 (Optional) To apply the configuration from one of the options in the search results to all nodes in a cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.
This step applies to Unified Communications Manager and IM and Presence Service clusters only.

Step 7 Select the community string that you want to view from the list of results.

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

Step 8 From the list of results, click the community string that you want to view.

Set Up Community String

Because the SNMP agent provides security by using community strings, you must configure the community string to access any management information base (MIB) in the SNMP managed device's system. Change the community string to limit access to the SNMP managed device's system. To add, modify, and delete community strings, access the SNMP Community String configuration window.

Procedure

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

Step 2 Select the required server from the **Server** list box, and then select **Find**.

Step 3 Perform one of the following tasks:

- To add a new community string, click **Add New**.

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

- To modify an existing community string, click the name of the community string that you want to edit from the list of results.

  You cannot change the name of the community string or the server.

Step 4 Enter the community string configuration settings.

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

Step 5 After you complete the configuration, click **Add New** to save a new community string or click **Save** to save changes to an existing community string.
A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 6 Perform one of the following actions:

- Select **OK** to restart the SNMP master agent service and effect the changes.
- Select **Cancel** to continue the configuration without restarting the SNMP master agent.

  Note Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service.

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

Related Topics

Community String Configuration Settings, on page 163
Start, Stop, and Restart Services in Control Center or CLI, on page 91

Community String Configuration Settings

The following table describes the community string configuration settings.

Table 60: Community String Configuration Settings

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

Field	Description
Access Privileges	From the drop-down list box, select the appropriate access level from the following list: **ReadOnly** The community string can only read the values of MIB objects. **ReadWrite** The community string can read and write the values of MIB objects. **ReadWriteNotify** The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** The community string can only send MIB object values for a trap and inform messages. **ReadNotifyOnly** The community string can read values of MIB objects and also send the values for trap and inform messages. **None** The community string cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a community string with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges. IM and Presence Service does not support ReadNoticyOnly.
Apply To All Nodes	To apply the community string to all nodes in the cluster, check this check box. This field applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Related Topics

Find Community String, on page 161

Delete Community String

To delete a community string, perform the following procedure:

Procedure

Step 1 Locate the community string.

Step 2 Check the community string that you want to delete from the list of matching records.

Step 3 Select **Delete Selected**. A message indicates that the system will delete notification entries that relate to this community string.

Step 4 Select **OK** to continue the deletion. A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following actions:

- Select **Cancel** to continue the configuration without restarting the SNMP master agent.
- Select **OK** to restart the SNMP master agent service.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service.

Related Topics

Start, Stop, and Restart Services in Control Center or CLI, on page 91

Find SNMP V1 and V2c Notification Destination

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

Procedure

Step 1 Choose **Snmp** > **V1/V2c** > **Notification Destination**.
The Find/List window displays.

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

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

Step 4 Enter the hostname or IP address of the server that supports the notification destination in the Server list box, and then click **Find**.
After you click Find, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 5 (Optional) Perform one or more of the following actions:

- To apply the configuration from one of the options in the search results to all nodes in the cluster, check the name of the option and check **Apply to All Nodes**.

  This step applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.
- Select an item in the search results to view the configuration for that item.

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

Set Up SNMP V1 and V2c Notification Destination

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

Procedure

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

Step 2 Select the required server from the **Server** list box, and then click **Find**.

Step 3 Perform one of the following tasks:

- To add a new SNMP notification destination, click **Add New**.

  You configure the notification destination for the server that you choose in the Server drop-down list box in the Find/List window.

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

- To modify an existing SNMP notification destination, find the notification destination that you want to edit, and then click the name of the SNMP notification destination in the **Find/List** window results list.

Step 4 Enter the notification destination configuration settings.

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

Step 5 Perform one of the following actions:

- Select **Insert** to save a notification destination.
- Select **Save** to save changes to an existing notification destination. A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 6 Select **OK** to restart the SNMP master agent or select **Cancel** to continue the configuration without restarting the SNMP master agent.

Note Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service.

Related Topics

Find SNMP V1 and V2c Notification Destination, on page 165

Notification Destination Settings for SNMP V1 and V2c, on page 167
Set Up SNMP V1 and V2c Notification Destination, on page 166
Start, Stop, and Restart Services in Control Center or CLI, on page 91

Notification Destination Settings for SNMP V1 and V2c

The following table describes the notification destination configuration settings for SNMP V1/V2c.

Table 61: Notification Destination Configuration Settings for SNMP V1/V2c

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

Field	Description
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Related Topics

Find Community String, on page 161
Find SNMP V1 and V2c Notification Destination, on page 165
Set Up Community String, on page 162
Set Up SNMP V1 and V2c Notification Destination, on page 166

Delete SNMP V1 and V2c Notification Destination

To delete an SNMP V1/V2c notification destination, perform the following procedure:

Procedure

Step 1 Find the notification destination that you want to delete.

Step 2 Check the check box next to the notification destination that you want to delete in the list of matching records in the **Find/List** window.

Step 3 Click **Delete Selected**. A message asks whether you want to delete the notification entries.

Step 4 Click **OK** to continue the deletion. A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following:

- To restart the SNMP master agent service, click **OK**.
- To continue the configuration without restarting the SNMP master agent, click **Cancel**.

Tip Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service.

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

Related Topics

Find SNMP V1 and V2c Notification Destination, on page 165
Start, Stop, and Restart Services in Control Center or CLI, on page 91

SNMP V3 Setup

This section describes how to configure the SNMP managed device for SNMP V3.

Find SNMP V3 User

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

To find a SNMP user, perform the following procedure.

Procedure

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

Step 2 Select the specific search criteria that you want to use to find the user; for example, begins with.

Step 3 Enter the username for which you want to search.

Step 4 Select the hostname or IP address of the server where you access the user from the **Server** list box, and then click **Find**.

Step 5 (Optional) To apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and check the **Apply to All Nodes** check box.
This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Step 6 Select the user that you want to view from the list of results.

Set Up SNMP V3 User

To setup users for SNMP V3, perform the following procedure.

Procedure

Step 1 Select **Snmp** > **V3** > **User** and locate the SNMP V3 user to set up.
See the procedure to find the SNMP V3 user for details.

Step 2 Perform one of the following tasks:

- To add a new SNMP user, click the **Add New** button in the **SNMP User Configuration Find/List** window.
- IM and Presence only: To add a new SNMP user, select **Snmp** > **V3** > **User** > **Add New**.

  Note The **Add New** button does not display in the **SNMP User Configuration** window until you select the **Find** button. If no users exist and you want to add want a user, select the **Find** button and wait for the window to refresh. The **Add New** button displays.
- To modify an existing SNMP user, search for the user in the **SNMP User Configuration Find/List** window, and then click the name of the SNMP user that you want to modify from the results list.

Step 3 Enter the SNMP V3 user configuration settings.

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

Step 4 To add a new user, click **Insert**, or click **Save** to save changes to an existing user.
A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following:

- To restart the SNMP master agent service, click **OK**.
- To continue the configuration without restarting the SNMP master agent, click **Cancel**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service.

Note To access this server that has the user that you configure, make sure that you configure this user on the NMS with the appropriate authentication and privacy settings.

Related Topics

Find SNMP V3 User, on page 169
SNMP V3 User Configuration Settings, on page 170
Start, Stop, and Restart Services in Control Center or CLI, on page 91

SNMP V3 User Configuration Settings

The following table describes the SNMP V3 user configuration settings.

Table 62: SNMP V3 User Configuration Settings

Field	Description
Server	This setting displays as read only because you specified the server when you performed the find notification destination procedure. To change the server where you want to provide access, perform the procedure to find an SNMP user.
User Name	In the field, enter the name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS). For existing SNMP users, this setting displays as read only.
Authentication Required	To require authentication, check the check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, you must choose **SHA** as the protocol.

Field	Description
Privacy Required	If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the check box, enter the password in the Password and Reenter Password fields, and check the protocol check box. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, you must choose **AES128** as the protocol.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Host IP Address field, enter a host from which you want to accept SNMP packets and click **Insert**. Repeat this process for each host from which you want to accept SNMP packets. To delete a host, choose that host from the Host IP Addresses pane and click **Remove**.
Access Privileges	From the drop-down list box, choose one of the following options for the access level: **ReadOnly** The user can only read the values of MIB objects. **ReadWrite** The user can read and write the values of MIB objects. **ReadWriteNotify** The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** The user can only send MIB object values for trap and inform messages. **ReadNotifyOnly** The user can read values of MIB objects and also send the values for trap and inform messages. **None** The user cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
Apply To All Nodes	To apply the user configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Related Topics

Find SNMP V3 User, on page 169

Delete SNMP V3 User

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

Procedure

Step 1 Select **Snmp** > **V3** > **User** and locate the SNMP V3 user to delete.
See the procedure to find the SNMP V3 user for details.

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

Step 3 Click **Delete Selected**.
A message indicates that the system will delete notification entries that relate to this user.

Step 4 To continue the deletion, click **OK**.
A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following actions:

- Select **OK** to restart the SNMP master agent service.
- Select **Cancel** to continue the configuration without restarting the SNMP master agent.

Cisco recommends that you wait until you finish all the SNMP configuration before you restart the SNMP master agent service.

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

Related Topics

Find SNMP V3 User, on page 169
Start, Stop, and Restart Services in Control Center or CLI, on page 91

Find SNMP V3 Notification Destination

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

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

Procedure

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

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

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

Step 4 In the Server field, choose the hostname or IP address of the server that supports the notification destination, and then click **Find**.
After you click **Find**, the Add New button displays. After the search results display, the Apply to All Nodes check box displays.

Step 5 (Optional) To apply the configuration from one of the options in the search results to all nodes in the cluster, check the check box next to the name of the option and then check the **Apply to All Nodes** check box.
This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Step 6 Select the notification destination that you want to view from the list of results.

Set Up SNMP V3 Notification Destination

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

Procedure

Step 1 Select **Snmp** > **V3** > **Notification Destination** and locate the notification destination for SNMP V3 to set up. See the procedure to find the notification destination for SNMP V3 for details.

Step 2 Perform one of the following tasks:

- To add a new SNMP notification destination, click the **Add New** button in the search results window.
- To modify an existing SNMP notification destination, click the name of the SNMP notification destination that you want to edit in the search results window.

Step 3 Configure the SNMP V3 notification destination configuration settings.

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

Step 4 Perform one of the following actions to save a notification destination:

- Select **Insert** to add the notification destination.
- Select **Save** to save changes to an existing notification destination.

A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following actions:

- To restart the SNMP master agent service, click **OK**.

- To continue the configuration without restarting the SNMP master agent, click **Cancel**.

Tip Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service.

Related Topics

Find SNMP V3 User, on page 169
SNMP V3 User Configuration Settings, on page 170
Start, Stop, and Restart Services in Control Center or CLI, on page 91

Notification Destination Settings for SNMP V3

The following table describes the notification destination configuration settings for SNMP V3.

Table 63: Notification Destination Configuration Settings for SNMP V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure to find an SNMP V3 notification destination. To change the server for the notification destination, perform the procedure to find an SNMP V3 notification destination and select a different server.
Host IP Addresses	From the drop-down list box, choose the Host IP address or choose **Add New**. If you chose Add New, enter the IP address for the host.
Port Number	In the field, enter the notification-receiving port number on the destination server.
Notification Type	From the drop-down list box, choose **Inform** or **Trap**. **Tip** Cisco recommends that you choose the Inform option. The Inform function retransmits the message until it is acknowledged, thus, making it more reliable than traps.
Remote SNMP Engine Id	This setting displays if you chose Inform from the Notification Type drop-down list box. From the drop-down list box, choose the engine ID or choose **Add New**. If you chose Add New, enter the ID in the Remote SNMP Engine Id field, which requires a hexidecimal value.

Field	Description
Security Level	From the drop-down list box, choose the appropriate security level for the user. **noAuthNoPriv** No authentication or privacy configured. **authNoPriv** Authentication configured, but no privacy configured. **authPriv** Authentication and privacy configured.
User Information pane	From the pane, perform one of the following tasks to associate or disassociate the notification destination with the user. 1 To create a new user, click **Create New User**. 2 To modify an existing user, click the radio button for the user and then click **Update Selected User**. 3 To delete a user, click the radio button for the user and then click **Delete Selected User**. The users that display vary depending on the security level that you configured for the notification destination.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Related Topics

Find SNMP V3 User, on page 169

Delete SNMP V3 Notification Destination

To delete an SNMP V3 notification destination, perform the following procedure.

Procedure

Step 1 Select **Snmp** > **V3** > **Notification Destination** and locate the notification destination to delete.
See the procedure to find the notification destination for SNMP V3 for details.

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

Step 3 Select **Delete Selected**. A message asks you if you want to delete the notification destination.

Step 4 Select **OK** to continue the deletion. A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 5 Perform one of the following actions:

- Select **OK** to restart the SNMP master agent service.
- Select **Cancel** to continue the configuration without restarting the SNMP master agent.

Note Cisco recommends that you wait until you finish the SNMP configuration before you restart the SNMP master agent service.

Related Topics

Find SNMP V3 Notification Destination, on page 172
Start, Stop, and Restart Services in Control Center or CLI, on page 91

MIB2 System Group

Use the serviceability GUI to configure the system contact and system location objects for the SNMP MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

Set Up MIB2 System Group

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

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

Procedure

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

Step 2 Configure the SNMP MIB2 system group configuration settings.

Step 3 Click **Save**. A message indicates that changes will not take effect until you restart the SNMP master agent.

Step 4 Select **OK** to restart the SNMP master agent service or select **Cancel** to continue the configuration without restarting the SNMP master agent.

Step 5 Perform one of the following actions:

- Select **Clear All** to clear the **System Contact** and **System Location** fields.
- Select **Clear All** and **Save** to delete the system configuration.

Related Topics

MIB2 System Group Settings, on page 177

MIB2 System Group Settings

The following table describes the MIB2 System Group configuration settings.

Table 64: MIB2 System Group Configuration Settings

Field	Description
Server	From the drop-down list box, choose the server for which you want to configure contacts, and then click **Go**.
System Contact	Enter a person to notify when problems occur.
System Location	Enter the location of the person that is identified as the system contact.
Apply To All Nodes	Check to apply the system configuration to all of the nodes in the cluster. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

SNMP Trap Settings

Use CLI commands to set the configurable SNMP trap settings. SNMP trap configuration parameters and recommended configuration tips are provided for CISCO-SYSLOG-MIB, CISCO-CCM-MIB, and CISCO-UNITY-MIB.

Set Up SNMP Traps

To set up SNMP traps, perform the following steps.

Procedure

Step 1 Login to Cisco Unified Serviceability and confirm that Cisco CallManager SNMP Services and SNMP Master Agent are activated and running by performing the following steps:

a) Choose **Tools** > **Control Center - Feature Services** and confirm that **Cisco CallManager SNMP Services** is started.

b) Choose **Tools** > **Control Center - Network Services** and confirm that **SNMP Master Agent** is started.

Step 2 If you want to run SNMP V1 or V2, confirm that the community string and notification destination is set up by performing the following steps:

a) Follow the Set up community string procedure and make sure that Access Privileges are set to either ReadWriteNotify, NotifyOnly, or ReadNotify.
b) Follow the Set up notification destination procedure.

Step 3 If you want to run SNMP V3, confirm that the user and notification destination is set up by performing the following steps:

a) Follow the Setup SNMP user procedure and make sure that Access Privileges are set to either ReadWriteNotify, NotifyOnly, or ReadNotify.
b) Follow the Set up notification destination procedure.

Step 4 Login to CLI and run the `utils snmp test` CLI command to verify that SNMP is running.

Step 5 Follow Generate SNMP traps to generate specific SNMP traps (for example, the ccmPhoneFailed or MediaResourceListExhausted traps).

Step 6 If the traps do not generate, perform the following steps:

- In Cisco Unified Serviceability, choose **Alarm** > **Configuration** and select **CM Services** and **Cisco CallManager**.
- Check the **Apply to All Nodes** check box.
- Under Local Syslogs, set the Alarm Event Level drop-down list box to **Informational**.

Step 7 Reproduce the traps and check if the corresponding alarm is logged in CiscoSyslog file.

Generate SNMP Traps

This section describes the process for generating specific types of SNMP traps. SNMP must be set up and running on the server in order for the individual traps to generate. Follow Set Up SNMP Traps, on page 177 for instructions on how to set up your system to generate SNMP traps.

Note The processing time for individual SNMP traps varies depending on which trap you are attempting to generate. Some SNMP traps may take up to a few minutes to generate.

Table 65: Generate SNMP Traps

SNMP Traps	Process
ccmPhoneStatusUpdate	To trigger the ccmPhoneStatusUpdate trap: **1** In the ccmAlarmConfig Info mib table, set ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 or higher. **2** Login to Cisco Cisco Unified Communications Manager Administration. **3** For a phone that is in service and that is registered to Cisco Cisco Unified Communications Manager, reset the phone. The phone deregisters, and then reregisters, generating the ccmPhoneStatusUpdate trap.
ccmPhoneFailed	To trigger the ccmPhoneFailed trap: **1** In the ccmAlarmConfigInfo mib table, set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 or higher. **2** In Cisco Cisco Unified Communications Manager Administration, change the MAC address of the phone to an invalid value. **3** In Cisco Cisco Unified Communications Manager Administration, reregister the phone. **4** Set the phone to point to the TFTP server A and plug the phone in to a different server.
ccmGatewayFailed	To trigger the ccmGatewayFailed SNMP trap: **1** Confirm that ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) is set to true. **2** In Cisco Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. **3** Reboot the gateway.
ccmGatewayLayer2Change	To trigger the ccmGatewayLayer2Change trap on a working gateway where layer 2 is monitored (for example, the MGCP backhaul load): **1** In the ccmAlarmConfig Info mib table, set ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true. **2** In Cisco Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. **3** Reset the gateway.

SNMP Traps	Process
MediaResourceListExhausted	To trigger a MediaResourceListExhausted trap: **1** In Cisco Cisco Unified Communications Manager Administration, create a media resource group that contains one of the standard Conference Bridge resources (CFB-2). **2** Create a media resource group list that contains the media resource group that you created. **3** In the Phone Configuration window, set the Media Resource Group List field to the media resource group lis that you just created. **4** Stop the IP Voice Media Streaming service. This action causes the ConferenceBridge resource (CFB-2) to stop working. **5** Make conference calls with phones that use the media resource group list. The "No Conference Bridge available" message appears in the phone screen.
RouteListExhausted	To trigger a RouteListExhausted trap: **1** Create a route group that contains one gateway. **2** Create a route group list that contains the route group that you just created. **3** Create a unique route pattern that routes a call through the route group list. **4** Deregister the gateway. **5** Dial a number that matches the route pattern from one of the phones.
MaliciousCallFailed	To trigger a MaliciousCallFailed trap: **1** Create a softkey template that includes all available "MaliciousCall" softkeys. **2** Assign the new softkey template to phones in your network and reset the phones. **3** Place a call between the phones. **4** During the call, select the "MaliciousCall" softkey.

SNMP Traps	Process
ccmCallManagerFailed	To trigger the ccmCallManagerFailed trap: **1** Run the `show process list` CLI command to get the Process Identifier (PID) of the CallManager application ccm. This command returns a number of processes and their PIDs. You must obtain the PID for ccm specifically since this is the PID that you must stop in order to generate the alarm. **2** Run the `delete process <pid>` crash CLI command. **3** Run the `utils core active list` CLI command. The CallManager Failed Alarm is generated when internal errors are generated. These internal errors may include an internal thread quitting due to the lack of CPU, pausing the CallManager server for more than 16 seconds, and timer issues. **Note** Generating a ccmCallManagerFailed alarm/trap shuts down the CallManager service and generates a core file. To avoid confusion, Cisco recommends that you delete the core file immediately.
syslog messages as traps	To receive syslog messages above a particular severity as traps, set the following two mib objects in the clogBasic table: **1** Set clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true(1). Default value is false(2). For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 **2** Set the clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) to a level that is greater than the level at which you want your traps to be produced. The default value is warning (5). All syslog messages with alarm severity lesser than or equal to the configured severity level are sent as traps. For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

CISCO-SYSLOG-MIB Trap Parameters

Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:

- Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to True by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to True from the linux command line using:

```
snmpset -c <community string>-v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  You can also use any other SNMP management application for the SNMP Set operation.

- Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset-c public-v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>
```

Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.

Severity values are as follows:

- 1: Emergency
- 2: Alert
- 3: Critical
- 4: Error
- 5: Warning
- 6: Notice
- 7: Info
- 8: Debug)

You can also use any other SNMP management application for the SNMP Set operation.

Note Before logging, Syslog truncates any trap message data that is larger than the specified Syslog buffer size. The Syslog trap message length limitation equals 255 bytes.

CISCO-CCM-MIB Trap Parameters

- Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset -c <community string> -v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

You can also use any other SNMP management application for the SNMP Set operation.

- Set ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset -c <community string> -v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

You can also use any other SNMP management application for the SNMP Set operation.

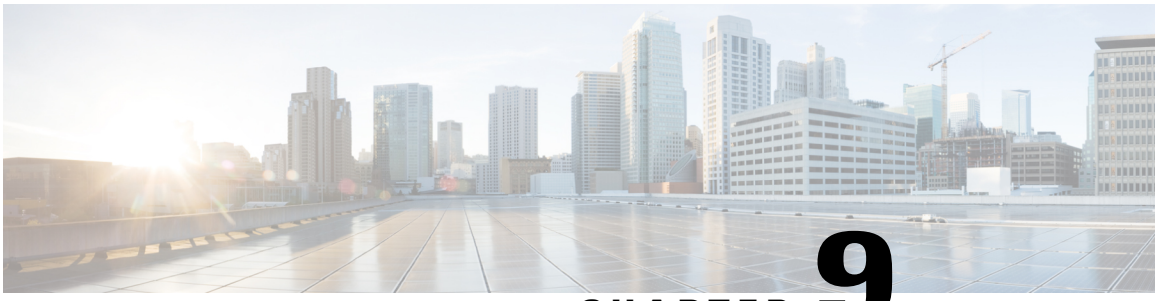
CISCO-UNITY-MIB Trap Parameters

Cisco Unity Connection only: The Cisco Unity Connection SNMP Agent does not enable trap notifications, though traps can be triggered by Cisco Unity Connection alarms. You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability, on the **Alarm** > **Definitions** screen.

You can configure trap parameters by using the CISCO-SYSLOG-MIB.

Related Topics

CISCO-SYSLOG-MIB Trap Parameters, on page 181



CHAPTER 9

Call Home

- Call Home, page 185

Call Home

This chapter provides an overview of the Cisco Cisco Unified Communications Manager Call Home service and describes how to configure the Cisco Cisco Unified Communications Manager Call Home feature. The Call Home feature allows to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server.

Smart Call Home

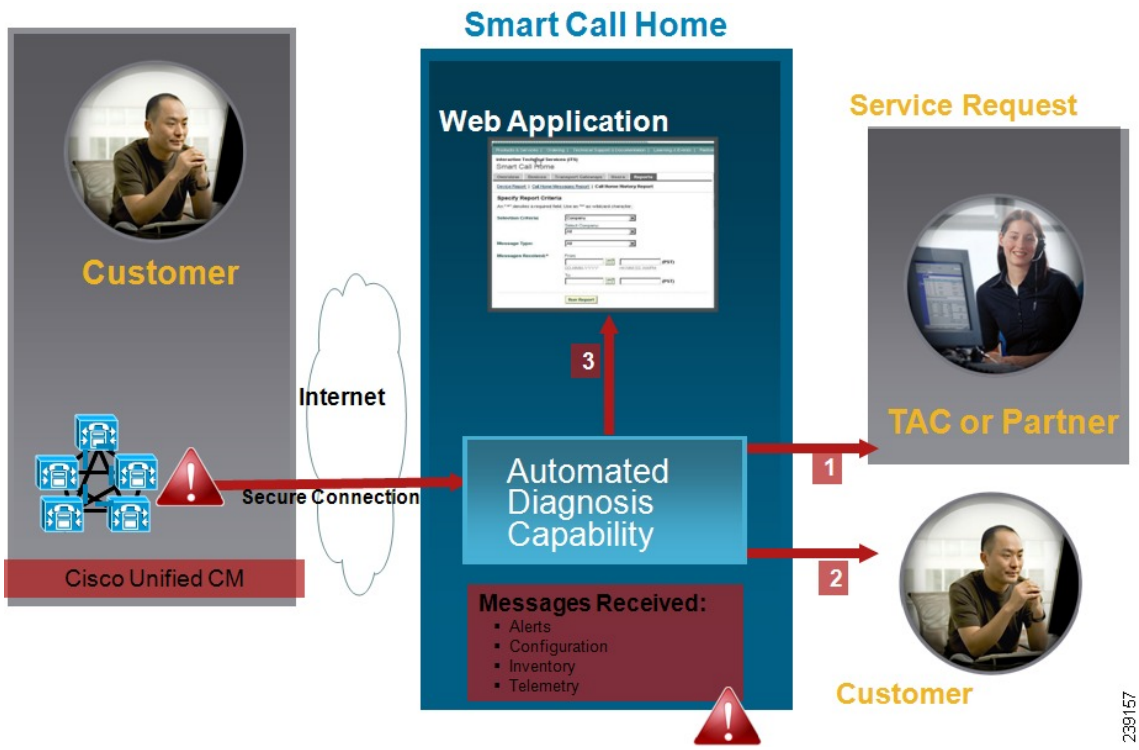
Smart Call Home provides proactive diagnostics, real-time alerts, and remediation on a range of Cisco devices for higher network availability and increased operational efficiency. It accomplishes the same by receiving and analyzing the diagnostic alerts, inventory, and other messages from Smart Call Home enabled Cisco Cisco Unified Communications Manager. This particular capability of Cisco Cisco Unified Communications Manager is called as Cisco Cisco Unified Communications Manager Call Home.

Smart Call Home offers:

- Higher network availability through proactive, fast issue resolution by:
  - Identifying issues quickly with continuous monitoring, real-time, proactive alerts, and detailed diagnostics.
  - Making you aware of potential problems by providing alerts that are specific to only those types of devices in the network. Resolving critical problems faster with direct, automatic access to experts at Cisco Technical Assistance Center (TAC).
- Increased operational efficiency by providing customers the ability to:
  - Use staff resources more efficiently by reducing troubleshooting time.
- Fast, web-based access to needed information that provides customers the ability to:
  - Review all Call Home messages, diagnostics, and recommendations in one place.

- Check Service Request status quickly.
- View the most up-to-date inventory and configuration information for all Call Home devices.

Figure 20: Cisco Smart Call Home Overview



Smart Call Home contains modules that perform the following tasks:

- Notify Customer of Call Home messages.
- Provide impact analysis and remediation steps.

For more information about Smart Call Home, see the Smart Call Home page at this location:

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Anonymous Call Home

The Anonymous Call Home feature is a sub-feature of the Smart Call Home feature that allows Cisco to anonymously receive inventory and telemetry messages. Enable this feature to keep your identification anonymous.

The following are the characteristics of Anonymous Call Home:

- The Cisco Unified Communications Manager sends only inventory and telemetry messages and not diagnostic and configuration information to Smart Call Home back-end.
- It will not send any user related information (for example, registered devices and upgrade history).

- Anonymous call home option does not require registration or entitlement for Smart Call Home feature with Cisco.
- The inventory and telemetry messages are sent periodically (first day of every month) to the Call Home back-end.
- **Include Trace logs and Diagnostic Information** option is disabled if Cisco Unified CM is configured to use Anonymous Call Home.

Inventory messages contains information about the cluster, nodes, and license.

The following table lists the inventory messages for Smart Call Home and Anonymous Call Home.

Table 66: Inventory Messages for Smart Call Home and Anonymous Call Home

Inventory messages	Smart Call Home	Anonymous Call Home
Contact Email	Applicable	Not Applicable
Contact Phone number	Applicable	Not Applicable
Street Address	Applicable	Not Applicable
Server Name	Applicable	Not Applicable
Server IP Address	Applicable	Not Applicable
Licence Server	Applicable	Not Applicable
OS Version	Applicable	Applicable
Model	Applicable	Applicable
Serial Number	Applicable	Applicable
CPU Speed	Applicable	Applicable
RAM	Applicable	Applicable
Storage Partition	Applicable	Applicable
Firmware version	Applicable	Applicable
BIOS Version	Applicable	Applicable
BIOS Information	Applicable	Applicable
Raid Configuration	Applicable	Applicable
Active Services	Applicable	Applicable
Publisher Name	Applicable	Not Applicable

Inventory messages	Smart Call Home	Anonymous Call Home
Publisher IP	Applicable	Not Applicable
Product ID	Applicable	Applicable
Active Version	Applicable	Applicable
Inactive Version	Applicable	Applicable
Product Short name	Applicable	Applicable

Telemetry messages contain information about the number of devices (IP phones, gateways, conference bridge, and so on) for each device type that is available on a Cisco Unified Communication Manager cluster. The telemetry data contains the device count for the entire cluster.

The following table lists the telemetry messages for Smart Call Home and Anonymous Call Home.

Table 67: Telemetry Messages for Smart Call Home and Anonymous Call Home

Telemetry messages	Smart Call Home	Anonymous Call Home
Contact Email	Applicable	Not Applicable
Contact Phone number	Applicable	Not Applicable
Street Address	Applicable	Not Applicable
Server name	Applicable	Not Applicable
CM User Count	Applicable	Not Applicable
Serial Number	Applicable	Applicable
Publisher name	Applicable	Not Applicable
Device count and Model	Applicable	Applicable
Phone User Count	Applicable	Applicable
CM Call Activity	Applicable	Applicable
Registered Device count	Applicable	Not Applicable
Upgrade history	Applicable	Not Applicable

Telemetry messages	Smart Call Home	Anonymous Call Home
System Status	Applicable for Host name, Date, Locale, Product Version, OS Version, Licence MAC, Up Time, MP Stat, Memory Used, Disk Usage, Active and Inactive partition used, and DNS	Applicable for Date, Locale, Product Version, OS Version, Licence MAC, Up Time, Memory Used, Disk Usage, and Active and Inactive partition used

Configuration messages contain information about the row count for each database table that is related to a configuration. The configuration data consists of table name and row count for each table across the cluster.

Smart Call Home Interaction

If you have a service contract directly with Cisco Systems, you can register Cisco Unified Communications Manager for the Cisco Smart Call Home service. Smart Call Home provides fast resolution of system problems by analyzing Call Home messages that are sent from Cisco Unified Communications Manager and providing background information and recommendations.

The Cisco Cisco Unified Communications Manager Call Home feature delivers the following messages to the Smart Call Home back-end server:

- Alerts - Contain alert information for various conditions related to environment, hardware failure, and system performance. The alerts may be generated from any node within the Cisco Cisco Unified Communications Manager cluster. The alert details contain the node and other information required for troubleshooting purposes, depending on the alert type. See topics related to Smart call home interaction for alerts that are sent to the Smart Call Home back-end server.

The following are the alerts for Smart Call Home.

By default, Smart Call Home processes the alerts once in 24 hours. Repeated occurrence of the same alert within the span of 24 hours in mixed cluster (Cisco Unified Communication Manager and Cisco Unified Presence) and is not processed by Smart Call Home.

Important The collected information is deleted from the primary AMC server after 48 years. By default, CUCM publisher is the primary AMC server.

- **Performance Alerts**
  - CallProcessingNodeCPUPegging
  - CodeYellow
  - CPUPegging
  - LowActivePartitionAvailableDiskSpace
  - LowAvailableVirtualMemory
  - LowSwapPartitionAvailableDiskSpace

- **Database - Related Alerts**
  - DBReplicationFailure
- **Failed Calls Alerts**
  - MediaListExhausted
  - RouteListExhausted
- **Crash - Related Alerts**
  - Coredumpfilefound
  - CriticalServiceDown

The configuration, inventory, and telemetry messages are sent periodically (first day of every month) to the Call Home back-end. The information in these messages enables TAC to provide timely and proactive service to help customers manage and maintain their network.

Related Topics

Smart Call Home Interaction, on page 189

Prerequisites for Call Home

To support the Cisco Cisco Unified Communications Manager Call Home service, you require the following:

- A Cisco.com user ID associated with a corresponding Cisco Cisco Unified Communications Manager service contract.
- It is highly recommended that both the Domain Name System (DNS) and Simple Mail Transfer Protocol (SMTP) servers are setup for the Cisco Cisco Unified Communications Manager Call Home feature.
  - DNS setup is required to send the Call Home messages using Secure Web (HTTPS).
  - SMTP setup is required to send the Call Home messages to Cisco TAC or to send a copy of the messages to a list of recipients through email.

Access Call Home

To access Cisco Unified Communications Manager Call Home, go to Cisco Unified Serviceability Administration and choose **CallHome** (**Cisco Unified Serviceability** > **CallHome** > **Call Home Configuration**).

Call Home Settings

The following table lists the default Cisco Cisco Unified Communications Manager Call Home settings.

Table 68: Default Call Home Settings

Parameter	Default
Call Home	Enabled
Send Data to Cisco Technical Assistance Center (TAC) using	Secure Web (HTTPS)

If default Smart Call Home configuration is changed during installation, then the same settings reflect in the Call Home user interface.

Note You must need to have a SMTP setup if you choose **Email** as the transport method and SMTP setup is not a required for **Secure Web (HTTPS)** option.

Call Home Configuration

In Cisco Unified Serviceability, choose **Call Home** > **Call Home Configuration**.

The Call Home Configuration window appears.

Note You can also configure the Cisco Smart Call Home while installing the Cisco Cisco Unified Communications Manager.

The Smart Call Home feature is enabled if you configure Smart Call Home option during installation. If you select **None**, a reminder message is displayed, when you log in to Cisco Cisco Unified Communications Manager Administration. Instructions to configure Smart Call Home or disable the reminder using Cisco Unified Serviceability is provided.

The following table describes the settings to configure the Cisco Cisco Unified Communications Manager Call Home.

Table 69: Cisco Cisco Unified Communications Manager Call Home Configuration Settings

Field Name	Description
Call Home Message Schedule	Displays the date and time of the last Call Home messages that were sent and the next message that is scheduled.

Field Name	Description
Call Home*	From the drop-down list, select one of the following options: • **None**: Select this option if you want to enable or disable the Call Home. A reminder message appears `Smart Call Home is not configured. To configure Smart Call Home or disable the reminder, please go to Cisco Unified Serviceability > Call Home or click here` on the administrator page. • **Disabled**: Select this option if you want to disable Call Home. • **Enabled (Smart Call Home)**: This option is enabled, if you have selected Smart Call Home during installation. When you select this option, all the fields under **Customer Contact Details** are enabled. With the same configuration, the options in **Send Data** are also enabled. • **Enabled (Anonymous Call Home)**: Select this option if you want to use Call Home in anonymous mode. When you select this option, all the fields under **Customer Contact Details** is disabled. With the same configuration, the Send a copy to the following email addresses (separate multiple addresses with comma) field in **Send Data** is enabled, and Include Trace logs and Diagnostics Information is disabled on Call Home page. **Note** If you enable Anonymous Call Home, the server sends usage statistics to Cisco systems from the server. This information helps Cisco to understand user experience about the product and to drive product direction.
Customer Contact Details	
Email Address*	Enter the contact email address of the customer. This is a mandatory field.
Company	(Optional) Enter the name of the company. You can enter up to 255 characters.
Contact Name	(Optional) Enter the contact name of the customer. You can enter up to 128 characters. The contact name can contain alphanumeric characters and some special characters like dot (.), underscore (_) and, hyphen (-).
Address	(Optional) Enter the address of the customer. You can enter up to 1024 characters.
Phone	(Optional) Enter the phone number of the customer.
Send Data	

Field Name	Description
Send Data to Cisco Technical Assistance Center (TAC) using	This is a Mandatory field. From the drop-down list, select one of the following options to send Call Home messages to Cisco TAC: • **Secure Web (HTTPS)**: Select this option if you want to send the data to Cisco TAC using secure web. • **Email**: Select this option if you want to send the data to Cisco TAC using email. For email, the SMTP server must be configured. You can see the Host name or IP address of the SMTP server that is configured. **Note** A warning message displays if you have not configured the SMTP server. • **Secure Web (HTTPS) through Proxy**: Select this option if you want to send the data to Cisco TAC through proxy. Currently, we do not support Authentication at the proxy level. The following fields appear on configuring this option: ◦ **HTTPS Proxy IP/Hostname***: Enter the proxy IP/Hostname. ◦ **HTTPS Proxy Port***: Enter the proxy port number to communicate.
Send a copy to the following email addresses (separate multiple addresses with comma)	Check this check box to send a copy of the Call Home messages to the specified email addresses. You can enter up to a maximum of 1024 characters.
Include Trace logs and Diagnostic Information	Check this check box to activate the Cisco Cisco Unified Communications Manager to collect logs and diagnostics information. **Note** This option is active only if the Smart Call Home is enabled. The message contains diagnostic information collected at the time of alert along with trace message. If the trace size is less than 3 MB, then the traces will be encoded and sent as part of alert message and if the traces are more than 3 MB then the path of the trace location is displayed in the alert message.
Save	Saves your Call Home configuration. **Note** After you save your Call Home Configuration, an End User License Agreement (EULA) message appears. If you are configuring for the first time, you must accept the license agreement. **Tip** To deactivate the Call Home service that you activated, select the **Disabled** option from the drop-down list and click **Save**.
Reset	Resets to last saved configuration.

Field Name	Description
Save and Call Home Now	Saves and sends the Call Home messages. **Note** A message appears **Call Home Configuration saved and all Call Home Messages sent successfully** if the messages are sent successfully.

Limitations

The following limitations apply when Cisco Cisco Unified Communications Manager or Cisco Unified Presence server is down or unreachable:

- Smart Call Home fails to capture the date and time of the last Call Home messages sent and the next message scheduled, until the server is reachable.
- Smart Call Home does not send the Call Home messages, until the server is reachable.
- Smart Call Home will be unable to capture license information in the inventory mail when the publisher is down.

The following limitations are due to Alert Manager and Collector (AMC):

- If an alert occurs on node A and the primary AMC server (by default, publisher) is restarted, and if the same alert occurs within a span of 24 hours on the same node, Smart Call Home resends the alert data from node A. Smart Call Home cannot recognize the alert that has already occurred because the primary AMC was restarted.
- If an alert occurs on node A and if you change the primary AMC server to another node, and if the same alert occurs within a span of 24 hours on the same node, Smart Call Home recognizes it as a fresh alert on node A and sends the alert data.
- The traces that are collected on the primary AMC server may reside on the primary AMC server for a maximum of 60 hours in few scenarios.

The following are the limitations in the mixed cluster (Cisco Unified Communications Manager and IM and Presence) scenario:

- Alerts like **CallProcessingNodeCpuPegging**, **Media List Exhausted**, **Route List Exhausted** are not applicable to IM and Presence.
- If the user changes primary AMC server to IM and Presence, then Smart Call Home cannot generate Custer Overview reports for **Media List Exhausted** and **Route List Exhausted.**
- If the user changes primary AMC server to IM and Presence, then Smart Call Home cannot generate Overview reports for **DB Replication** alert.

References for Call Home

For more information about Smart Call Home, refer the following URL:

- Smart Call Home Service Introduction

http://www.cisco.com/en/US/products/ps7334/serv_home.html